UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
DEPARTAMENTO DE ELETRÔNICA E SISTEMAS
CURSO DE GRADUAÇÃO EM ENGENHARIA ELETRÔNICA

BRENO CORDEIRO BISPO

SISTEMA DE CONTROLE DE ACESSO VIA RFID/NFC

Recife
2019

BRENO CORDEIRO BISPO

SISTEMA DE CONTROLE DE ACESSO VIA RFID/NFC

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Eletrônica da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Bacharel em Engenharia Eletrônica.

Área de concentração: Sistemas Embarcados.

Orientador: Profº. Dr. Marco Aurélio Benedetti Rodrigues.

Recife

2019

Catalogação na fonte
Bibliotecária Maria Luiza de Moura Ferreira, CRB-4 / 1469

B622s Bispo, Breno Cordeiro.
Sistema de controle de acesso via RFID/NFC / Breno Cordeiro Bispo. - 2019.
65 folhas, il., abr. e sigl.

Orientador: Prof. Dr. Marco Aurélio Benedetti Rodrigues.

TCC (Graduação) – Universidade Federal de Pernambuco. CTG. Departamento de Engenharia Eletrônica, 2019.
Inclui Referências.

1. Engenharia Eletrônica. 2. RFID. 3. NFC. 4. ESP32. 5. MQTT. 6. Internet das Coisas. 7. Android. I. Rodrigues, Marco Aurélio Benedetti (Orientador). II. Título.

UFPE

621.381 CDD (22. ed.) BCTG/2019-229

BRENO CORDEIRO BISPO

SISTEMA DE CONTROLE DE ACESSO VIA RFID/NFC

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Eletrônica da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Bacharel em Engenharia Eletrônica.

Aprovada em: __07__/__06__/_2019_.

BANCA EXAMINADORA

_____

Profº. Dr. Marco Aurélio Benedetti Rodrigues (Orientador)
Universidade Federal de Pernambuco

_____

Profº. Dr. Gilson Jerônimo da Silva Junior (Examinador Interno)
Universidade Federal de Pernambuco

_____

Profº. Dr. Raul Camelo de Andrade Almeida (Examinador Interno)
Universidade Federal de Pernambuco

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, por todos os ensinamentos, profissionais e pessoais, ao qual venho construindo ao longo do tempo. Seguidamente a meus pais, batalharam e ainda lutam para que não falte nada nos meus estudos. Desde o meu nascimento até a formação em engenharia.

Em seguida ao meu orientador, Prof. Marco Aurélio Benedetti, me auxiliou na construção deste trabalho, me guiou e abriu novos caminhos e ideias, para eu seguir em frente com meus objetivos. Por último, a todos os integrantes do Laboratório de Interface Homem-Maquina (LIHOM), tiveram a tremenda paciência nas diversas vezes que deixei muitos deles trancados no laboratório quando o sistema falhava. Em especial, agradeço a Naelso Cunha (que sugeriu a utilização da placa de desenvolvimento utilizada neste trabalho e me auxilio nas devidas modificações do hardware), a Érico Cavalcante (que deu boas aulas introdutórias ao abrangente uso do Sistema de Banco de Dados SQL) e a Gustavo Ribeiro (profissional em design de objetos CAD e impressora 3D, auxiliou na prototipagem deste projeto).

RESUMO

Este trabalho apresenta a implementação das tecnologias RFID e NFC aplicadas a um Sistema de Controle de Acesso, constituído por Módulo RFID/NFC e Servidor, no qual são hospedados serviços de Banco de Dados MySQL, Broker MQTT e Interface gráfica NODE-RED, ambos alocados na mesma rede local. Por meio de protocolos de rede via WiFi ou Ethernet, o Módulo e o Servidor se comunicam em tempo real, o que possibilita o monitoramento dos registros de acesso ao estabelecimento feitos pelo Módulo RFID/NFC. Este trabalho exemplifica uma aplicação de um típico sistema IoT (*Internet of Things*) de rápida implementação e bom custo-benefício em conjunto com uma tecnologia simples de comunicação wireless que muitos smartphones aderem cada vez mais no mercado, o NFC.

Palavras-chave: RFID. NFC. ESP32. MQTT. Internet das Coisas. Android.

ABSTRACT

This work presents the implementation of RFID and NFC technologies applied to an Access Control System, consisting of RFID / NFC Module and Server, where it is hosted by MySQL Database, MQTT Broker and NODE-RED Graphical Interface, both allocated to the same local network. Through WiFi or Ethernet network protocols, the Module RFID/NFC and Server communicate to each other in real time, which enables the monitoring of the access records of the establishment made by the RFID / NFC Module. This work exemplifies an application of a typical IoT (Internet of Things) system of fast implementation and good cost-benefit. In conjunction with a simple wireless communication technology that many smartphones increasingly adhere to the market, the NFC.

Keywords: RFID. NFC. ESP32. MQTT. Internet of Things. Android.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ESP32	Microcontrolador
HCE	Host Card Emulation
HF	Alta frequência (High Frequency)
HTTP	Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol)
IDE	Ambiente de Desenvolvimento Integrado (Integrated Development Environment)
IoT	Internet das Coisas (Internet of Things)
ISO	Organização Internacional para Padronização (International Organization for Standardization)
LF	Baixa frequência (Low Frequency)
LIHOM	Laboratório de Interface Homem-Máquina
Mosquitto	Broker MQTT
MQTT	Transporte de Telemetria em Fila de Mensagens (Message Queue Telemetry Transport)
MySQL	Banco de Dados
NFC	Comunicação por campo próximo (Near Field Communication)
PN532	Leitor RFID/NFC
RFID	Identificação por radio-frequência (Radio-Frequency IDentification)
RTC	Relógio de Tempo Real (Real Time Clock)
SE	Secure Element
SSID	Service Set Identifier
UART	Transmissor/Receptor Universal Assíncrono (Universal Asynchrounous Receiver/Transmiter)
UHF	Ultra-High Frequency
UID	Identificação Única (Unique Identification)

SUMÁRIO

1 INTRODUÇÃO

Recentemente, procedimentos de identificação automática se tornam cada vez mais populares nos serviços das indústrias, compras, distribuições logísticas, etc. Procedimentos automáticos de identificação, como códigos de barra, QR *Code* e identificação por radio-frequência (RFID) existem para prover informações sobre pessoas, animais, objetos ou produtos em trânsito (FINKENZELLER, 2010).

As grandes vantagens de utilizar rádio frequência para este tipo de identificação é a possibilidade de fazer leitura da informação sem a necessidade de contato. Além disto, estas etiquetas podem carregar uma quantidade muito maior de informações que um código de barras, por exemplo.

Esta característica de permitir gravar e ler informações cria a possibilidade de manter um histórico a respeito do deslocamento e modificações de um produto ou pessoas dentro de um estabelecimento.

Um sistema de RFID é a integração de uma série de componentes que permite a identificação e o gerenciamento de objetos ou pessoas. Com o passar do tempo houve o surgimento de uma sub-divisão do RFID chamada NFC (*Near Field Communication*), cuja frequência de trabalho é de 13,5 MHz. Feita a partir da tecnologia de contato sem fio para melhorar a transmissão de dados ponto a ponto e a emulação de cartões de acesso e pagamento, por exemplo, através de um celular (IGOE; COLEMAN; JEPSON, 2014/01).

A acessibilidade destas tecnologias se tornou cada vez mais fácil, tornando assim possível construir um sistema completo de controle de acesso baseado nas tecnologias anteriormente citadas, de forma simples e de fácil construção. Além disto, com o auxílio de um servidor provedor dos serviços de Banco de Dados MySQL (XAMPP, 2019), MQTT Broker Mosquitto (HILLAR, 04/2017) e o *software* NODE-RED (NODE-RED, 2019) é possível o acompanhamento em tempo real dos registros feitos pelos Módulos RFID/NFC de um estabelecimento, tornando o trabalho apresentado um exemplo típico de uma aplicação IoT (CHABANNE; URIEN; SUSINI, 2011).

O principal diferencial deste projeto com relação aos sistemas de controle de acesso no mercado, foi a utilização da tecnologia NFC presente em diversos smartphones aplicada ao sistema de controle de acesso. Com isto, é possível a comunicação via NFC com o Módulo RFID/NFC, devidamente configurado no celular, para execução de determinadas tarefas. Por exemplo, habilitar uma porta com o celular através de um aplicativo Android construído especificamente para este sistema de controle de acesso. Esse tipo de projeto se torna mais conveniente ao usuário, pois, cria um novo método de acesso aos locais desejados com apenas um smartphone,

sem a necessidade de manuseio de uma etiqueta pelos usuários, como consequência a redução de etiquetas e custo de implementação do sistema.

1.1 Objetivo geral

Criar um sistema completo de controle de acesso utilizando a tecnologia de RFID e NFC em portas eletromagnéticas.

1.2 Objetivo específico

- Determinar os componentes de *hardware* que compõem o sistema.
- Criar um *software* dedicado ao Módulo, para aquisição dos dados, via RFID ou NFC, e transmissão dos dados ao servidor.
- Criar *software* de gerenciamento, armazenamento e exibição dos dados pelo servidor.
- Criar um aplicativo dedicado à comunicação NFC entre o smartphone Android e o Módulo.
- Confecção dos invólucros (em impressão 3D) para proteção, isolamento e instalação do Módulo RFID/NFC no acesso ao Laboratório de Interface Homem-Máquina (LIHOM).

1.3 Estrutura do trabalho

Este trabalho se divide em três partes principais:

1) Fundamentação teórica: Neste tópico é apresentado todo o conhecimento teórico necessário para o entendimento da tecnologia que este trabalho utiliza, assim como o fenômeno físico por trás da transmissão de dados sem contato, a descrição do Microcontrolador utilizado e os protocolos de comunicação utilizados.

2) Materiais e Métodos: Neste tópico é apresentado os *hardwares* utilizados para a construção completa do sistema, os *softwares*, as diversas funcionalidades do sistema e rotinas.

3) Resultados e discussões: Neste tópico são apresentados todos os resultados obtidos, mostrando o sistema em funcionamento até o momento, limitações, possíveis aplicações e planos futuros.

4) Conclusão: Neste tópico é apresentada uma breve recapitulação do que foi desenvolvido e as principais características que torna este trabalho singular em relação aos sistemas de controle de acesso no mercado.

2 FUNDAMENTAÇÃO TEÓRICA

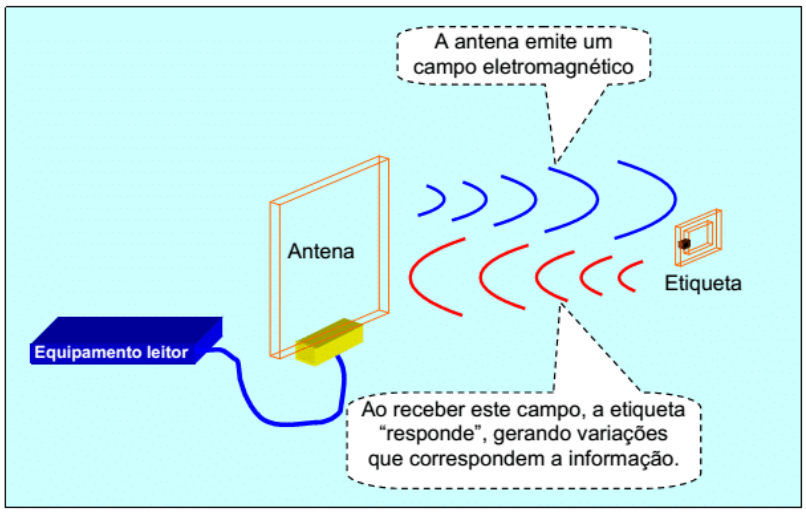
Neste capítulo é apresentado todo o conhecimento teórico necessário para o desenvolvimento e entendimento do sistema implementado. Dividida em quatro partes:

1) Tecnologia RFID - Ilustra diversos conceitos existentes na tecnologia de identificação por rádio-frequência e aplicações.
2) Tecnologia NFC - Ilustra os principais conceitos desta tecnologia de comunicação *wireless* entre dois dispositivos e suas aplicações.
3) Microcontrolador ESP32 - Ilustra de forma breve o principal *hardware* responsável por executar as funções do Módulo RFID/NFC.
4) Protocolo de Comunicação MQTT - Ilustra os principais conceitos e aplicações de um dos protocolos de comunicação de rede mais utilizados em IoT.

2.1 Tecnologia RFID

O funcionamento de uma etiqueta RFID é obtido através da indução eletromagnética em circuitos ressonantes, chamados também de transpônderes. O leitor gera campo eletromagnético que se propaga pelo meio até chegar ao circuito ressonante existente na etiqueta RFID e excitando-o. Esta excitação gera corrente que alimenta o circuito da etiqueta. A resposta deste circuito causam modulações no campo eletromagnético refletido pela etiqueta, que são captadas pelo leitor e posteriormente decodificadas. A Figura 1 abaixo, apresenta de forma ilustrativa a troca de informações entre a antena do leitor e a etiqueta RFID (CUNHA, 2016).

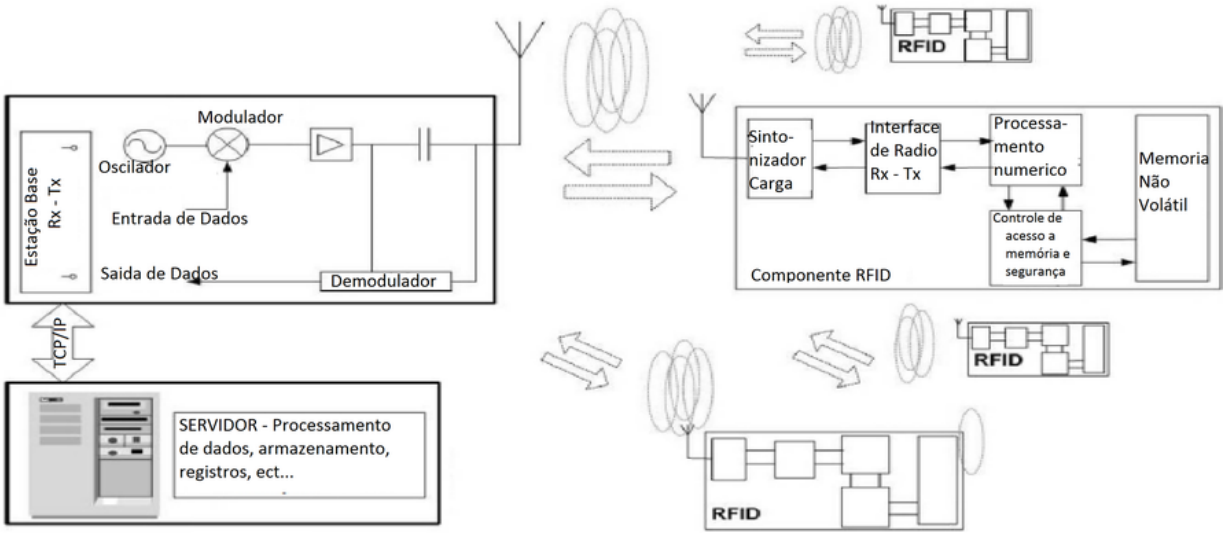
Figura 1 – Troca de informações entre antena e etiqueta RFID.



Fonte: CUNHA (2016).

Sistemas de RFID tipicamente consistem em módulos fixos com funções de identificação e processamento das informações contidas nas etiquetas, *tokens* eletrônicos ou *Smart Cards*. Estes módulos quando conectados a servidores de processamento de dados e implementados de forma adequada a níveis de análises, armazenamento e rastreabilidade, podem ter aplicabilidade singular no mercado, conforme a Figura 2.

Figura 2 – Elementos de um Sistema RFID.



Fonte: Adaptado de CHABANNE (2011).

A faixa de frequência determina também as características de atuação do sistema RFID. Essas faixas são classificadas em (CHABANNE; URIEN; SUSINI, 2011):

- LF (L*ow Frequency*) - de 30 a 300 kHz. As etiquetas desta faixa de frequência são fabricadas em 125 kHz ou 134,2 kHz. O alcance do campo magnético para leitura das etiquetas, nas aplicações existentes no mercado para esta faixa de frequência, giram em torno de 10 a 50 cm.
- MF (*Medium Frequency*) - de 300 kHz a 3 MHz. Cujo alcance do campo magnético para leitura gira em torno de 50 a 80 cm.
- HF (*High Frequency*) - de 3 MHz até 30 MHz. Etiquetas construídas em 13,56 MHz. O alcance do campo magnético para leitura fica em torno de 50 a 80 cm.
- UHF (*Ultra-High Frequency*) - de 300 MHz até 3 GHz. Nesta faixa, as etiquetas são fabricas em 868 MHz na Europa e em 915 MHz nos Estados Unidos.

A sensibilidade do campo eletromagnético, que geralmente se encontra no mercado, é cerca de 1 a 5 m.

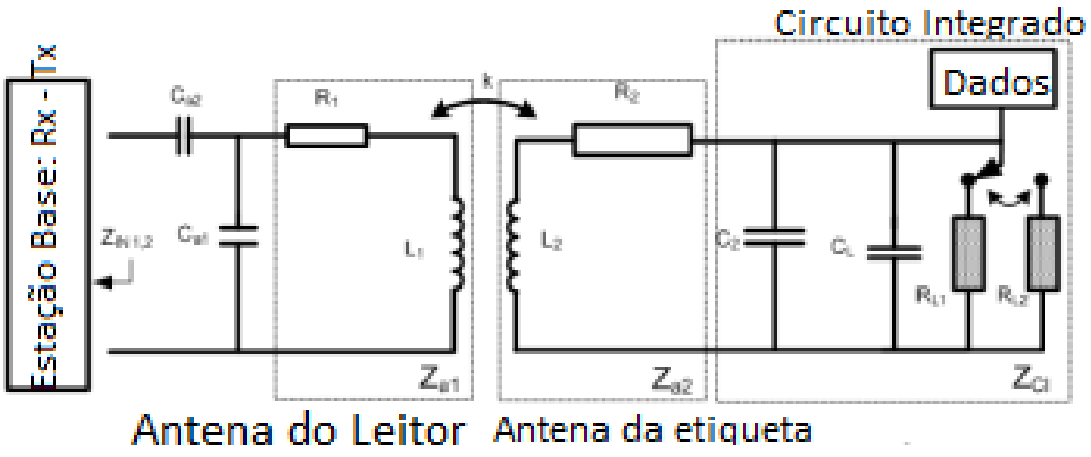
- SHF (*Super-High Frequency*) ou Micro-ondas - de 3 GHz a 30 GHz. Duas frequências para RFID no mercado: 2,45 GHz e 5,8 GHz. Esta faixa de frequência é utilizada em aplicações industriais, científicas e médicas. A sensibilidade de leitura pode atingir distâncias maiores que 10 m.

As características de propagação, alcance e recepção de cada faixa de frequência são inerentes ao ambiente, tipo do material existente, obstruções, técnicas de fabricação ou potência de emissão do campo eletromagnético. Portanto, as características de sensibilidade ou alcance nas faixas de frequência podem variar.

Os mais importantes princípios de operação da tecnologia RFID são:

Acoplamento indutivo - A maioria das Etiquetas de RFID são passivas. Nas faixas de frequências entre LF e HF, o campo excitante é predominantemente magnético. Quando o chip RFID passivo se aproxima do campo magnético gerado pelo leitor, há transferência de energia entre o leitor e a etiqueta (pelo principio da Lei de Faraday) e o chip é alimentado. O chip é visto pelo leitor como cargas devido ao fenômeno de indução mútua e variações da corrente elétrica da antena, conforme a Figura 3. Para a transferência de dados, quando há transferência adequada de energia para alimentar o chip da etiqueta RFID, o mesmo modula sua carga de acordo com os dados que o chip apresenta em sua memória. Já que o leitor vê a etiqueta como carga, as variações de carga são interpretadas pelo leitor como dados da etiqueta RFID. A natureza da carga no chip pode ser resistiva ou capacitiva. Muitos dos chips RFID usam o mecanismo de modulação resistiva (CHABANNE; URIEN; SUSINI, 2011).

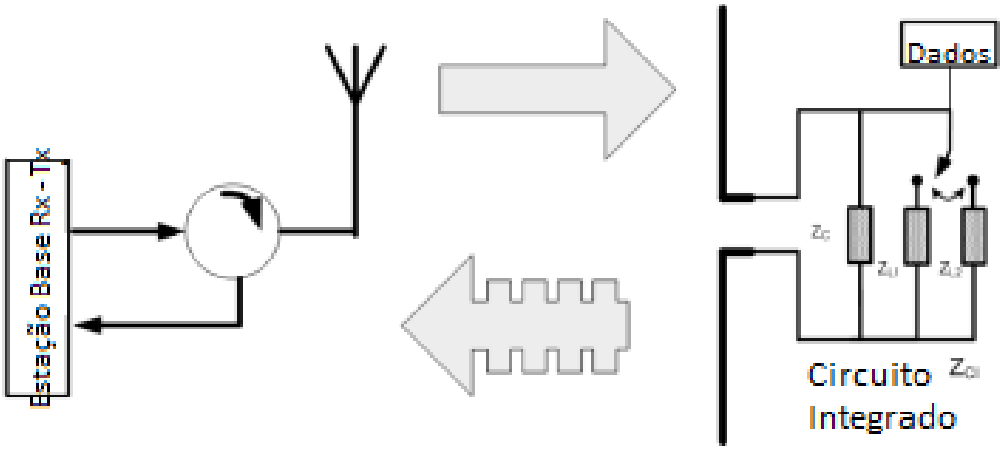
Figura 3 – Acoplamento indutivo.



Fonte: Adaptado de CHABANNE (2011).

Acoplamento Retrodifusão - A partir da faixa de frequência UHF, o efeito de acoplamento é eletromagnético. Quando a onda incidente, emitida pelo leitor, encontra uma etiqueta RFID, esta onda é refletida. A potência recebida pela etiqueta deve ser suficiente para que a potência refletida por esta chegue ao leitor. O chip RFID modula sua impedância de acordo com os dados presentes em sua memória ao qual se deseja transmitir. A variação da impedância pode ser resistiva, capacitiva ou ambas. A informação é então transmitida até o leitor, através do campo eletromagnético modulado, refletido pela etiqueta (conforme a Figura 4) (CHABANNE; URIEN; SUSINI, 2011).

Figura 4 – Acoplamento retrodifusão.



Fonte: Adaptado de CHABANNE (2011).

A principal lei física que rege o funcionamento de dispositivos RFID é a Lei de Faraday descrita pela equação (1)

$$\oint_c E.dl = -\frac{d}{dt}\int_s B.dA \tag{1}$$

> "A força eletromotriz induzida em qualquer circuito fechado é igual ao negativo da variação do fluxo magnético com o tempo na área delimitada pelo circuito". (HAYT, WILLIAM. Engineering Electromagnetics 5ª ed. [S.l.]: McGraw-Hill. p. 312.)

A faixa de frequência utilizada pelo sistema RFID construído neste trabalho é em torno de 13,5 MHz, cuja forma de propagação da energia no espaço se dá pela variação do campo magnético no meio.

Reescrevendo a Equação (1) temos

$$u_i = \oint E_i.dl = -\frac{d\Psi(t)}{dt}, \tag{2}$$

onde Ψ_i é o fluxo total que passa pelo respectivo enrolamento definindo pela respectiva área A_i, u_i a tensão induzida no enrolamento i, I_i equivale à corrente induzida no enrolamento i, M equivale à indutância mútua entre os enrolamentos e L equivale à indutância própria do enrolamento, conforme a Figura 5. Através da definição de indutância própria e indutância mútua (FINKENZELLER, 2010)

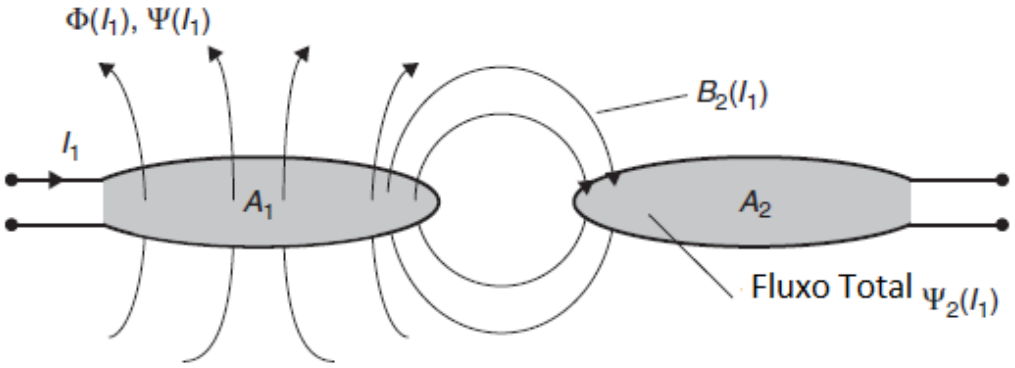
$$L = \frac{\Psi}{I}, \tag{3}$$

$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \oint_{A2} \frac{B_2(I_1)}{I_1}.dA_2, \tag{4}$$

$$M = M_{12} = M_{21}, \tag{5}$$

é possível descrever analiticamente, através de modelos físicos em análise de circuitos, o acoplamento magnético entre a antena do leitor e a etiqueta RFID (FINKENZELLER, 2010), ilustrado na Figura 3.

Figura 5 – Acoplamento entre duas espiras ou enrolamentos via fluxo magnético.



Fonte: Adaptado de FINKENZELLER (2010).

2.2 Tecnologia NFC

A tecnologia RFID pode ser definida como um processo de identificação através de rádio frequência. Já a NFC nada mais é do que uma subdivisão do RFID, feita para melhorar a transmissão de dados ponto a ponto.

2.2.1 Fórum NFC

> "O Fórum NFC é uma aliança para especificar os padrões NFC baseados nos padrões ISO / IEC. O Fórum NFC foi estabelecido com o objetivo de habilitar a tecnologia NFC e se espalhar pelo mundo. É uma associação da indústria sem fins lucrativos, formada para melhorar o uso de comunicação sem fio de curto alcance em eletrônicos de consumo, dispositivos móveis e PCs. A missão do Fórum NFC é promover o uso da tecnologia NFC através do desenvolvimento de especificações, garantir a interoperabilidade entre dispositivos e serviços, além disso educar o mercado sobre a tecnologia NFC" (COSKUN; OK; OZDENIZCI, 2012).

O Fórum NFC padronizou três modos de operação (BACIOCCOLA, 2019):

- Modo leitura e gravação.
- Comunicação peer-to-peer.
- Emulação de cartão.

Outro importante desenvolvimento introduzido pelo Fórum NFC é a marca registrada "N" que é um símbolo universal do NFC, para que os consumidores possam identificar facilmente onde dispositivos habilitados para NFC podem ser usados (COSKUN; OK; OZDENIZCI, 2012).

2.2.2 Modos de funcionamento

O NFC opera entre dois dispositivos numa distância relativamente curta. A comunicação ocorre através do espectro de frequência de 13,56 MHz, como no RFID. Porém, a tecnologia NFC opera em três diferentes modos (ilustrados na Figura 6, os três modos de funcionamento da tecnologia NFC):

Modo Ler/Escrever - Este modo de comunicação permite que o dispositivo ativo NFC, por exemplo, um celular, leia o conteúdo existente na memória das etiquetas NFC ou escreva. Neste modo de operação, o Fórum NFC determina várias especificações e padrões de tipos das etiquetas, a operação das mesmas e o formato dos dados transmitidos entre os dispositivos. Cinco categorias de etiquetas são definidas no Fórum NFC (IGOE; COLEMAN; JEPSON, 2014/01).

Tipo 1:

- Baseado na especificação ISO-14443A.
- Compatibilidade de leitura e escrita, configurado por fabricação.
- 96 bytes a 2 kilobytes de memória.
- Exemplo: Innovision Topaz, Broadcom BCM20203.

Tipo 2:

- Similar ao tipo 1, o tipo 2 é baseado nas especificações das etiquetas NXP/Philips Mifare Ultralight (ISO-14443A).
- Compatibilidade de leitura e escrita, configurado por fabricação.
- 96 bytes a 2 kilobytes de memória.
- Exemplo: NXP Mifare Ultralight.

Tipo 3:

- São baseados nas etiquetas Sony FeliCa (ISO-18092 e JIS-X-6319-4).
- Compatibilidade de leitura e escrita, configurado por fabricação.
- Memória variável até 1MB.
- Examplo: Sony FeliCa.

Tipo 4:

- Similar ao tipo 1, o tipo 4 é baseado nas especificações das etiquetas NXP DESFire (ISO-14443A).
- Compatibilidade de leitura e escrita, configurado por fabricação.
- 2, 4 ou 8 KB de memória.
- Examplo: NXP DESFire, SmartMX-JCOP.

Tipo 5:

- Baseada na etiqueta Mifare Classic (ISO-14443A). Propriedade da empresa NXP Semiconductors.
- Provavelmente o tipo de etiqueta mais utilizada hoje em dia.

- Opções de memória: 192, 768, ou 3,584 bytes.
- Examplo: NXP Mifare Classic 1K, Mifare Classic 4K, Mifare Classic Mini.

Modo Ponto-a-Ponto (Peer-to-Peer) - Neste modo a comunicação ocorre entre dois dispositivos ativos NFC (smartphones, Geladeiras ou Maquinas de Lavar Inteligentes, Microcontroladores com Sensores e Módulos NFC acoplados para comunicação, etc) de forma bidirecional. Estes dispositivos podem trocar informações, como uma carteira virtual, fotos digitais, ou qualquer outro tipo de dado, como sites, informações de pareamento *Bluetooth*, senhas de *Wifi*, etc. Este modo de operação é regulamentado pela ISO/IEC 18092. A quantidade de informações trocadas é pequena na maioria das aplicações de comunicação Ponto-a-Ponto, para a praticidade do usuário que estão utilizando esta tecnologia (COSKUN; OK; OZDENIZCI, 2012).

Modo Emulação de Cartão - Neste modo, o smartphone emula um cartão inteligente baseado na (ISO - 14443). Quando o usuário aproxima o smartphone de um leitor NFC, o leitor reconhece como um cartão e lê as informações presentes no "cartão" emulado pelo smartphone. Umas das grandes aplicações desse método é a transferência segura de dados como pagamento via NFC, ou aplicações de validação de *tiquets* virtuais, etc (COSKUN; OK; OZDENIZCI, 2012).

A Figura 6 demonstra de forma ilustrativa todos os modos de operação da tecnologia NFC.

Figura 6 – Modos de funcionamento NFC.

Fonte: Adaptado de CUNHA (2016).

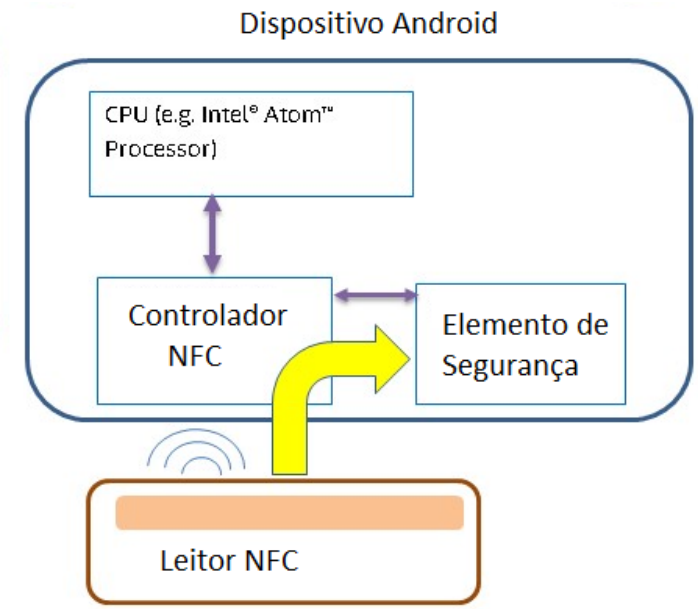
2.2.3 Android Card Emulation

Muitos dos smartphones Android, que oferecem a funcionalidade NFC, tem suporte para Emulação de Cartão via NFC. Geralmente, o cartão é emulado por um chip separado no dispositivo móvel, chamado de elemento de segurança (SE).

A versão do Android 4.4 introduz um método adicional de emulação de cartão que não envolve elemento de segurança, chamado host-based card emulation (HCE). Isso permite que muitos aplicativos Android possam emular cartão e se comunicar diretamente com o leitor NFC (BASYARI; NASUTION; DIRGANTARA, 2015).

Emulação de Cartão com Elemento de Segurança (SE) - Quando a emulação do cartão provém de elemento de segurança, por exemplo o chip SIM, este é responsável por fornecer as informações durante a comunicação com o terminal NFC presente no *smartphone* e nenhuma aplicação Android é envolvida na transação, como ilustrado na Figura 7. Depois que a transação de dados é completada, um aplicativo Android pode consultar o SE diretamente para consultar o *status* da transação e notificar o usuário (WEI, 09/2014).

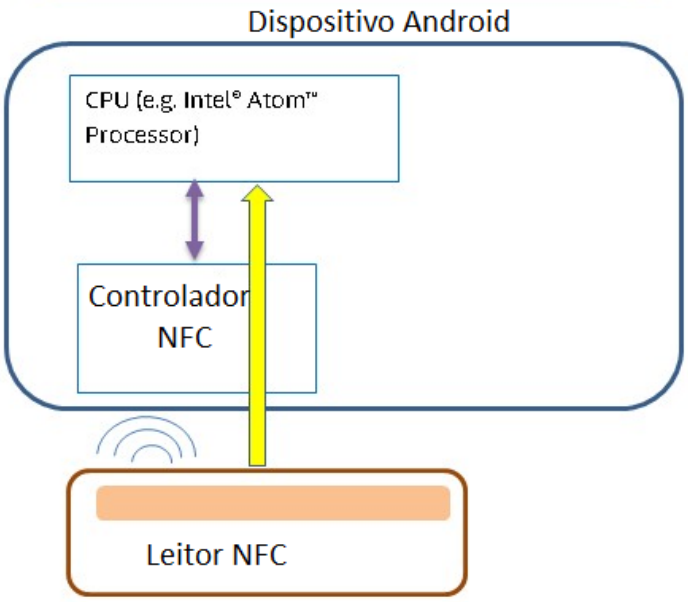
Figura 7 – Emulação de cartão com SE.



Fonte: Adaptado de WEI (2014).

Host-based Card Emulation (HCE) - Quando um cartão NFC é emulado utilizando HCE, os dados são derivados diretamente da CPU do smartphone, ao qual a aplicação Android está rodando diretamente (ilustrado na Figura 8), ao invés do protocolo feito pelo SE (WEI, 09/2014).

Figura 8 – Sistema HCE.



Fonte: Adaptado de WEI (2014).

A partir do Android 4.4, o suporte de emulação de cartão é baseado na especificação ISO/IEC 14443-4 e o processo das Unidades de Aplicação do Protocolo (APDUs) são definidas pela especificação ISO/IEC 7816-4. Através desta APDU é possível criar mais uma camada de segurança, via *software*, entre a comunicação de dois dispositivos NFCs. A comunicação entre um dispositivo NFC e um aplicativo Android apenas será realizada com sucesso, caso haja validação de segurança, ou seja, a mesma APDU coexistam em ambos os lados.

A arquitetura HCE no Android é baseada em componentes do Serviço Android (conhecidos como “HCE Services”). Uma das principais vantagens de um serviço é que ele pode ser executado em segundo plano sem qualquer interface do usuário. Esse é um ajuste natural para muitos aplicativos HCE, como cartões de fidelidade ou de trânsito, com os quais o usuário não precisa lançar o aplicativo para usá-lo. Em vez disso, aproximar o dispositivo contra o leitor NFC inicia o serviço corretamente (mesmo que o aplicativo não esteja aberto no smartphone), executando a transação em segundo plano. Deixando livre para o desenvolvedor criar sua própria interface de notificações com o serviço HCE funcionando em segundo plano (BASYARI; NASUTION; DIRGANTARA, 2015).

Quando o usuário toca um dispositivo em um leitor de NFC, o sistema Android precisa saber com qual serviço de HCE o leitor de NFC realmente deseja se comunicar. É aqui que entra a especificação (ISO) / IEC 7816-4, esta define uma maneira de selecionar aplicativos, centralizada em torno de uma identificação de aplicativo (AID).

Um AID consiste em até 16 bytes. Caso esteja emulando cartões para uma infraestrutura de leitor de NFC existente, os AIDs que esses leitores estão procurando devem estar bem definidos na construção do aplicativo no qual se deseja utilizar o serviço HCE (BASYARI; NASUTION; DIRGANTARA, 2015).

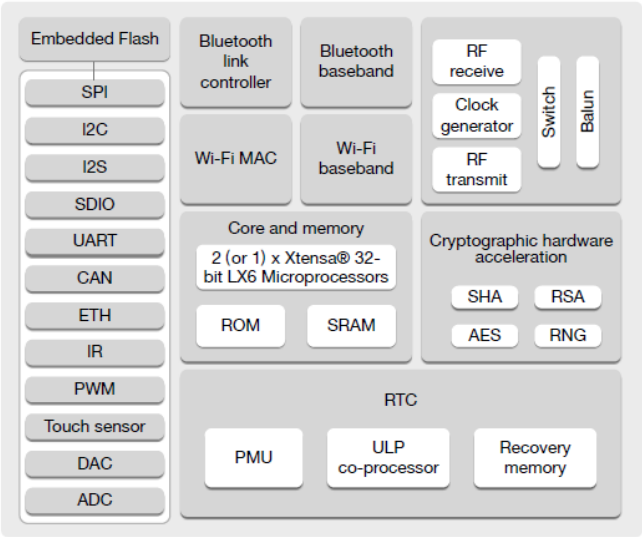
2.3 Microcontrolador ESP32

O ESP32 (ilustrado na Figura 9) é o microcontrolador desenvolvido pela Espressif Systems e utilizado neste trabalho. Pode ser programado através da Arduino IDE e possui diversas funcionalidades embutidas em *hardware. T*ornou-se um microcontrolador de referência para projetos voltados para a área de IoT e comunicação *wireless*. Periféricos e funcionalidades do ESP32 estão ilustrados com mais detalhes na Figura 10 (ESP32. . . , 2019).

Figura 9 – ESP32.

Fonte: ESPRESSIF (2019).

Figura 10 – Diagrama de Blocos das funcionalidades do ESP32.



Fonte: ESPRESSIF (2019).

2.4 Protocolo de Comunicação MQTT

O MQTT é um protocolo de conectividade Machine-to-Machine (M2M) em IoT. É um protocolo leve para transferência de dados que trabalha com o mecanismo de Publicação-Subscrição (Publish-Subscribe) que tem como base o protocolo TCP/IP. Através da comunicação tipo Ethernet ou WiFi, os dispositivos presentes na rede comunicam entre si (HILLAR, 04/2017).

O MQTT é um protocolo que oferece o equilíbrio ideal para os desenvolvedores de IoT:

1. Protocolo leve - permite a implementação em hardware de dispositivo altamente restringido e em redes de largura da banda limitada e de alta latência.

2. Protocolo flexível - possibilita o suporte a diversos cenários de aplicativo para dispositivos e serviços de IoT.

De todos os protocolos de comunicação o MQTT é um protocolo de rede que vem se popularizando em diversas aplicações IoT. Em comparação com o tradicional protocolo de rede HTTP 1.1:

1. O HTTP é um protocolo síncrono. O cliente espera que o servidor responda. No mundo da IoT, a comunicação síncrona tem sido um problema devido ao grande número de dispositivos e à rede, muitas vezes não confiável e de alta latência. Um protocolo de mensagem assíncrono é muito mais adequado para aplicativos de IoT. Assim, os sensores podem enviar leituras e permitir que a rede descubra o caminho e a sincronização ideal para entregar aos dispositivos e serviços de destino (YUAN, 2017/04).

2. O HTTP é um protocolo de um para um. O cliente faz uma solicitação e o servidor responde. Sem a possibilidade de enviar a mesma informação para diversos clientes simultaneamente.

3. No HTTP o cliente precisa iniciar a conexão, ou seja, o cliente deve primeiramente enviar solicitação de comando para o servidor e posteriormente receberá resposta, contendo instruções a serem feitas vindas do servidor. Em um aplicativo de IoT, muitos dispositivos e sensores apenas aguardam alguma instrução vinda de outro dispositivo, ou seja, sem a necessidade de solicitar algum comando.

4. O HTTP é um protocolo pesado com muitos cabeçalhos e regras. Ele não é adequado para redes com muitas limitações de velocidade e constantes instabilidades.

O protocolo MQTT define duas entidades na rede: broker e inúmeros clientes (ilustrado na Figura 11). O broker se comporta como um separador que recebe todas

as mensagens dos clientes e, em seguida, roteia essas mensagens para os clientes de destino relevantes. Um cliente é qualquer dispositivo que possa interagir com o broker, recebendo ou enviando mensagens. Um cliente pode ser um sensor de IoT em campo ou um aplicativo em um Data Center que processa dados de IoT. Após a conexão dos dispositivos na rede, a conexão do cliente ao broker é realizada através do direcionamento de IP do broker feita pelo cliente e pela porta de rede (geralmente se utiliza a porta 1883).

1. O cliente conecta-se ao broker. Ele pode se subscrever (*subscribe*) a qualquer "tópico" de mensagens no broker. Essa conexão pode ser uma TCP/IP simples ou uma conexão TLS criptografada para mensagens sensíveis.

2. O cliente publica (*publish*) as mensagens em um tópico, enviando a mensagem no respectivo tópico ao qual se deseja enviar ao broker.

3. Em seguida, o broker encaminha a mensagem a todos os clientes que se subscreveram (*subscribe*) nesse tópico.

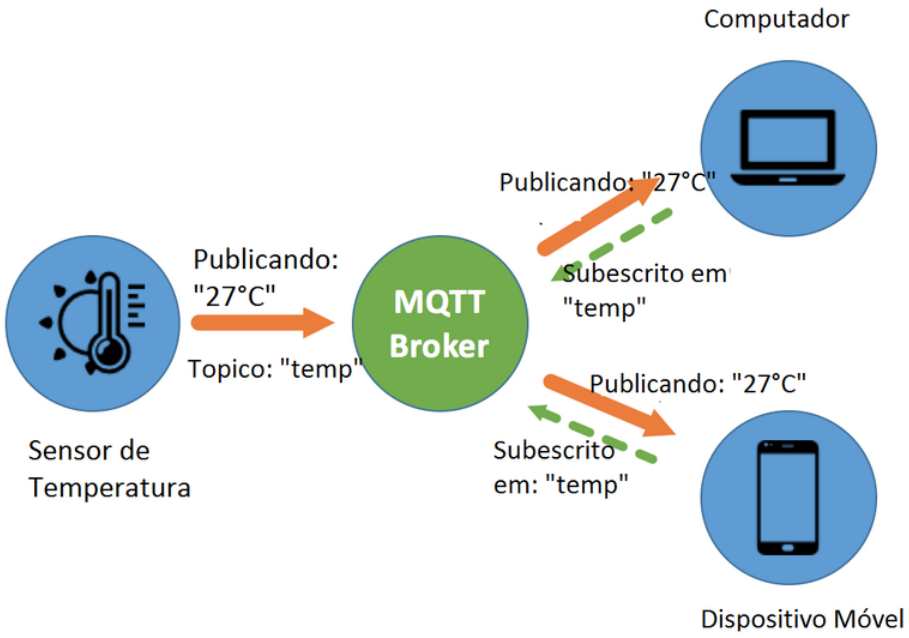
O mecanismo de Publicação-Subscrição (Publish-Subscribe) é ilustrado na Figura 11 da seguinte forma:

Primeiramente o dispositivo ao se conectar com o broker através do IP da máquina onde o broker está alocado e pela porta 1883 (porta padrão do protocolo MQTT), subscreve-se nos respectivos tópicos ao qual deseja receber mensagens. São ilustrados o Computador e o Dispositivo Móvel que se subscreveram no tópico "temp".

Posteriormente, o dispositivo responsável por enviar informações a outros dispositivos, conecta-se ao broker e envia mensagens ao broker através do respectivo tópico ao qual deseja repassar as informações.

Na Figura 11, temos um Sensor de Temperatura que publica a mensagem "27ºC" no tópico "temp". Em seguida o broker verifica quais dispositivos estão subscritos no tópico "temp" e realiza uma publicação para todos os dispositivos (Computador e Dispositivo Móvel) subscritos no respectivo tópico.

Figura 11 – Exemplo de um sistema MQTT.



Fonte: Adaptado de AZEVEDO (2018).

Como as mensagens do MQTT são organizadas por tópicos, o desenvolvedor tem a flexibilidade de especificar qual os determinados clientes podem interagir com determinadas mensagens (YUAN, 2017/04).

3 MATERIAIS E MÉTODOS

Primeiramente foi analisado os equipamentos e métodos de análise mais adequados para este projeto (placa de desenvolvimento, leitor RFID/NFC, tipos de *softwares*, etc). Em seguida é descrito de forma detalhada quais equipamentos e *softwares* utilizados ao qual se tornou possível a realização deste projeto. Este capitulo é divido em duas partes:

1) Equipamentos de Hardware - É descrito todos os componentes eletrônicos utilizados neste projeto, desde os componentes que constituem o Módulo RFID/NFC até a construção da topologia implementada no sistema de controle de acesso.
2) Desenvolvimento do *Software* - É descrito de forma detalhada todos as rotinas e *softwares* desenvolvidos para o funcionamento adequado do sistema de controle de acesso. Ilustra os algoritmos utilizados pelo microcontrolador, protocolos de comunicação em rede, método de armazenamento dos registros e construção de uma interface gráfica.

3.1 Equipamentos de Hardware

Nesta seção é apresentado todos os elementos de hardware utilizados neste trabalho. Cada componente do Módulo RFID/NFC é descrito de forma isolada e posteriormente é apresentado a montagem e topologia de comunicação de todo o sistema.

3.1.1 Placa de Desenvolvimento

Foi utilizada a placa de desenvolvimento da OLIMEX ESP32-EVB (ilustrada na Figura 12), cujo microcontrolador é o ESP32. Esta placa possui diversos recursos de hardware já embutidos que foram utilizados em conjunto com o microcontrolador ESP32, por exemplo, módulo cartão SD, Relé e módulo Ethernet, além de outros não utilizados, como interface de comunicação CAN (*Controller Area Network*), emissor e receptor Infravermelho, suporte e gerenciamento de baterias LiPo de 3.7 V, entre outros. Embora o microcontrolador funcione a 3.3 V, a placa de desenvolvimento funciona a somente 5 V (OLIMEX. . . , 2017).

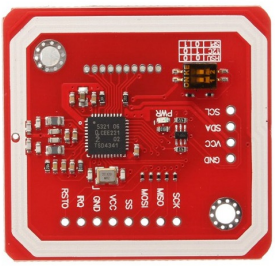
Figura 12 – Placa de desenvolvimento OLIMEX ESP32-EVB.

Fonte: OLIMEX (2017).

3.1.2 Leitor RFID/NFC

Para a integração das tecnologias RFID e NFC em um mesmo Módulo foi utilizado o chip PN532 como leitor RFID/NFC. Através da configuração adequada deste leitor, o funcionamento das rotinas de leitura RFID ou NFC podem coexistir.

Figura 13 – Leitor RFID/NFC PN532



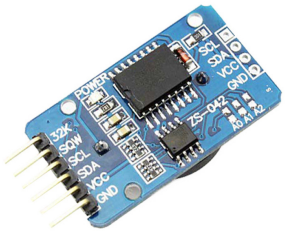
Fonte: EBAY (2019).

O chip, localizado aproximadamente no centro da placa, possui antena em PCB debaixo das marcações brancas, conforme a Figura 13. Este leitor, criado pela NXP *Semiconductors*, foi utilizado neste projeto, pois, além de identificar as etiquetas passivas descritas pela ISO-14443, também pode se comunicar com outros dispositivos com tecnologia de NFC. Além disto possui três formas de comunicação (UART, SPI, I2C), sendo de fácil interação com a placa de desenvolvimento utilizada neste projeto.

3.1.3 Relógio *Real Time Clock* DS3231

Para a configuração do sistema de tempo real, foi utilizado o relógio com bateria RTC (Real Time Clock) DS3231, conforme a Figura 14, para a aquisição da data e hora de entrada e saída no estabelecimento.

Figura 14 – RTC DS3231.



Fonte: EBAY (2019).

3.1.4 *Buzzer*

Foi utilizado um *buzzer* (ilustrado na Figura 15) como sinalizador sonoro das diversas funções que ocorrem no Módulo.

Figura 15 – Buzzer.

Fonte: EBAY (2019).

3.1.5 Equipamento Eletroímã

Para realizar a liberação ou bloqueio do acesso às portas, foi utilizado um eletroímã convencional para porta, com alimentação de 12V (ilustrado na Figura 16):

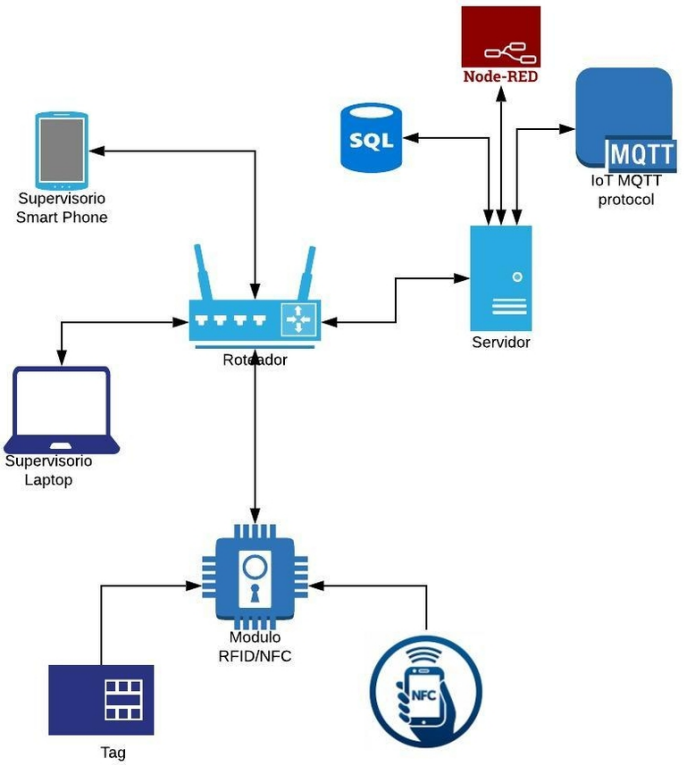
Figura 16 – Fechadura tipo Eletroimã.

Fonte: AMAZON (2019).

3.1.6 O Sistema Operacional

Foi utilizada uma máquina com sistema operacional Windows Server 2012 como servidor dos serviços de Banco de Dados MySQL, Broker MQTT Mosquitto e NODE-RED. Alocado na mesma rede local do Módulo RFID/NFC, hospedando todos os serviços necessários para o funcionamento integral do sistema, conforme a Figura 17.

Figura 17 – Sistema Geral.



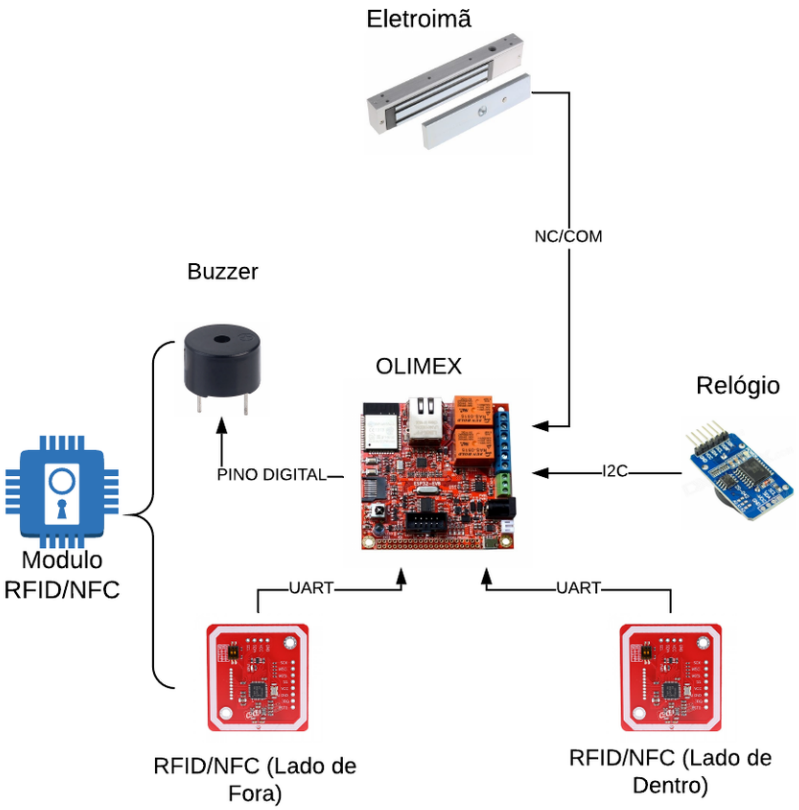
Fonte: O autor.

3.1.7 O Módulo RFID/NFC

Os componentes eletrônicos presentes no Módulo RFID/NFC são (ilustrados na Figura 18):

- Placa de desenvolvimento OLIMEX ESP32 EVB: Responsável por executar todas as rotinas do Módulo RFID/NFC.
- Dois leitores RFID/NFC PN532: Conectados à placa OLIMEX via comunicação UART (3.3 V, GND, Rx, Tx), responsáveis pela leitura das etiquetas RFID e comunicação NFC.
- Relógio RTC DS3231: Conectado à placa OLIMEX via comunicação I2C (3.3 V, GND, SDA, SCL), responsável pela aquisição da data e hora atual.
- *Buzzer:* Conectado à placa OLIMEX a um pino digital genérico da placa OLIMEX (Pino Digital, GND), responsável por emitir sinais sonoros de acordo com a rotina executada pelo microcontrolador.

Figura 18 – Módulo RFID/NFC.



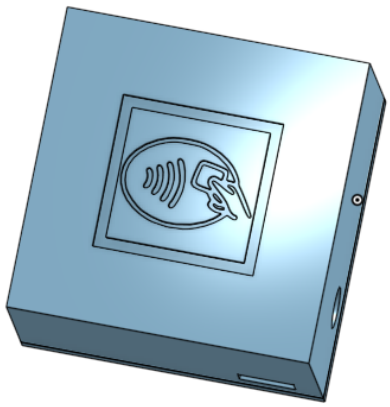
Fonte: O autor.

Para isolamento, proteção e posicionamento do módulo na parede, foram confeccionadas invólucros (fabricados em impressão 3D) para a parte de dentro do estabelecimento e parte de fora do estabelecimento, conforme a Figura 19 e 20, respectivamente.

Dentro da caixa, ilustrada na Figura 19, encontra-se a placa de desenvolvimento. Foram interconectados um dos leitores PN532 com comunicação tipo UART, o relógio RTC DS3231 com comunicação tipo I2C e um *buzzer* conectado a um pino digital da placa de desenvolvimento.

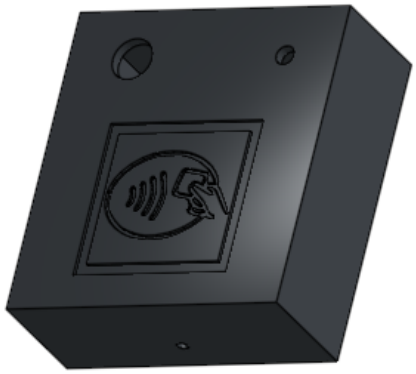
Dentro da caixa, ilustrada na Figura 20, encontra-se o outro leitor RFID/NFC. Foi utilizado um cabo tipo RJ45 para interligar o leitor à placa de desenvolvimento, através de um furo na parede do estabelecimento. Esta ligação estabelece a comunicação UART e fornece energia ao leitor.

Figura 19 – Invólucro da parte interna do estabelecimento.



Fonte: O autor.

Figura 20 – Invólucro da parte externa do estabelecimento.



Fonte: O autor.

3.2 Desenvolvimento do Software

Nesta seção é apresentado todos *softwares* e rotinas utilizados neste trabalho. É apresentado todos os algoritmos e funcionalidades executadas pelo Módulo RFID/NFC. Em seguida a apresentação do aplicativo iTAG, responsável pela comunicação NFC entre o dispositivo Android e o Módulo RFID/NFC. Posteriormente os *softwares* utilizados para a implementação do protocolo MQTT e o Banco de Dados. Por fim é ilustrado o *software* NODE-RED, responsável pela construção da interface gráfica e processamento dos dados trafegados entre o Módulo RFID/NFC, Banco de Dados e Broker MQTT.

3.2.1 Firmware para IDE Arduino

Para programação de todas as rotinas e funcionalidade do Módulo RFID/NFC executadas pelo microcontrolador ESP32, foi utiliza a IDE do Arduino, cuja linguagem nativa de programação é C/C++. Como já existem bibliotecas prontas na comunidade Arduino, muitas delas foram utilizadas e modificadas para o desenvolvimento deste projeto.

3.2.2 Rotina geral do Módulo RFID/NFC

A Figura 21, ilustra todas as principais rotinas e funções que são executadas no microcontrolador.

Primeiramente, assim que o Módulo é ligado, todos os parâmetros, variáveis globais da rotina e as devidas configurações de comunicação são realizadas.

Posteriormente, o Módulo verifica se ha alguma etiqueta RFID presente. Caso tenha, é verificado se é alguma etiqueta especial como MAC (etiqueta para cadastro) ou MDC (etiqueta para exclusão de cadastro) ou etiqueta de Reset.

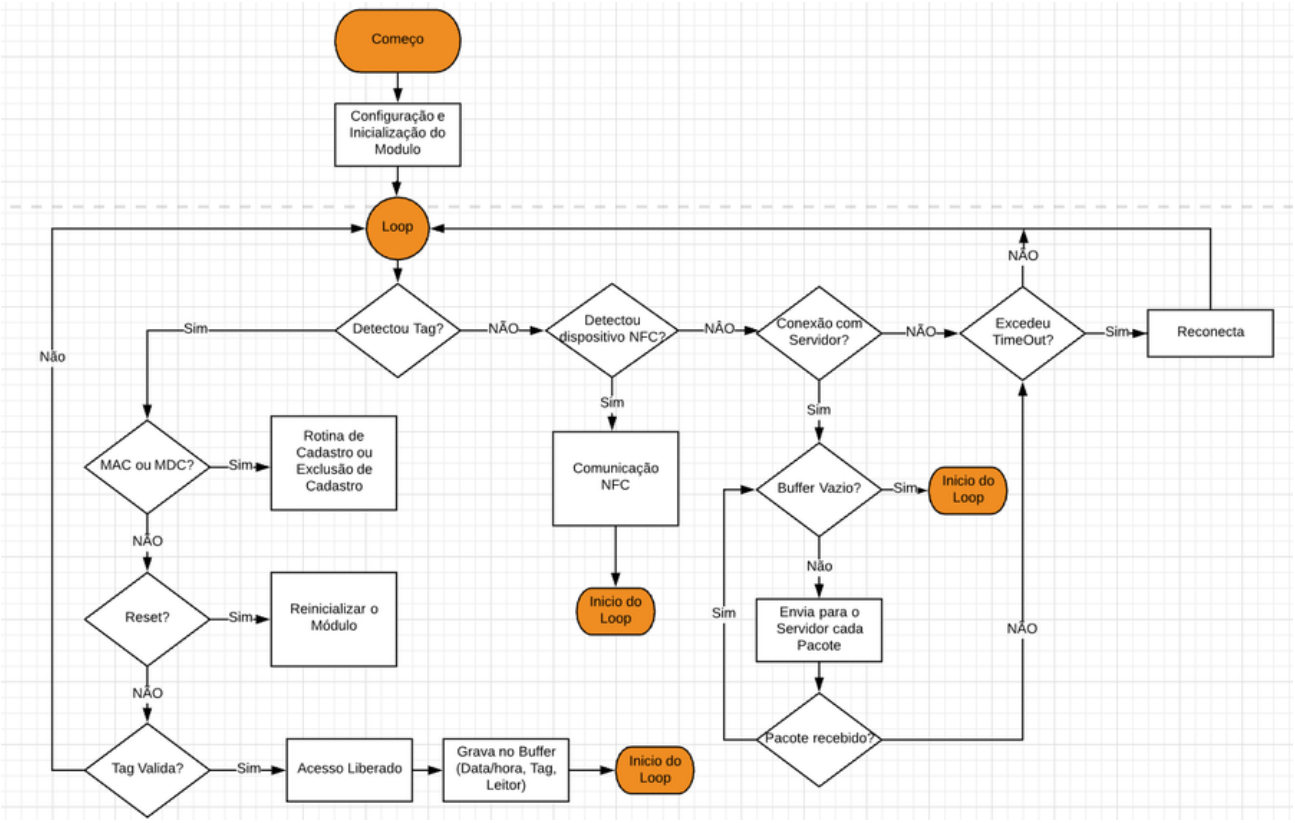
- Se sim, entrará na rotina de cadastro ou exclusão de cadastro do sistema ou de reinicialização do Módulo.
- Senão, entrará na rotina de liberação ou bloqueio do sistema.

Por fim, é armazenado na memória o pacote de dados contendo todas as informações necessárias para o envio ao servidor.

Caso haja a presença de um smartphone, o Módulo executará a comunicação NFC descrita com mais detalhe na Figura 22. Se não for detectado algum dispositivo NFC, então verificará a conexão com o broker alocado no servidor. A conexão com o servidor será verificada. Após a confirmação de conexão, verifica-se primeiramente

se o buffer está vazio, senão enviará o primeiro pacote da fila de pacotes. Após o envio, serão aguardados no máximo 2 segundos de resposta do servidor. Caso o Módulo receba o mesmo pacote que enviou, conclui-se que os dados foram recebidos pelo servido com sucesso e a rotina seguirá para o próximo pacote da fila. Se não tiver recebido nenhum pacote nesse intervalo de 2 segundos ou ter recebido de forma equivocada, a conexão será verificada novamente. Se a conexão estiver comprometida, será realizada uma nova tentativa, após um intervalo “TimeOut” de 30 segundos.

Figura 21 – Rotina principal.



Fonte: O autor.

3.2.3 Funcionalidades do Módulo

Nesta seção é apresentado todas as rotinas e funcionalidades presentes no Módulo RFID/NFC.

I) *Modo leitura de etiqueta*

Ao aproximar uma etiqueta (que não seja etiquetas especiais como MAC, MDC ou de Reset) perto do leitor, caso seja identificada e válida, um ‘bip’ será entoado e

a porta ficará aberta por 2 segundos e fechará. Caso não seja autorizada, um ‘bip’ continuo e longo será entoado negando o acesso ao usuário.

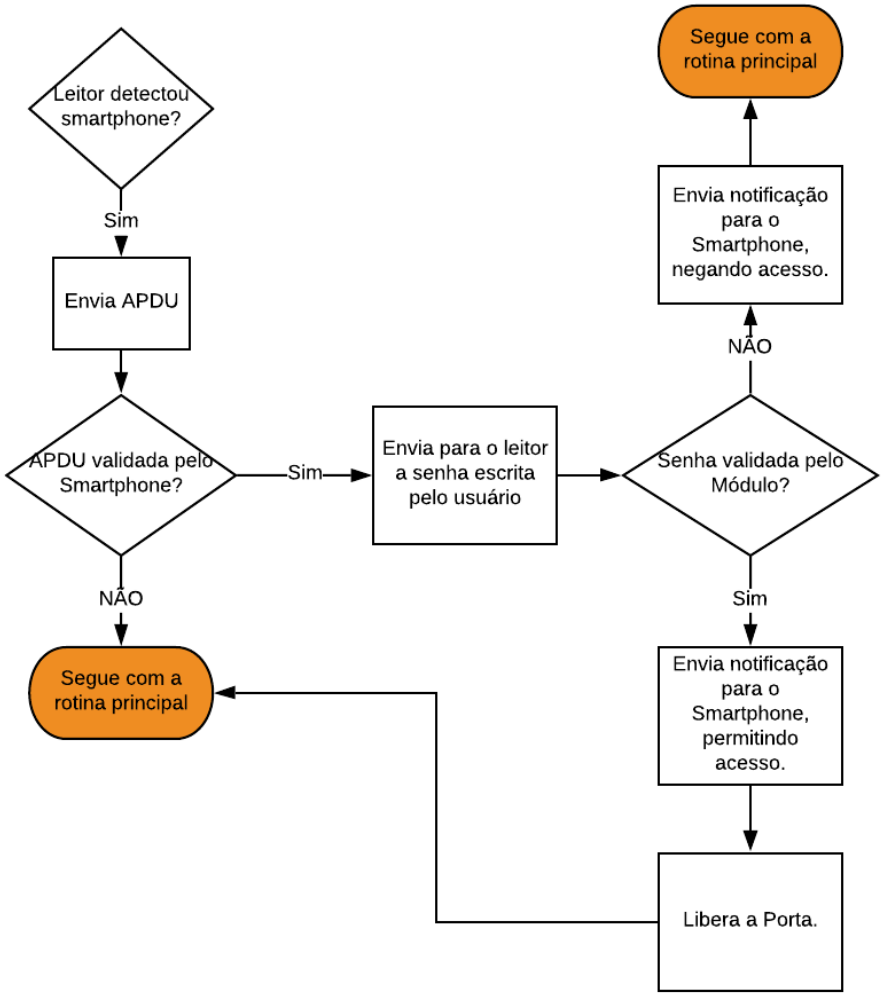
II) *Modo leitura NFC HCE*

Para que o smartphone se comporte como cartão inteligente, deve - se realizar os seguintes passos:

- Habilitar o dispositivo para comunicação NFC no dispositivo Android.
- Abrir o aplicativo iTAG.
- Inserir a senha de acesso no campo abaixo do tópico “Digite sua Senha”, conforme a Figura 23, ilustrada no tópico 3.2.4. Esta senha por convenção foi adotada como a própria identificação única (UID) do cartão do usuário após o seu cadastro no sistema.
- Aproximar o smartphone contra o leitor para que a leitura seja efetuada com sucesso. Caso a senha seja autorizada um ‘bip’ é entoado e a porta ficará aberta por 2 segundos e fechará. Caso não for autorizada, um ‘bip’ continuo e longo será entoado negando o acesso ao usuário.

A Figura 22 descreve de forma breve a rotina de comunicação NFC que ocorre entre o leitor NFC e o smartphone.

Figura 22 – Rotina de comunicação NFC.



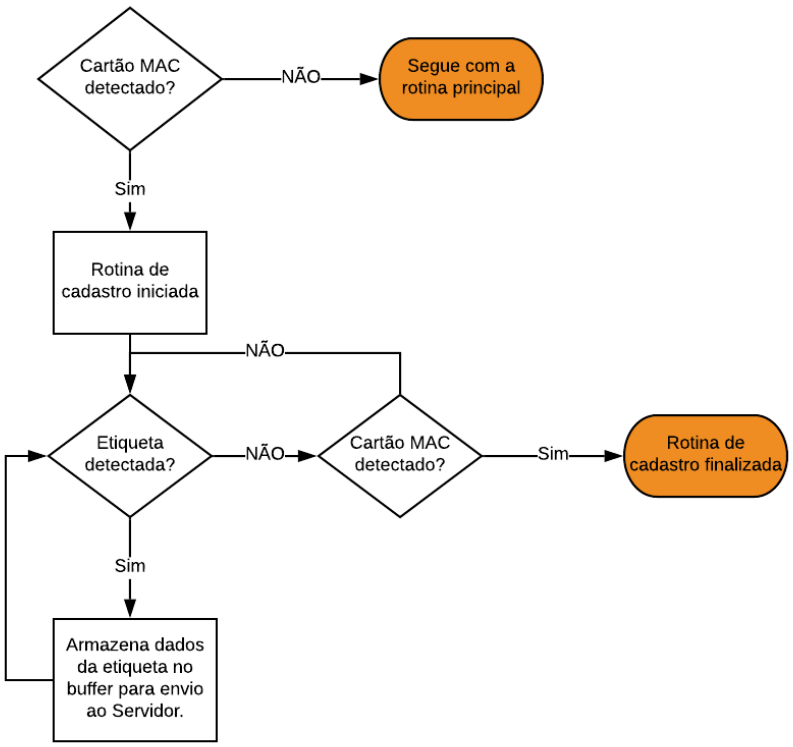
Fonte: O autor.

III) *Modo Cadastro*

Primeiramente é necessário obter a etiqueta MAC (etiqueta especial nomeada para cadastro). Segundo, ao passar o cartão no Módulo, e o cartão for detectado, começará a função de cadastramento de cartões.

Após passar o MAC, passe os cartões que se deseja cadastrar. Depois passe o MAC novamente para finalizar o cadastro, conforme a Figura 23.

Figura 23 – Rotina de cadastro.



Fonte: O autor.

Após o fechamento do cadastro irá aparecer na tela do Supervisório em Uxx (o índice “xx” representa a numeração do Módulo no sistema, podendo ser 01, 02, 03, etc. . .), todas as etiquetas que foram guardadas no módulo, porém, sem validação. Na tabela Uxx irá aparecer o campo USER em branco, para todas as etiquetas recém inseridas no sistema.

Para a validação dessas etiquetas é necessário preencher o campo do tópico UPDATE/CADASTRO, no Supervisório. Após o lançamento de cadastro de uma etiqueta, o Módulo emitirá um ‘bip’, indicando que a respectiva etiqueta foi validada com sucesso.

Obs: Após o cadastro da etiqueta no Sistema, evitar desligamento do Módulo até a validação da etiqueta no Módulo.

IV) *Modo Exclusão do Cadastro*

É apresentado neste tópico três métodos para a exclusão de cadastro de um ou mais usuários do sistema.

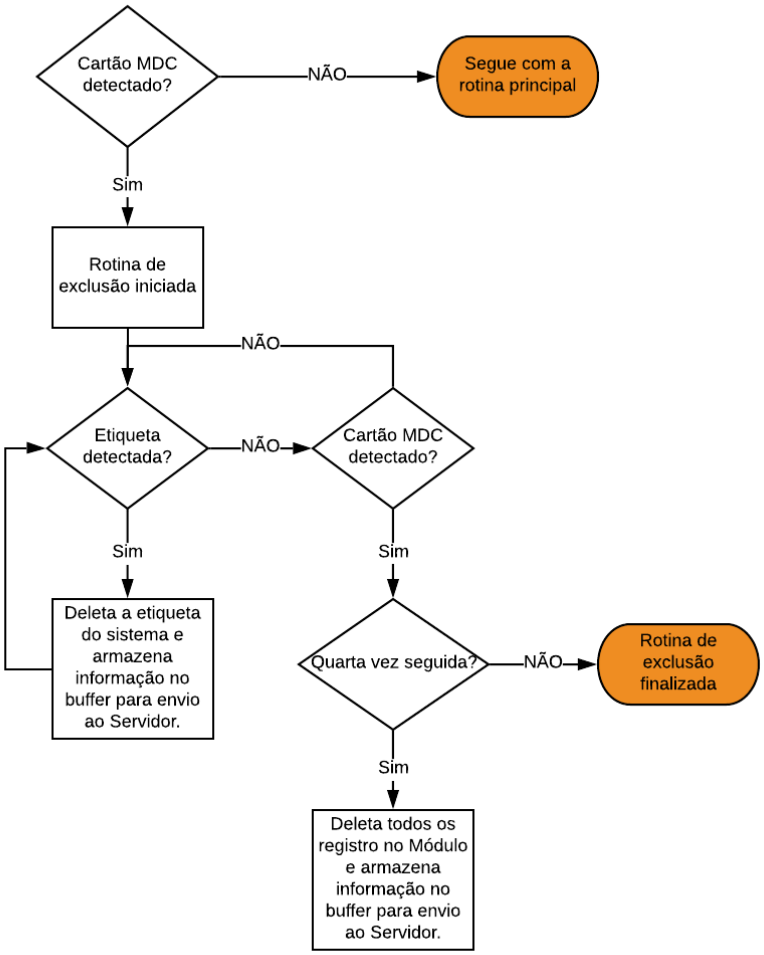
Exclusão Manual: Feito através de uma etiqueta especial chamada MDC. Após passar o MDC no Módulo, a função de exclusão será acionada e passar as etiquetas

que se deseja excluir do sistema. Por fim, deve-se passar o MDC novamente para finalizar a função de exclusão de cadastro, conforme o diagrama.

Exclusão Total: Para limpar todos os registros do Módulo é necessário passar 4 vezes seguidas a etiqueta MDC. Após este procedimento toda a memória de 1 MB do Módulo será zerada.

A figura 24, ilustra as rotinas de exclusão de cadastro manual e total:

Figura 24 – Rotina de exclusão de cadastro manual.



Fonte: O autor.

Exclusão Remoto: Através do Supervisório no tópico Descadastro, para exclusão é necessário digitar a respectiva etiqueta que se deseja deletar do sistema, assim um 'bip' vindo do Módulo será entoado sinalizando que a respectiva etiqueta foi excluída do sistema e da memória do Módulo.

V) *Configuração do Módulo*

A primeira rotina do Módulo, após a inicialização, são as definições das variáveis globais que serão utilizadas na rotina principal. As variáveis a serem utilizadas no Módulo para conexão da rede, servidor, etiqueta de cadastro (MAC), etiqueta de exclusão de cadastro (MDC) e Reset são:

- CONN = Variável que escolhe o método de conexão (**ETH** ou **WIFI**).
- SERVER = Variável que indica o IP do servidor.
- IP = Variável que indica o IP do Modulo.
- GATEWAY = Variável que indica o Gateway da Rede.
- SUBNET = Variável que indica a máscara da rede.
- IDM = Variável que indica o nome do Módulo.
- MAC = Variável que indica a etiqueta MAC.
- MDC = Variável que indica a etiqueta MDC.
- RESET = Variável que indica a etiqueta responsável em reiniciar manualmente o Módulo.
- MQTT_USER = Variável que indica o usuário para conexão ao MQTT Broker.
- MQTT_PASS = Variável que indica a senha para conexão ao MQTT Server.
- SSID = Variável que indica o SSID da Rede WiFi da Rede.
- PASS = Variável que indica a senha da Rede WiFi da Rede.

Para a configuração dessas variáveis, é necessário um cartão MicroSD contendo arquivo de texto chamado “/CONFIG.txt”. Através desse arquivo texto o Módulo lerá todas as variáveis respeitando o seguinte formato obrigatório:

CONN:ETH / WIFI**;**

SERVER:192.168.0.2**;**

IP:192.168.0.10**;**

GATEWAY:192.168.0.1**;**

SUBNET:255.255.255.0**;**

IDM:LIH_NFC_U02**;**

MAC:14845634**;**

MDC:14868538**;**

RESET:14865986**;**

MQTT_USER:u02**;**

MQTT_PASS:12345**;**

SSID:“SSID da rede WiFi”**;**

PASS:“Senha da rede WiFi”**;**

Caso o tópico CONN for ETH, a conexão do módulo com a rede será realizada via Protocolo Ethernet. Caso for WiFi, a conexão do módulo com a rede sera realizada via Protocolo WiFi utilizando o SSID e PASS definidas na configuração.

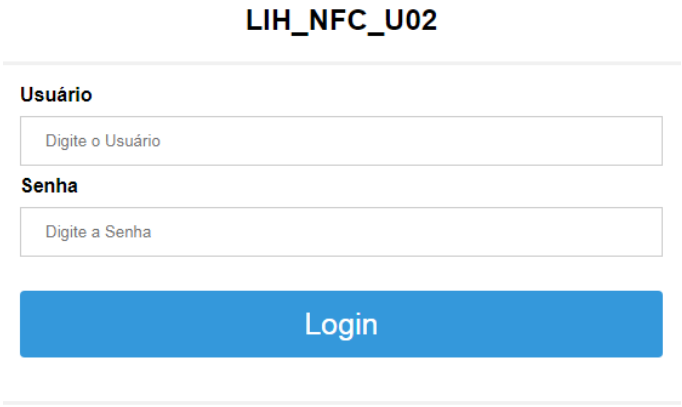
Com este método, o Módulo se torna mais simples de ser configurado. Pois, através de um cartão MicroSD, as constantes do Módulo podem ser facilmente adaptadas para qualquer outro sistema semelhante ao descrito neste trabalho. Com o propósito de evitar a reprogramação do microcontrolador ESP32 via *software*.

Após a primeira configuração do Módulo RFID/NFC com o cartão MicroSD, todas as informações presentes no arquivo de texto “/CONFIG.txt” são armazenadas na memória interna não-volátil do microcontrolador ESP32, logo não será mais necessário o uso constante do cartão MicroSD. Caso seja necessário atualizar algum dado dentro da memória do microcontrolador, nesta situação a utilização do cartão Micro SD se tornará necessária.

VI) *Web Server Independente*

Essa funcionalidade, chamada “Modo SOS”, foi implementada para que em casos de emergência, por exemplo, não haja comunicação com o servidor e os leitores RFID/NFC, o ESP32 se comporta como Ponto de Acesso WiFi e Web Server ocultos. Portanto, com um *smartphone* ou computador, somente é possível verificar um ponto de acesso vindo do Módulo, caso seja adicionada uma rede com mesmo nome ao qual o Módulo foi atribuído após sua configuração. Ao entrar na rede local do Módulo, o usuário habilitado poderá abrir uma página em um navegador qualquer, controlar a fechadura magnética da porta e efetuar as devidas medidas de manutenção do sistema, conforme as Figuras 25 e 26.

Figura 25 – Login.



Fonte: O autor.

Figura 26 – Controle do Sistema.

Fonte: O autor.

3.2.4 O Aplicativo iTAG

Conforme apresentado no tópico 2.2 sobre a tecnologia NFC e especificamente no tópico 2.2.3 sobre o funcionamento em dispositivos Android, uma das principais propostas deste trabalho foi desenvolver um aplicativo no *smartphone* capaz de se comunicar via NFC com o Módulo RFID/NFC, cuja principal funcionalidade é a Emulação de Cartão aplicada ao sistema de controle de acesso desenvolvido neste trabalho. Portanto, torna-se possível ter acesso à estabelecimentos com um simples *smartphone* Android devidamente configurado.

Desta forma foi desenvolvido pelo autor através do *software* Android Studio um aplicativo, conforme a Figura 27.

Figura 27 – Aplicativo iTAG.

Fonte: O autor.

Funcionamento do iTAG:

1) Ao aproximar o smartphone com o aplicativo instalado. O leitor NFC detecta a presença de um dispositivo e envia uma solicitação de informação ao serviço HCE hospedado no smartphone, através do APDU pré-definidos.

2) Caso APDU seja validado pelo smartphone, então o mesmo disponibilizará a senha armazenada pelo usuário no aplicativo para o leitor NFC.

3) Ao receber a senha (neste projeto foi adotada a senha como a própria identificação da etiqueta do usuário) disponibilizada pelo smartphone, o Módulo verificará se a mesma é válida.

4) Caso a senha seja válida, a porta será liberada e o Módulo envia uma notificação contendo a hora e data do acesso. Caso não ocorra a liberação, o sistema permanecerá bloqueado e o Módulo envia uma notificação ao dispositivo negando o acesso.

3.2.5 Firmware Mosquitto

Para permitir a comunicação via rede entre o Módulo RFID/NFC e o servidor, o *software* Mosquitto foi definido como broker do Sistema MQTT. Livre, leve e de fácil manuseio, este broker foi hospedado na mesma máquina onde foi hospedado os serviços de Banco de Dados MySQL e Node-Red, utilizados neste projeto (MOSQUITTO, 2019).

A Figura 28 mostra a topologia criada para a comunicação entre o Módulo e o servidor através de tópicos.

O servidor recebe informações do Módulo pelos tópicos, ou seja, está subscrito nos tópicos:

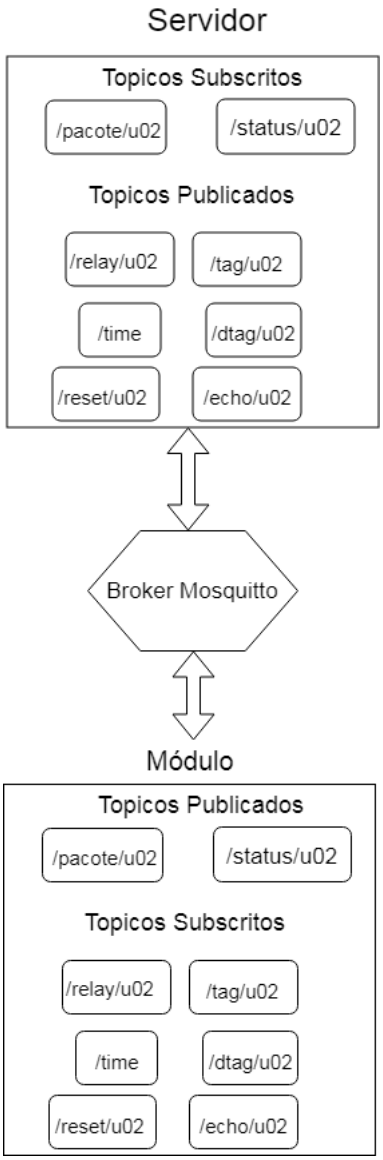
- /pacote/u02 - Através deste tópico o servidor recebe todos os dados necessários para o registro de qualquer movimentação no Módulo.
- /status/u02 - Recebe a situação atual da porta, se está aberta ou fechada.

O servidor envia informações ao Módulo pelos tópicos, ou seja, publica através dos tópicos:

- /relay/u02 - Através deste tópico, o servidor envia comando de habilitar a porta por 2 segundos.
- /time - Envia para o Módulo a data e hora atual, para a atualização do RTC no Módulo.
- /reset/u02 - Envia para o Módulo o comando de reinicializá-lo.
- /tag/u02 - Envia para o Módulo a respectiva UID da etiqueta ao qual se deseja validar no sistema.
- /dtag/u02 - Envia para o Módulo a respectiva UID da etiqueta ao qual se deseja excluir do sistema.
- /echo/u02 - Através deste tópico, o servidor reenvia o mesmo pacote de dados que ele recebeu do tópico “/pacote/u02”, como uma certificação que o pacote chegou ao servidor sem erros.

Todos os tópicos subscritos pelo servidor se torna tópicos de publicação no Módulo e todos os tópicos de publicação do servidor se torna tópicos subscritos pelo Módulo, conforme a Figura 28.

Figura 28 – Comunicação MQTT entre o Servidor e Módulo RFID/NFC.



Fonte: O autor.

3.2.6 Banco de Dados MySQL

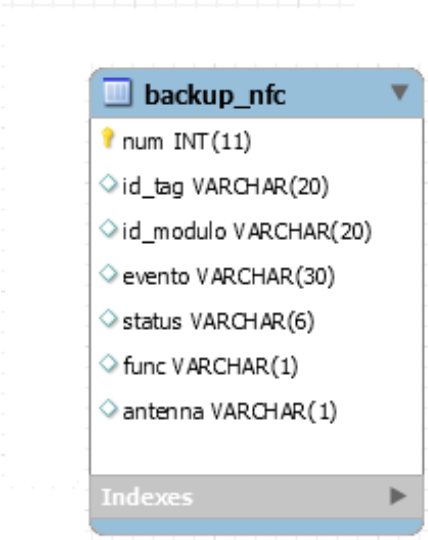
Para a hospedagem do serviço de Banco de Dados MySQL no servidor, foi instalado o programa XAMPP. Um servidor independente de plataforma, *software* livre, que consiste principalmente da base de dados MySQL. Embora tenha vários outros recursos para servidores, somente o Banco de Dados foi utilizado para armazenamento das informações coletadas pelo Sistema de Controle de Acesso (XAMPP, 2019).

Tabela "backup_nfc" - Ilustrada na Figura 29, refere a todos os registros de movimentação, cadastros, exclusão de cadastros ,etc. do Módulo LIH_NFC_U02.

- id_tag = etiqueta do Usuário

- id_modulo = Identificação do Modulo.
- evento = Tempo em que ocorreu o registro.
- status = Situação daquele evento.
- func = Função que mostra o que foi executado no sistema.
- antenna = Antena pela qual o usuário passou a etiqueta.

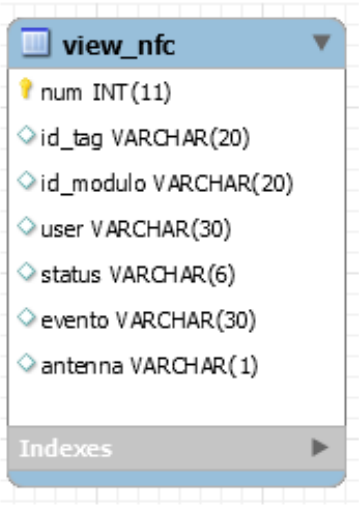
Figura 29 – Tabela "backup_nfc".



Fonte: O autor.

Tabela "view_nfc" - Ilustrada na Figura 30, refere a todas as etiquetas cadastradas no Módulo LIH_NFC_U02. Mostra apenas a última movimentação do indivíduo naquele Módulo. É semelhante a estrutura da tabela de backup descrita na Figura 25, mas com o acréscimo do tópico "user", onde é associado o nome do usuário à sua respectiva etiqueta.

Figura 30 – Tabela “view_nfc”.



Fonte: O autor.

3.2.7 Software NODE-RED

Software NODE-RED é uma ferramenta em programação gráfica com base em JavaScript, foi responsável pelo processamento de dados que chega do broker Mosquitto, construção da interface gráfica para exibição dos registros e comunicação com o Banco de Dados MySQL. Em resumo, através desta ferramenta foi possível realizar o armazenamento dos dados recebidos pelo servidor e a construção da interface de tela para exibição das informações adquiridas por todo sistema (NODE-RED, 2019). Assim que o NODE-RED se conecta com o broker Mosquitto, a própria máquina onde está hospedado o serviço de Banco de Dados MySQL e o Broker Mosquitto, torna-se cliente do broker no Sistema MQTT o que permite a comunicação com outros dispositivos conectados ao broker como o Módulo RFID/NFC.

I) *Rotina de comunicação*

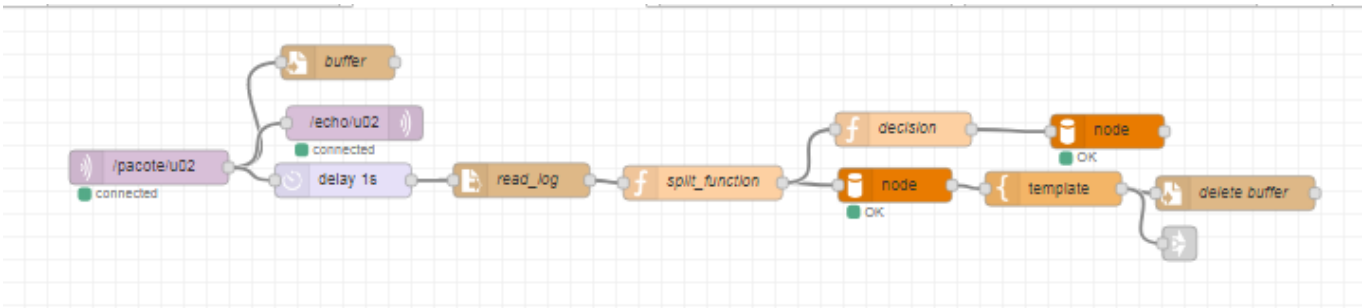
Em um registro realizado pelo Módulo RFID/NFC, há diversas informações que devem ser transmitidas dentro de uma mensagem para o broker (via protocolo MQTT) e armazenadas no banco de dados alocados no servidor. Para isso foi estruturado uma rotina responsável por enviar todas as informações necessárias de um registro através do pacote de dados.

Neste tópico é ilustrado a rotina de processamento dos pacotes de dados enviados pelo Módulo RFID/NFC e recebido pelo servidor.

O fluxo da Figura 31 é responsável por:

- Receber os pacotes de dados através do tópico “/pacote/u02”.
- Posteriormente o mesmo pacote é reenviado para o tópico “/echo/u02” (enviado para o Módulo) com o propósito de confirmar o recebimento do pacote, sem erros, pelo servidor.
- Logo em seguida, o servidor armazena todos os pacotes e realiza as devidas funções no banco de dados (INSERT, UPDATE ou DELETE em SQL).

Figura 31 – Fluxo de armazenamento e decisão do pacote de dados.



Fonte: O autor.

O pacote de dados recebido pelo servidor se divide em 6 elementos:

1 – Nome do Modulo (id_modulo)

2 – Nome da etiqueta (id_tag)

3 – Data e hora (evento)

4 – Situação atual da etiqueta (status)

5 – Função a ser executado no sistema (func)

6 – Indica qual Leitor detectou a etiqueta (antenna)

Onde cada um dos componentes é separado por um delimitador “,” (vírgula) e a separação de cada pacote é separado por um “;” (ponto e vírgula).

Exemplo de template do pacote:

id_modulo,id_tag,evento,status,func,antenna;

Exemplo de pacote:

LIH_NFC_U02,E3A7D8,2018-12-07 10:37:50,0,u,1;

id_modulo - Identificação do Módulo.

id_tag - Identificação única da etiqueta de cada usuário.

evento - Data e hora do evento em que ocorreu aquele registro no formato:

AAAA-MM-DD HH:MM:SS

O mesmo formato é utilizado pelo MySQL, para facilitar a manipulação dos registros no Banco de dados.

status - Indica a situação atual do usuário, podendo assumir até 7 valores:

- 1 - Caso o usuário tenha passado o cartão na antena externa ao setor, subintenderá que o usuário pretende entrar do setor, logo status = 1.
- 0 - Caso o usuário tenha passado o cartão na antena interna ao setor, subintenderá que o usuário pretende sair do setor, logo status = 0.
- ON – Indicador que a função de Cadastro ou Exclusão de Cadastro começou. As próximas etiquetas registradas a partir deste ON serão cadastrados ou excluídas do sistema.
- OFF - Indicador que a função de Cadastro ou Exclusão de Cadastro terminou.
- NEW – Indicador que a etiqueta foi recém cadastrada.
- DEL – Indicador que a etiqueta foi recém excluída.
- CLC – Indicador que todos os registros da memória interna do Módulo foram apagadas, ou seja, nenhuma etiqueta está habilitada no sistema.

func: Variável tipo carácter que indicará qual função o sistema executará no Banco de dados.

- “u” – Carácter responsável por realizar a função UPDATE, em SQL, na Tabela de Usuários do Módulo no Banco de Dados.
- “d” – Carácter responsável por realizar a função DELETE, em SQL, na Tabela de usuários do Modulo no Banco de Dados.
- “i” - Carácter responsável por realizar a função INSERT, em SQL. Ou seja, cadastro de novos usuários na Tabela de Registros do Módulo no Banco de Dados.
- “c” – Carácter responsável por realizar a função DELETE FROM TABLE, em SQL. Ou seja, excluir todos os usuários da Tabela de Registros do Modulo no Banco de Dados.

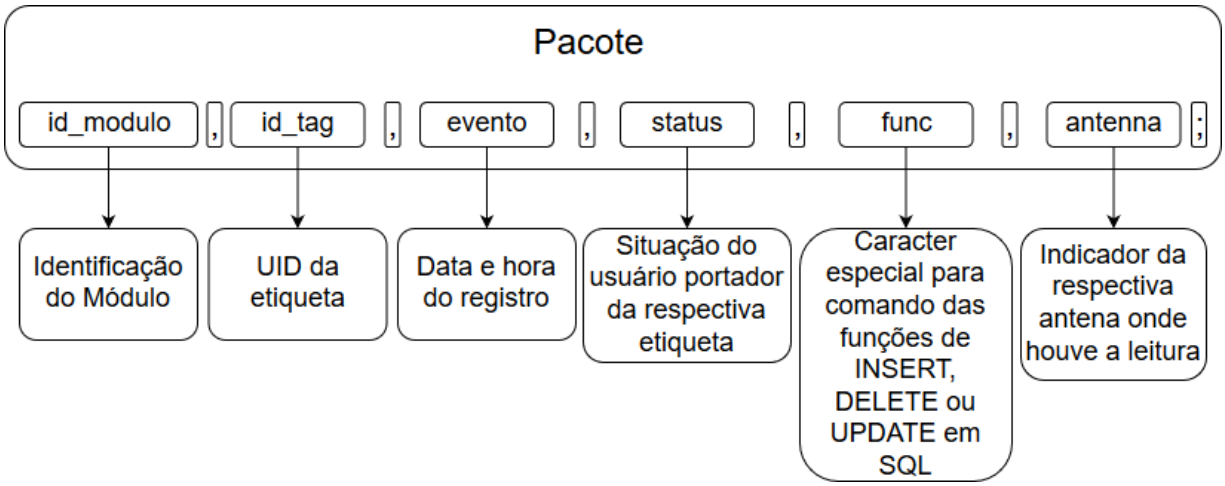
- “b” – Carácter responsável por realizar a função INSERT, em SQL. Apenas insere qualquer movimentação registrada pelo Módulo na Tabela Backup no Banco de dados.

antenna - Indica qual antena detectou a etiqueta. Assume apenas dois valores (0 ou 1).

- Caso o usuário tenha passado o cartão na antena interna ao setor, então *antenna* = 1.
- Caso o usuário tenha passado o cartão na antena externa ao setor, então *antenna* = 0.

A estrutura do pacote contém todos os dados necessários para a interpretação e processamento desses dados pelo servidor. A Figura 32 ilustra de forma resumida os elementos presentes no pacote de dados.

Figura 32 – Estrutura do pacote de dados.



Fonte: O autor.

II) *Rotina da Interface do Supervisório*

Para um supervisor ter acesso aos registros de maneira rápida e simples, realizar busca de registro, cadastro ou exclusão de cadastro no sistema e controle do Módulo RFID/NFC de forma remota, foi necessário a construção de rotinas que proporcionem tais funções.

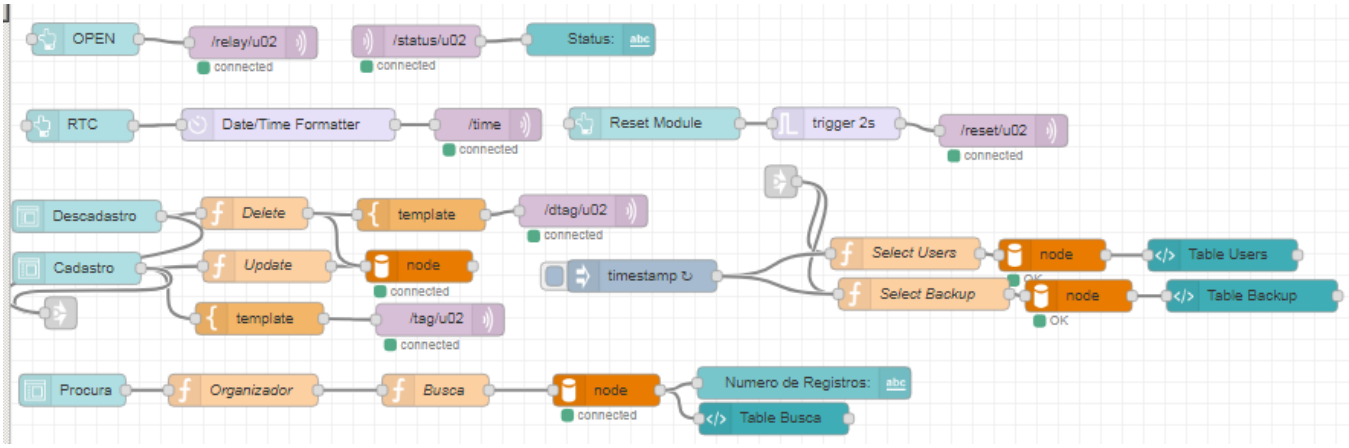
Neste tópico é ilustrado o funcionamento das rotinas disponíveis na interface gráfica do sistema.

Os fluxos da Figura 33, são responsáveis por:

- O primeiro fluxo iniciado por “OPEN”, é responsável por criar a interface de um botão no supervisório e enviar um comando para o tópico MQTT “/relay/u02”. Consequentemente, o Módulo recebe um comando através deste tópico e libera a porta por 2 segundos.
- O fluxo seguinte, iniciado pelo tópico MQTT “/status/u02”, é responsável por receber as mensagens enviadas pelo Módulo e exibir na interface do supervisório.
- O fluxo iniciado por “RTC” é responsável por criar a interface de um botão no supervisório e enviar a data e hora para o tópico MQTT “/time”. Tem o propósito de atualizar o RTC do Módulo.
- O fluxo iniciado por “Reset Module” é responsável por criar a interface de um botão no supervisório e enviar um comando para o tópico MQTT “/reset/u02”. Com o proposito de reiniciar Módulo.
- O fluxo iniciado por “Descadastro”, é responsável por criar um campo na interface do supervisório para a exclusão da respectiva etiqueta no sistema de banco de dados, logo em seguida o software Node-Red envia a UID da etiqueta para o tópico MQTT “/dtag/u02”. Assim que o Módulo recebe a UID através deste tópico, subentende-se que a respectiva etiqueta foi deletada do sistema e bloqueia o acesso desta.
- O fluxo iniciado por “Cadastro” é responsável por criar um campo na interface do supervisório para validação da respectiva etiqueta no sistema de banco de dados, logo em seguida o software Node-Red envia a UID da etiqueta para o tópico MQTT “/tag/u02”. Assim que o Módulo recebe a UID através deste tópico, subentendi que a respectiva etiqueta foi validada no sistema e habilita o acesso desta.
- O fluxo iniciado por “Procura” é responsável por criar um campo na interface do supervisório para o sistema de busca no banco de dados, de acordo com datas e/ou respectiva etiqueta que o supervisor deseja procurar. Exibi-se assim todos os resultados de acordo com os parâmetros que o supervisor definiu anteriormente.
- O fluxo iniciado por “timestamp” é responsável por atualizar constantemente a lista de registros e usuários. As funções de SELECT em SQL são acionadas

para busca e, logo em seguida, exibe na interface do supervisório os registros e usuários cadastrados no sistema de banco de dados.

Figura 33 – Fluxos de Interface do Supervisório.



Fonte: O autor.

III) *Interface gráfica do Supervisório*

Abaixo são ilustrados todos os tópicos existentes no Supervisório para a interação do usuário com o sistema de registros (posteriormente ilustrado nas Figuras 37, 38 e 39 no Capítulo 4).

- **Login**: Digitar Usuário e Senha válidos. Após a inserção de Usuário e Senha válidos, é apresentado um relatório rápido dos registros feitos pelo respectivo Módulo.
- **Backup_U02**: Exibe os últimos 20 registros do Módulo (Index,User,ID Tag, Data/Hora, Status).
- **U02**: Exibe todas as etiquetas, usuários registrados e situação atual do mesmo (User, ID Tag, Data/Hora, Status). Etiquetas registradas, seus respectivos usuários, data e hora do último registro feito pelo usuário e seu *status*, se está dentro ou fora do respectivo setor (Zero 0 – Significa fora do Setor e Um 1 – Significa dentro do Setor) e a antena cujo o usuário passou o cartão (Zero 0 – Significa que o Leitor RFID do lado de fora do Setor detectou a etiqueta e Um 1 – Significa o Leitor do lado de dentro do Setor).

- **Config_U02**: Abre a porta remotamente.
- **Status**: Situação atual da Porta (Aberta ou Fechada).
- **Update**: Atualiza o Relógio RTC na data e hora atual.
- **Reset Module**: Comando para o respectivo módulo reiniciar.
- **Procura_U02**: Faz uma busca com campos de data, hora e a etiqueta a ser procurada a partir da respectiva data definida no campo anterior. A partir de uma determinada Data e Hora (campo obrigatório), até determinada Data e Hora (caso deixe em branco o sistema buscará a partir da data e hora obrigatoriamente determinada acima até a data e hora atual) e a respectiva etiqueta a ser buscada (caso deixe em branco, selecionará todas as etiquetas naquele determinado tempo).
- **Update/Cadastro**: Responsável por Inserir ou Atualizar o nome do Usuário com a respectiva etiqueta.

Obs: Após o cadastro manual da etiqueta no Módulo, através do cartão especial MAC, o Supervisor deve terminar o cadastro através desta página no Supervisório para validar a etiqueta que está armazenada no Módulo. Inserindo assim o Nome do usuário e a respectiva etiqueta que foi cadastrada manualmente.

- **Descadastro**: Exclui o cadastro da respectiva etiqueta do sistema do Banco de Dados e do Modulo.
- **Logout**: Voltar para tela de login.

4 RESULTADOS E DISCUSSÃO

Todo o sistema foi testado e validado no Laboratório de Interface Homem-Maquima (LIHOM) - UFPE, no departamento de Engenharia Eletrônica (DES).

Para a realização dos testes de validação, todas as pessoas que frequentam o laboratório (professores, alunos de IC's e pós-graduandos) receberam etiquetas tipo cartão RFID e os que possuem *smartphone* Android com NFC tiveram acesso ao aplicativo iTAG. Por fim, puderam entrar ou sair do estabelecimento regularmente após o devidos procedimentos de cadastro no sistema.

4.1 Laboratório de Interface Homem-Máquina - LIHOM

A Figura 34 ilustra o local onde o Módulo RFID/NFC (sinalizado em vermelho) foi instalado e realizado os testes. Onde todos os estudantes e professores habilitados com etiqueta RFID, tipo cartão, ou aplicativo iTAG devidamente configurados, tiveram acesso ao laboratório.

Figura 34 – Porta de acesso ao LIHOM.

Fonte: O autor.

A Figura 35 ilustra o involucro localizado na parte externa do laboratório, feito

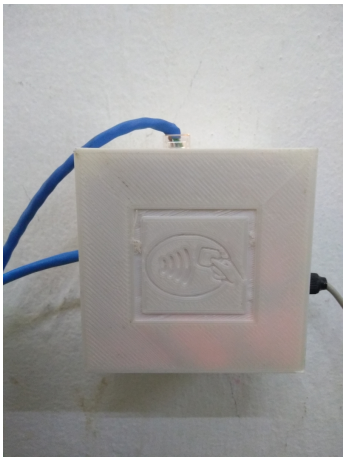
em impressão 3D, cujo leitor RFID/NFC se encontra dentro do involucro. O botão vermelho serve como campainha. Assim que apertado, o *buzzer* será acionado na parte de dentro do laboratório.

Figura 35 – Leitor RFID/NFC, parte externa ao LIHOM.

Fonte: O autor.

A Figura 36 ilustra o invólucro feito em impressão 3D, cujo leitor RFID/NFC, RTC DS3231, *buzzer* e a placa de desenvolvimento se encontram dentro, cujo cabo à direita do Módulo é responsável pela alimentação 5V, o cabo tipo RJ45 acima é responsável pela comunicação Ethernet e o cabo RJ45 à esquerda é responsável pela ligação entre o Módulo RFID/NFC (localizado na parte interna do laboratório) e o Leitor RFID/NFC (localizado na parte externa do laboratório).

Figura 36 – Módulo RFID/NFC, parte interna ao LIHOM.



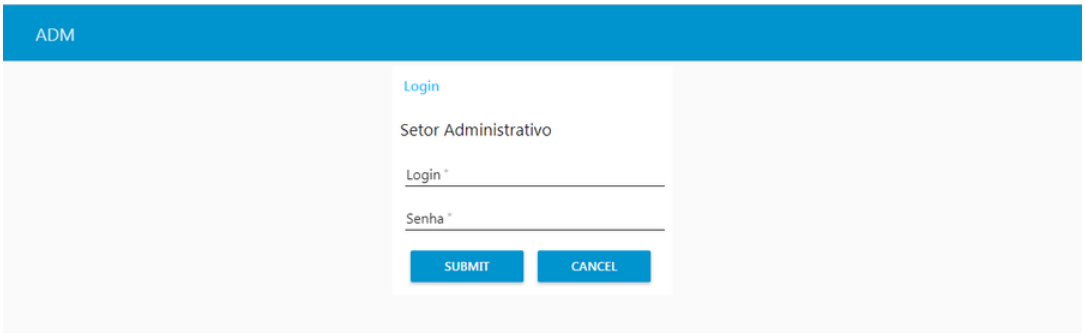
Fonte: O autor.

4.2 Supervisório

Com o auxílio das ferramentas que o *software* NODE-RED disponibiliza, foi desenvolvida uma interface amigável e segura para o acompanhamento em tempo real dos registros feitos pelo Módulo. Registros de todas as entradas e saídas, rotinas de procura, configuração do Módulo,etc, foram alocados em um servidor no laboratório. Com esta interface é possível analisar todos os registros efetuados pelo Módulo e também controlá-lo remotamente dentro da rede interna.

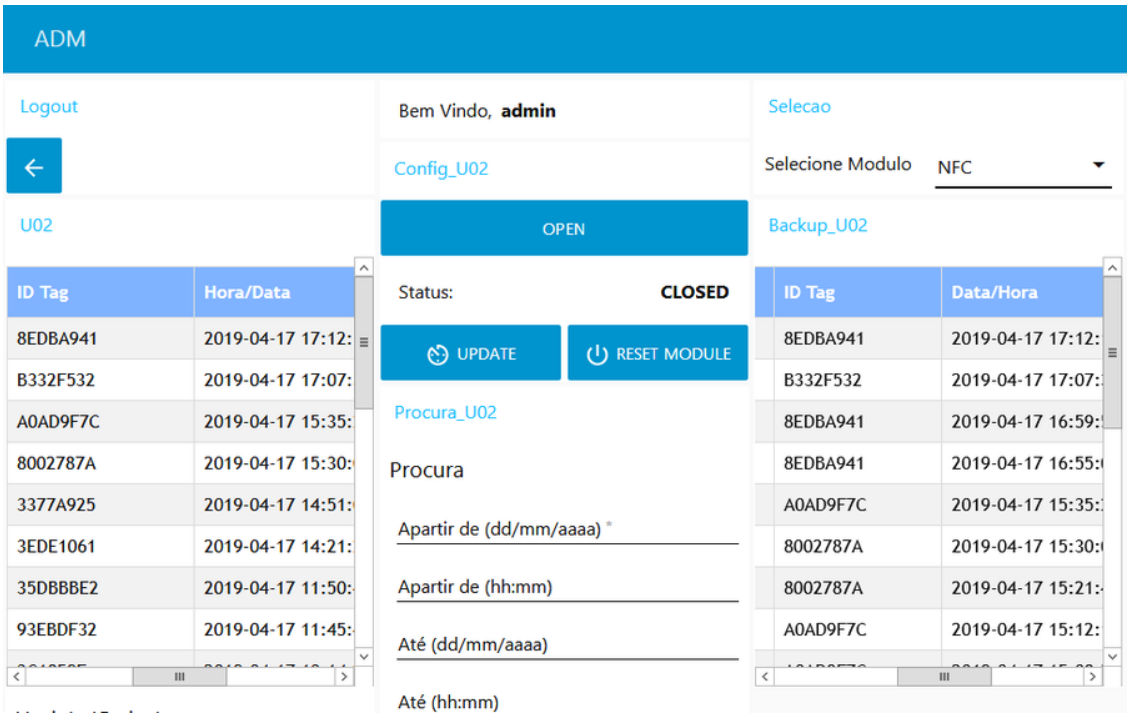
Ao acessar o endereço IP do servidor na porta 1880, por exemplo http://192.168.0.2:1880/ui, conforme a Figura 37, será exibido o login do setor administrativo. Após a inserção de login e senha válidos, será exibida a tela ilustrada nas Figuras 38 e 39.

Figura 37 – Login do Supervisório.



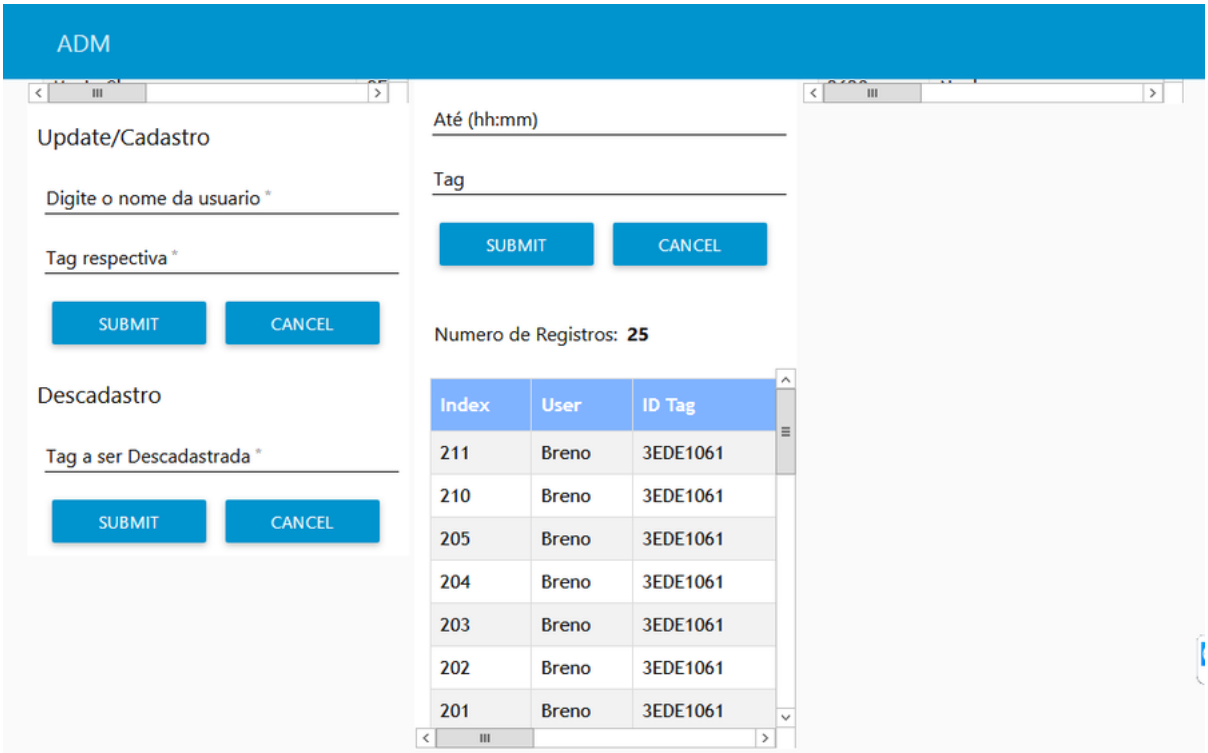
Fonte: O autor.

Figura 38 – Tela do Supervisório - Parte 1.



Fonte: O autor.

Figura 39 – Tela do Supervisório - Parte 2.



Fonte: O autor.

Os resultados obtidos foram satisfatórios para a validação deste projeto. Mais de 2000 registros foram coletados e analisados constantemente, conforme a Figura 40. Onde são ilustrados os últimos registros armazenados no sistema até o dia 30/05/2019.

- Index: Índice do registro.
- User: Nome do usuário.
- ID Tag: Respectiva identificação da etiqueta do usuário.
- Data/Hora: Momento em que o registro foi feito.
- Status: Suposta situação do usuário. “1” significa que o usuário supostamente está dentro do estabelecimento e “0” significa que o usuário supostamente está fora do estabelecimento.

Figura 40 – Últimos registros feito no dia 30/05/2019.

Backup_U02

Index	User	ID Tag	Data/Hora	Status
2631	Aline	50C0F979	2019-05-30 22:16:44	1
2630	Aline	50C0F979	2019-05-30 22:16:14	0
2629	Euller Lima	93EBDF32	2019-05-30 20:54:35	0
2628	Aline	50C0F979	2019-05-30 19:04:54	1
2627	Ana Morais	4EFC4D5D	2019-05-30 17:48:42	0
2626	João Vicente	B332F532	2019-05-30 16:39:11	0
2625	Euller Lima	93EBDF32	2019-05-30 16:38:39	1
2624	Ana Morais	4EFC4D5D	2019-05-30 16:01:05	1

Fonte: O autor.

Tendo como meta o controle em tempo real de acessos, o sistema implementado possui algumas limitações:

- O usuário, ao abrir a porta utilizando sua etiqueta, caso desista de entrar ou sair do setor fará com que o sistema considere que ele realmente planejara entrar ou sair do setor. Por exemplo, a pessoa libera a porta pelo lado de dentro do setor, o sistema atualizará que ele estará em breve fora do setor ou vice-versa.
- Caso a pessoa libere a porta pelo lado de dentro ou lado de fora, não há controle de fluxo de pessoas. Ou seja, entre o tempo da porta aberta e porta fechada, o sistema ficará “cego”, pois, não terá como saber quem entrou ou saiu neste intervalo. Apenas o registro da pessoa que passou a etiqueta ficará salvo.

Uma possível solução seria a implementação de outro sistema em conjunto, para maior segurança ao processo, como por exemplo, sistemas a laser infravermelho que detecte o sentido de movimentação do indivíduo ou a utilização de leitores RFID UHF de longa distância que detecte a presença usuários portadores de etiquetas RFID.

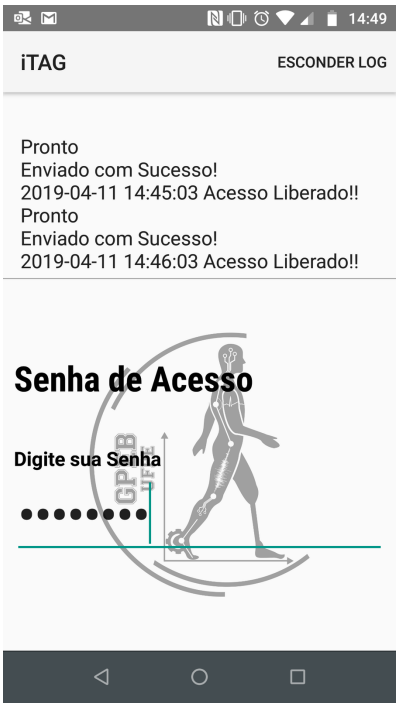
Como o foco deste trabalho não é o estudo de banco de dados, o sistema foi feito de forma simples, eficaz para o problema de armazenamento, controle e exibição dos registros feitos pelo Módulo remotamente e em tempo real.

4.3 Aplicativo iTAG

As Figura 41 e 42 demonstram a utilização do aplicativo iTAG, onde foi aproximado contra o Módulo RFID/NFC um celular habilitado com tecnologia NFC.

A Figura 41 abaixo, mostra um exemplo, ao qual foi inserido a identificação de uma etiqueta habilitada pelo sistema e a notificação na tela do *smartphone* “2019-06-11 14:46:03 Acesso Liberado!!”, liberando o acesso ao laboratório.

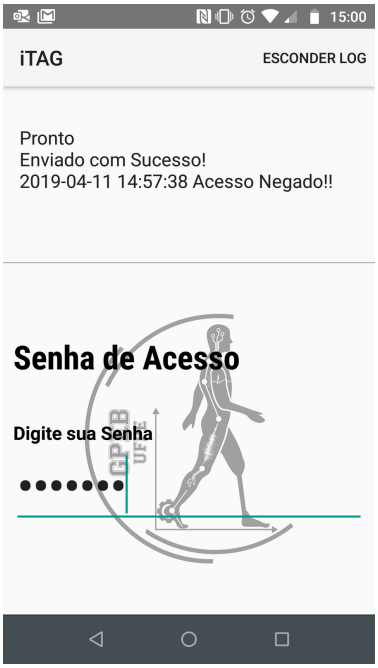
Figura 41 – Utilização do iTAG: Acesso Liberado.



Fonte: O autor.

A Figura 42 ilustra o resultado obtido pelo aplicativo após a inserção de uma senha inválida pelo Módulo RFID/NFC. O Módulo nega o acesso do usuário emitindo uma mensagem via NFC para o *smartphone* “2019-06-11 14:57:38 Acesso Negado!!”.

Figura 42 – Utilização do iTAG: Acesso Negado.



Fonte: O autor.

4.4 Aplicações futuras

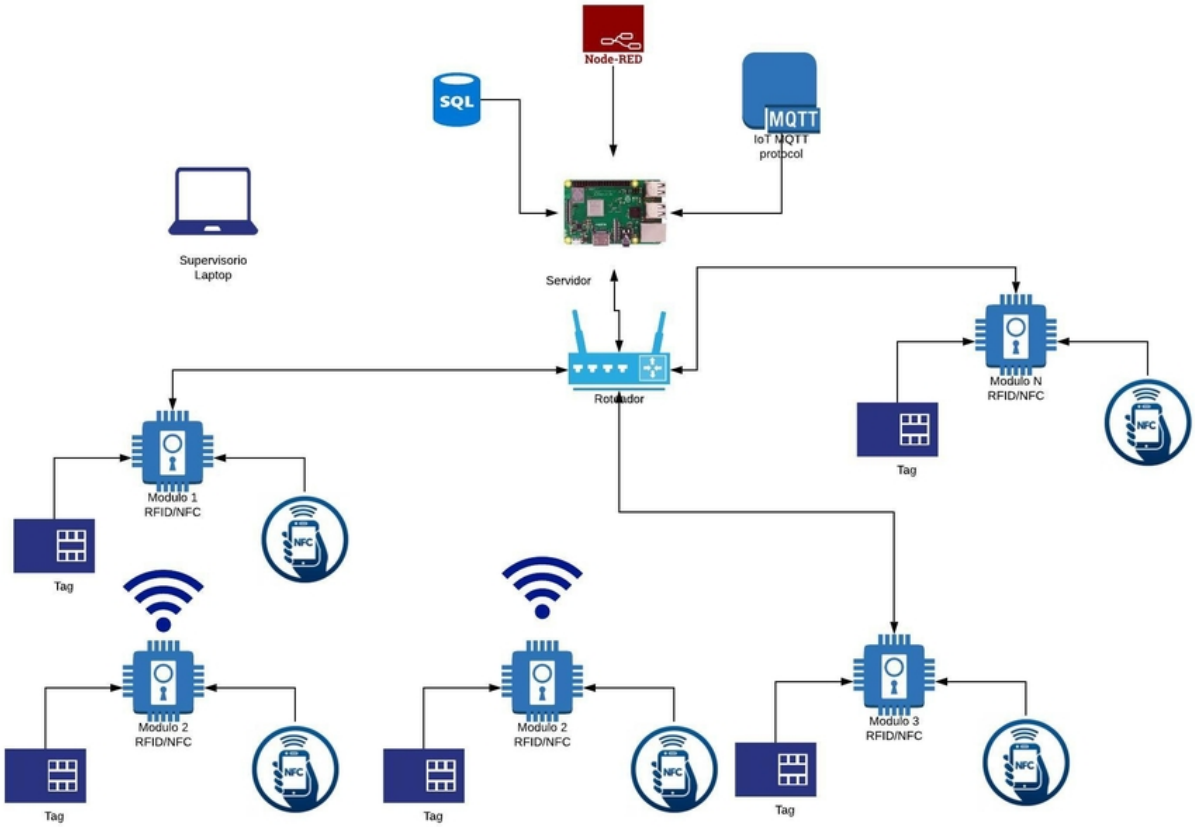
1) O mesmo sistema criado (ilustrado na Figura 28) pode ser expandida para mais Módulos (ilustrado na Figura 43) conectados a um mesmo servidor. É necessário apenas inserir mais tópicos e fluxos de tratamentos dos dados no *software* NODE-RED.

2) Outra possibilidade bem interessante é que os mesmos serviços e *softwares* utilizados neste trabalho podem ser executados em computadores de placa única ou *Single Board Computer* (SBC). Um exemplo clássico é uma Raspberry Pi, conforme a Figura 43. Isso torna o projeto mais simples e barato.

3) O desenvolvedor pode expandir sua rede interna para rede externa. Ultimamente existem vários Brokers MQTT na Internet , alguns livres e outros pagos. Isto torna possível a comunicação entre servidor e cliente através da Internet.

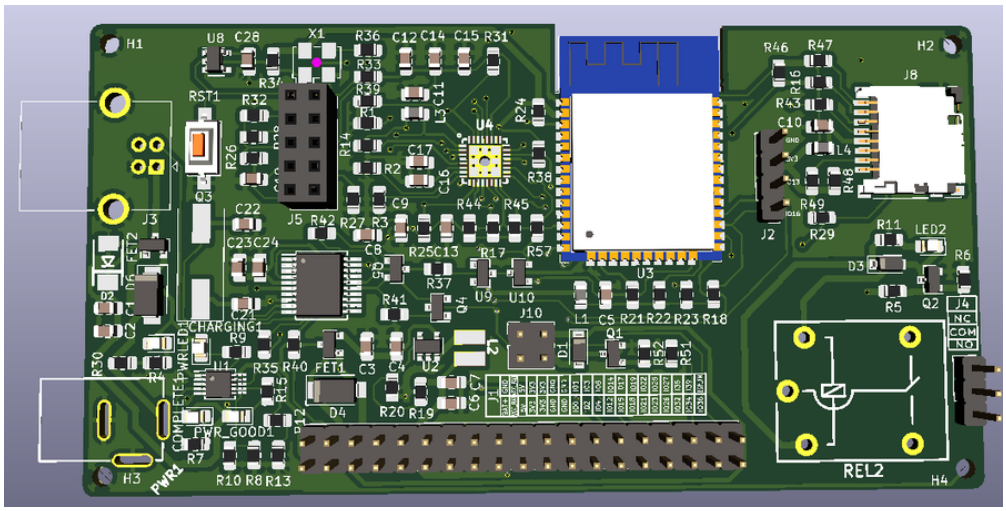
4) Como a placa de desenvolvimento OLIMEX ESP32-EVB possui vários periféricos não utilizados no sistema de controle de acesso, o desenvolvimento de uma placa dedicada foi posto em prática para apenas atender as funcionalidades do sistema de controle de acesso construído, conforme a Figura 44.

Figura 43 – Rede com múltiplos módulos de controle de acesso.



Fonte: O autor.

Figura 44 – Placa PCB em desenvolvimento.



Fonte: O autor.

5 CONCLUSÃO

Neste trabalho foi construído um sistema para controlar o acesso de um estabelecimento remotamente e em tempo real. O sistema disponibiliza opções variadas de comunicação dos Módulos, seja via cabo (Ethernet) ou *wireless* (WiFi). Este projeto pode impactar positivamente o planejamento da infraestrutura, montagem do sistema e alocação de Módulos através da integração de tecnologias como RFID e NFC para o controle de acesso.

Um fator relevante para o sistema desenvolvido é a possibilidade de aplicação da tecnologia NFC presente em diversos *smartphones* atuais. Isso torna o acesso mais conveniente aos usuários e cria uma nova possibilidade de acesso ao sistema. Pode-se trazer mais comodidade ao usuário que utiliza seu *smartphone* ao invés de um cartão ou reduzir o custo do sistema sem a necessidade de utilização de etiquetas RFID. Para isso, tornou-se necessário a construção de um aplicativo dedicado ao sistema implementado, o iTAG, desenvolvido pelo autor deste trabalho. Este aplicativo permite que o *smartphone* se comporte como um *smart card*, viabilizando a comunicação entre o dispositivo e o Módulo RFID/NFC.

Através da análise dos resultados apresentados e avaliados no capítulo 4, este tipo de sistema se apresentou promissor no que diz respeito a outros sistemas de controle de acesso existentes no mercado, pois, permite o monitoramento de indivíduos em tempo real de um estabelecimento, controle do Módulo RFID/NFC de forma remota e por fim a integralização de duas tecnologias vigentes no mercado, o RFID e NFC, em apenas um Módulo.

Como demostrado no tópico 4.3, a topologia do servidor desenvolvido no presente trabalho pode ser embarcada em um SBC com múltiplos Módulos, devido à compatibilidade dos *softwares* utilizados, tornando o sistema de controle simples e barato de ser produzido. Por fim, a construção de uma placa em PCB dedicada ao sistema de controle de acesso torna este projeto tangível às necessidades do mercado no que diz respeito ao valor comercial de todo o sistema, desde a construção dos *hardwares* aos *softwares* utilizados.

REFERÊNCIAS

BACIOCCOLA, A. **NFC Forum**. 2019. Fórum. Disponível em: https://nfc-forum.org/our-work/specifications-and-application-documents/application-documents/. Acesso em: 22/05/2019.

BASYARI, R. S.; NASUTION, S. M.; DIRGANTARA, B. Implementation of Host Card Emulation Mode Over Android Smartphone as Alternative ISO 14443A for Arduino NFC Shield. **2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)**, p. 160 – 165, 2015.

CHABANNE, H.; URIEN, P.; SUSINI, J. (ed.). **RFID and the Internet of Things**. [S.l.]: Wiley, 2011.

COSKUN, V.; OK, K.; OZDENIZCI, B. **NEAR FIELD COMMUNICATION**: FROM THEORY TO PRACTICE. 1. ed. [S.l.]: Wiley, 2012.

CUNHA, A. **RFID – Etiquetas com eletrônica de ponta**. 2016. Fórum. Disponível em: https://www.embarcados.com.br/rfid-etiquetas-com-eletronica-de-ponta/.

ESP32 Datasheet. 2019. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf. Acesso em: 10/03/2019.

FINKENZELLER, K. **RFID Handbook**: Fundamentals and Applications in contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. 3. ed. [S.l.]: Wiley, 2010.

HILLAR, G. C. **MQTT Essentials**: A Lightweight IoT Protocol. 1. ed. [S.l.]: Packt Publishing Ltd., 04/2017.

IGOE, T.; COLEMAN, D.; JEPSON, B. **Beginning NFC**: Near Field Communication with Arduino, Android & PhoneGap. 1. ed. [S.l.]: O'Reilly, 2014/01.

MOSQUITTO. 2019. Disponível em: https://mosquitto.org. Acesso em: 01/12/2018.

NODE-RED. 2019. Disponível em: https://nodered.org. Acesso em: 01/12/2018.

OLIMEX ESP32 - EVB. 2017. Shop Online. Disponível em: https://www.olimex.com/Products/IoT/ESP32/ESP32-EVB/open-source-hardware. Acesso em: 01/12/2018.

WEI, M. **Developing Android* Business Apps Using NFC Host-based Card Emulation Capabilities**. 09/2014. Disponível em: https://software.intel.com/en-us/articles/developing-android-business-apps-using-nfc-host-based-card-emulation-capabilities. Acesso em: 22/05/2019.

XAMPP. 2019. Disponível em: https://www.apachefriends.org/pt_br/index.html. Acesso em: 01/03/2018.

YUAN, M. **Conhecendo o MQTT**. 2017/04. Disponível em: https://www.ibm.com/developerworks/br/library/iot-mqtt-why-good-for-iot/index.html. Acesso em: 07/04/2019.