UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ENGENHARIA ELETRÔNICA

LUIZ FELIPE KIM EVARISTO
TAUAN MARINHO
TIAGO HENRIQUE FAXINA
TIAGO MARIANI PALTE

SISTEMA DE CONTROLE DE ACESSO BASEADO EM RECONHECIMENTO DE SENHA FALADA

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2018

LUIZ FELIPE KIM EVARISTO
TAUAN MARINHO
TIAGO HENRIQUE FAXINA
TIAGO MARIANI PALTE

SISTEMA DE CONTROLE DE ACESSO BASEADO EM RECONHECIMENTO DE SENHA FALADA

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

Orientador: Prof. Dr. Bruno Sens Chang
UTFPR

CURITIBA
2018

LUIZ FELIPE KIM EVARISTO
TAUAN MARINHO
TIAGO HENRIQUE FAXINA
TIAGO MARIANI PALTE

SISTEMA DE CONTROLE DE ACESSO BASEADO EM RECONHECIMENTO DE SENHA FALADA

Este Trabalho de Conclusão de Curso de Graduação foi apresentado como requisito parcial para obtenção do título de Engenheiro Eletrônico, do curso de Engenharia Eletrônica do Departamento Acadêmico de Eletrônica (DAELN) outorgado pela Universidade Tecnológica Federal do Paraná (UTFPR). Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Curitiba, 18 de Junho de 2018.

Prof. Dr. Robinson Vida Noronha
Coordenador de Curso
Engenharia Eletrônica

Profª Drª Carmem Caroline Rasera
Responsável pelos Trabalhos de Conclusão de Curso
de Engenharia Eletrônica do DAELN

BANCA EXAMINADORA

Prof. Dr. Bruno Sens Chang
UTFPR
Orientador

Prof. PhD. João Luiz Rebelatto
UTFPR

Prof. MSc. Ricardo Umbria Pedroni
UTFPR

A folha de aprovação assinada encontra-se na Coordenação de Curso de Engenharia Eletrônica.

AGRADECIMENTOS

Aos professores do curso de Engenharia Eletrônica, por seu incansável desejo de disseminar o conhecimento e expô-lo à nós de maneira admirável.

Ao Prof. Bruno Sens Chang, nosso orientador, por sua paciência e disposição em nos auxiliar durante a realização do projeto, sempre nos motivando e nos mantendo no caminho.

Aos nossos familiares, amigos e colegas por todo o apoio e motivação dados durante o difícil processo que é o desenvolvimento de um trabalho de conclusão de curso.

São as perguntas que não sabemos responder que mais no ensinam. Elas nos ensinam a pensar. Se você dá uma resposta a um homem, tudo o que ele ganha é um fato qualquer. Mas se você lhe der uma pergunta, ele procurará suas próprias respostas (. . .)
Assim, quando ele encontrar as respostas, elas lhe serão preciosas. Quanto mais difícil a pergunta, com mais empenho procuramos a resposta. Quanto mais a procuramos, mais aprendemos.
(ROTHFUSS, P., "O Temor do Sábio", 2011).

RESUMO

KIM EVARISTO, L. F.; MARINHO, T.; FAXINA, T. H.; PALTE, T. M.. Sistema de Controle de Acesso Baseado em Reconhecimento de Senha Falada. 2018. 64 f. Trabalho de Conclusão de Curso – Curso de Engenharia Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

O sistema de controle de acesso desenvolvido visa fornecer uma alternativa contemporânea para o segmento de segurança, utilizando a voz como objeto de validação. Dado que é comum a perda de chaves e esquecimento de palavras-chave, o emprego de senhas faladas se mostra uma solução para tal problema. O projeto implementado possui o diferencial de utilizar um algoritmo de correlação de sinais, mais simples e eficiente que os sistemas similares existentes. Além disso, é escalável, pois está conectado a um banco de dados que permite o gerenciamento de diversos acessos e diversos usuários, aumentando a gama de aplicações do sistema.

Palavras-chave: Segurança. Controle de Acesso. Reconhecimento de Senha Falada. Correlação de Sinais. Banco de Dados.

ABSTRACT

KIM EVARISTO, L. F.; MARINHO, T.; FAXINA, T. H.; PALTE, T. M.. Access Control System Based on Voice Password Recognition. 2018. 64 f. Trabalho de Conclusão de Curso – Curso de Engenharia Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The access control system developed in this work aims to provide a contemporary alternative for the security segment, using voice as the validation object. It is common to lose keys or forget passwords, so the usage of spoken phrases presents itself as a solution for these problems. The project has the differential of using a signal correlation algorithm, which is simpler and more efficient than those used by similar existing systems. It is also scalable, since it is connected to a database that allows the management of several accesses and users, providing a large span of applications for the system.

Keywords: Security. Access Control. Voice Password Recognition. Signal Correlation. Database.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADC	*Analogic-Digital Converter* (Conversor Analógico-Digital)
CPU	*Central Processing Unit* (Unidade Central de Processamento)
CSRF	*Cross-Site Request Forgery* (Falsificação de solicitação entre sites)
CSS	*Cascading Style Sheets* (Folhas de Estilos em Cascata)
GPIO	*General Purpose Input/Output* (Entrada/Saída de Propósito Geral)
HTML	*HyperText Markup Language* (Linguagem de Marcação de Hipertexto)
HTTP	*HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto)
IDE	*Integrated Development Environment* (Ambiente Integrado de Desenvolvimento)
ISR	*Interrupt Service Routine* (Rotina de Serviço de Interrupção)
JVM	*Java Virtual Machine* (Máquina Virtual Java)
JWT	*JSON Web Token*
LCD	*Liquid Crystal Display* (Display de Cristal Líquido)
LED	*Light Emitting Diode* (Diodo Emissor de Luz)
PDS	Processamento Digital de Sinais
PLL	*Phase-Locked Loop*
RFID	*Radio-Frequency Identification* (Identificação por Rádio-Frequência)
SPI	*Serial Peripheral Interface* (Interface Serial para Periféricos)
TCP/IP	*Transmission Control Protocol/Internet Protocol* (Protocolo de Controle de Transmissão/Protocolo de Internet)
URL	*Uniform Resource Locator* (Localizador Uniforme de Recursos)
WAV	*WAVEform audio format* (Formato de áudio WAVE)

LISTA DE SÍMBOLOS

A	Ampères (Corrente Elétrica)
B	Bytes
bps	Bits por Segundo
F	Faradays (Capacitância)
Hz	Hertz (Frequência)
sps	Amostras por Segundo
V	Volts (Tensão)
Ω	Ohms (Resistência)

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem como objetivo descrever a metodologia e os procedimentos de desenvolvimento empregados para a construção de um sistema de controle de acesso baseado em reconhecimento de senha falada.

O projeto é construído sobre uma moderna plataforma da Texas Instruments baseada na arquitetura ARM, a Tiva TM4C. O processador desta plataforma atende aos requisitos necessários para o correto e eficiente funcionamento do sistema. Alguns dos periféricos presentes na plataforma, tais como módulos ADC, Timers, Ethernet e SPI, são utilizados como parte vital do sistema, agregando as funcionalidades propostas e permitindo um eficaz desenvolvimento de todas as partes do sistema.

Como importante aspecto do projeto está a interface com o usuário, construída para tornar o sistema mais amigável. Ainda com o objetivo de suavizar essa interação, todo o sistema é concebido de maneira a facilitar o uso do mesmo, sendo bastante intuitivo e simples, tanto na parte física (hardware) como na parte web (software).

1.1 JUSTIFICATIVA

Com o crescimento da indústria tecnológica, diversos sistemas de segurança foram desenvolvidos e, recentemente, começaram a utilizar características biométricas para realizar autenticação, como impressão digital, íris e também a voz.

Muitos dos sistemas que empregam a chamada biometria de voz utilizam algoritmos bastante complexos, como Redes Neurais Artificiais, Modelos Ocultos de Markov e Misturas Gaussianas, para a validação do sinal de voz de entrada com algum armazenado, o que requer uma plataforma com alto poder computacional. Este tipo de sistema é bastante empregado em bancos, fazendo o reconhecimento através do telefone. Alguns outros sistemas foram desenvolvidos para aplicações comerciais e domésticas, contudo ainda são escassos e não apresentam vantagens significativas.

Um outro quesito que torna os atuais sistemas comerciais não tão vantajosos é a possibilidade de falha, pois muitos utilizam apenas o reconhecimento de palavras no processo de validação, que pode ser facilmente burlado assim como o de uma senha digitada.

A ideia do projeto é simplificar o método de análise, fazendo uso de um algoritmo de correlação de sinais. Somado ao custo computacional reduzido, vem ainda a escalabilidade do sistema, pois o mesmo é conectado a um banco de dados gerenciável. Com isto, pode-se criar uma rede de segurança que compartilha uma mesma base de dados mas que possui particularidades, como definir quais usuários têm acesso à quais áreas.

1.2 ESTRUTURA DO TRABALHO

O trabalho está dividido em 6 capítulos, respectivamente: Introdução, Revisão Bibliográfica, Metodologia, Desenvolvimento, Plano de Negócios e Conclusão.

Primeiramente estão apresentados os objetivos do trabalho e a justificativa, além de introduzir o assunto tratado no trabalho.

No segundo capítulo, Revisão Bibliográfica, um apanhado de trabalhos correlatos já desenvolvidos, bem como bases pertinentes ao projeto aqui descrito são discutidos.

Serão tratados com maior profundidade os procedimentos metodológicos, o embasamento teórico utilizado na formulação dos requisitos e definições do projeto no terceiro capítulo, Metodologia.

Os detalhes da implementação de todas as partes do sistema (hardware, firmware e software), os testes realizados e mudanças efetuadas, bem como o gerenciamento do projeto serão apresentados no quarto capítulo, Desenvolvimento.

No quinto capítulo é exposto o plano de negócios para o projeto implementado, envolvendo todos os aspectos pertinentes ao lançamento do sistema como um produto.

A avaliação dos resultados obtidos, o envolvimento do trabalho com as disciplinas cursadas no decorrer da formação, uma análise geral do projeto e sua relevância são apresentados ao final do texto, no sexto capítulo, Considerações Finais.

2 REVISÃO BIBLIOGRÁFICA

Muitos trabalhos foram desenvolvidos na área de biometria de voz, tema indireto deste trabalho. A maioria leva em conta o reconhecimento de palavras e padrões de voz, utilizando para isso complexos algoritmos de processamento. Existem inclusive, sistemas comerciais utilizados em bancos que fazem a validação do usuário via voz falada ao telefone. Alguns projetos foram considerados na construção do sistema apresentado neste trabalho.

O principal projeto existente na área de segurança residencial envolvendo comandos de voz é o aplicativo Sesame, da empresa CandyHouse (2015), considerado um "smart-lock". O mesmo utiliza funções existentes da plataforma Apple para, em conjunto com um dispositivo instalado sobre uma fechadura, trancar e destrancar portas. No entanto, este sistema desperta a atenção quanto à segurança dos dados envolvidos, pois um smartphone pode ser roubado ou o sistema como um todo pode sofrer ataques (SEGRETTI, 2015). Além disso, é necessário que a fechadura tenha dimensões dentro do padrão estabelecido pela marca. O aplicativo possui funcionalidades interessantes, como controle automático por horário e liberação de acesso a terceiros, ideias que foram modificadas e aplicadas em nosso sistema. As principais vantagens do projeto em relação ao Sesame são a alta escalabilidade, possibilidade de aplicação em ambientes comerciais, ainda mais tipos de restrições controláveis e segurança do sistema.

No livro "The Scientist and Engineer's Guide to Digital Signal Processing" (SMITH, 1999, p. 364) é apresentado o contexto de reconhecimento de voz e fala, ilustrando detalhes fundamentais pertinentes à acústica e também mostrando os desafios e motivações dos estudos na área. Segundo o autor, a fala é o meio de comunicação mais rápido e eficiente entre seres humanos, e tem potencial para substituir a escrita, digitação e outros controles físicos. O autor apresenta ainda uma mensagem motivacional, explanando que sistemas de reconhecimento de voz ou fala não devem ser pensados como difíceis tecnicamente, mas como oportunidades de desenvolvimento e inovação.(SMITH, 1999, p. 368).

Semelhantemente, Stein (2000, p. 739) apresenta diversas abordagens ao problema de reconhecimento de voz e fala, alguns deles simples como a técnica de correlação e diferenciação por distâncias euclidianas, e alguns mais complexos como o processo de codificação preditiva linear de fala. Os critérios relacionados à quantização e correlação apresentados no livro também foram empregados como base para o processo de validação implementado em nosso sistema. Uma importante demonstração do processo de verificação de semelhança entre sinais utilizando conceitos de correlação foi utilizada como a principal base para o algoritmo de reconhecimento. Esta demonstração será apresentada no capítulo 3.

(MONTALVÃO FILHO et al., 2003) desenvolveram uma fechadura eletrônica, com o princípio de reconhecimento de voz através de redes neurais artificiais. O trabalho

descreve a metodologia de pré-processamento do sinal com a Transformada de Fourier e a utilização de redes neurais do tipo competitiva para a validação. Uma estratégia apresentada no texto foi adaptada e utilizada neste projeto, que é o uso de uma janela temporal fixa de 2 segundos para captação do sinal de voz, levando à maior eficiência do sistema conforme relatado pelos autores. O protótipo construído assemelha-se ao planejado para o nosso sistema, no entanto ainda possuímos o diferencial de escalar o sistema através de servidor web e banco de dados.

(VILLA REAL; HEINEN; DE OLIVEIRA, 2003) apresentam um trabalho que também é semelhante ao sistema a ser apresentado aqui. O processo de reconhecimento de senha falada apresentado pelos autores constitui da comparação correlacional dos coeficientes da Transformada Rápida de Fourier, o que é uma solução que provê tolerância à cadência das palavras faladas mas não à composição de frequências do sinal de voz. Este algoritmo serviu como base para o processamento dos sinais de voz em nosso sistema. A metodologia empregada para a implementação do projeto no entanto é diferente da nossa proposta, pois não inclui desenvolvimento de hardware, utilizando apenas um computador ou sistema embarcado que execute Linux, sistema operacional aberto. Outras implementações pertinentes ao projeto não foram relevantes para o nosso sistema.

Krasheninnikov et al. (2011) desenvolveram um projeto utilizando comandos de voz como retratos, no caso imagens 2D, e a partir de técnicas de processamento de imagens e correlação cruzada, reduzindo a interferência de ruídos nos sinais. O experimento é descrito no artigo, bem como o método utilizado para a geração das imagens e também para a operação de correlação cruzada. O aspecto de determinação de qualidade de aproximação, apesar de simplesmente baseado na distância euclidiana, mostrou-se bastante promissor e foi observado para possível utilização em nosso sistema.

Exemplos de aplicações de processos parecidos que usam correlação como base são apresentados por diversos autores, em diversas áreas de estudo. Savulea e Constantinescu (2010) realizaram e descreveram um estudo de processos correlacionais e estatísticos sobre dados sócio-econômicos de diversos países. Os resultados são mostrados no trabalho, mas o mais importante é a descrição dos processos empregados, sendo estes utilizados como base para definição do processo de validação da senha falada em nosso trabalho.

Tubbs (1989) pontua em seu trabalho importantes aspectos relativos ao reconhecimento de padrões em imagens, a partir de um modelo de referência. Diversas metodologias conhecidas na área de processamento de imagem são comparadas do ponto de vista de eficiência, sendo medido o tempo de computação de um processo de correlação.

Puth, Neuhäuser e Ruxton (2014) demonstram a aplicação do coeficiente de correlação produto-momento de Pearson na biologia, bem como as diversas interpretações possíveis sobre este e outros coeficientes relacionados à análises estatísticas. Outro campo de estudo em que é possível se aplicar métodos correlacionais para análise de dados é a psicologia, conforme descrito por Boker et al. (2002). Em seu trabalho, a correlação cruzada

janelada é usada em conjunto com detecção de picos para analisar a variabilidade de dados em séries temporais. Como a psicologia normalmente envolve padrões comportamentais, pesquisas sobre reconhecimento de doenças e condições através da análise vocal também são desenvolvidas, utilizando análise minuciosas do sinal de voz.

Como pode ser observado pela quantidade de trabalhos existentes sobre reconhecimento de padrões, o processo de correlação é amplamente utilizado na detecção de similaridade entre sinais e séries temporais, principalmente sinais biológicos que raramente são exatamente iguais. A vasta gama de áreas de aplicação também torna algoritmos correlacionais uma alternativa importante a processos mais custosos do ponto de vista computacional. A partir de referências como as supracitadas e tendo em mente os aspectos pontuados, grande parte dos segmentos do projeto pôde ser definida, delimitando o caminho a ser seguido no desenvolvimento do sistema. Mais detalhes relativos a essas bases serão descritas no próximo capítulo.

3 METODOLOGIA

Este capítulo trata dos métodos utilizados na orientação da pesquisa para o desenvolvimento do trabalho, além de um panorama dos requisitos do projeto, definidos a partir da proposição do sistema e da teoria envolvida nos aspectos de implementação.

3.1 DELIMITAÇÃO DA PESQUISA

As pesquisas realizadas para o desenvolvimento do projeto envolvem conhecimentos de diversas áreas, e estes conhecimentos são amplos e muitas vezes esparsos. Evitando trabalho desnecessário, um maior enfoque foi dado nas áreas pertinentes ao sistema.

No que diz respeito às técnicas de processamento de sinais e ao algoritmo, a partir dos trabalhos já existentes na área, foi definido um estreito escopo de estudo, envolvendo algoritmos mais simples de comparação de sinais, tal como a correlação. Técnicas complexas são empregadas em sistemas avançados e custosos, os quais não são o objetivo deste trabalho. Por isso, algoritmos de alta complexidade foram descartados, sendo referenciados apenas a nível de comparações.

São inúmeros os protocolos de comunicação existentes, no entanto, considerando os componentes presentes no projeto e as necessidades impostas pelo sistema, poucas foram as opções ponderadas para utilização. A maioria destes protocolos já possuem diretrizes bem definidas, diferentemente do algoritmo que precisou ser implementado e melhor estudado, o que diminuiu de maneira considerável o trabalho requerido para sua utilização.

A arquitetura do sistema é outro aspecto mais definido, apesar das diversas opções disponíveis no mercado. Na fase inicial do projeto, muitas dessas opções foram observadas e estudadas, buscando o melhor custo-benefício e atendimento aos requisitos. Fabricantes variadas possuem microcontroladores baseados em arquitetura ARM, previamente escolhida por afinidade dos desenvolvedores e quantidade de material de referência. Após a definição da plataforma, a Texas Tiva C baseada em ARM M4F, os estudos necessários para sua utilização foram feitos sobre os manuais e guias fornecidos, bem como outros materiais e fontes disponíveis para acesso.

3.1.1 DIVISÃO DE RESPONSABILIDADES

Por se tratar de um projeto com escopo amplo, que engloba diversos tópicos de diferentes áreas, optou-se por fazer uma divisão do trabalho de acordo com a afinidade de cada membro. É importante ressaltar que apesar das áreas de concentração de pesquisa e desenvolvimento serem diferentes e atribuídas quase que separadamente, a atuação de cada aluno não é limitada a apenas o que cabe à ele, extrapolando as ”barreiras” e assim promovendo um verdadeiro trabalho em equipe.

As responsabilidades por membro estão elencadas:

- Luiz Felipe: Algoritmos, Documentação, Protótipo, Testes;
- Tauan: Comunicações, Web, Aplicativo;
- Tiago Henrique: Hardware, Interface, Sensores;
- Tiago Mariani: Software, Servidor, Banco de Dados, Web;

3.2 EMBASAMENTO TEÓRICO

O background teórico do projeto envolve diversos aspectos de diferentes áreas, mas principalmente relacionados ao algoritmo de processamento e à parte de comunicações. Nesta seção são apresentados os principais conceitos necessários para a correta utilização das teorias e princípios das técnicas expostas. Especificamente, os conceitos que mais demandam atenção e que requerem alto nível de entendimento para serem empregados de maneira eficiente envolvem questões de processamento de sinais e comunicações, além de um aspecto essencial, a arquitetura do sistema utilizado.

3.2.1 FILTRAGEM

Constantemente em aplicações que utilizam sinais de áudio, o ruído é um grande vilão. O efeito por ele provocado é capaz de inviabilizar comunicações, ou no caso do projeto, inutilizar o áudio captado. De modo a evitar tais efeitos, é uma solução usual a implementação de filtros.

De acordo com a teoria de circuitos, um filtro é uma rede eletrônica capaz de alterar características de amplitude e/ou fase de um sinal, relativamente à frequência. O comportamento no domínio da frequência é descrito por sua função de transferência, que é dada pela razão da saída pela entrada, no domínio da frequência complexa. (LACANETTE, 1991).

Diversas características de filtros são levadas em consideração quando da sua utilização em determinadas aplicações, como resposta em fase ou resposta em amplitude. No entanto, a mais importante, que normalmente é o foco da sua utilização é a resposta em frequência. Tal característica diferencia os tipos de filtro como passa-baixas, passa-altas, passa-faixa e rejeita-faixa, entre outros menos usuais. Um outro aspecto é a ordem do filtro. Tal parâmetro altera a capacidade de atenuação em relação à frequência; quanto maior a ordem, maior a atenuação por década (ordem de magnitude de frequência).

Com o advento e o avanço da computação, um novo segmento de filtros passou a existir e ser amplamente utilizado, os filtros digitais. Tais filtros possuem as propriedades da linearidade e invariância no tempo, essenciais para a análise de seu funcionamento e estabelecimento de parâmetros relevantes.

Uma representação muito usual para os filtros digitais é na forma de equações à diferenças, onde, no domínio do tempo, dadas as entradas pode-se calcular as saídas. A

ideia é válida tanto para filtros causais quanto não-causais. Um componente importante nessa análise é o conjunto de coeficientes, uma vez que tais coeficientes representam o filtro e operam sobre o conjunto de amostras de entrada, dentro de um intervalo de amostras temporais, que é a ordem do filtro. (SMITH III, 1985, p. 19).

Existem duas formas de implementação de filtros digitais: a forma convolucional, popularmente conhecida como FIR (resposta finita ao impulso) e a forma recursiva, conhecida como IIR (resposta infinita ao impulso). A primeira tem performance melhor na filtragem, mas é mais lentamente executada que a segunda. (SMITH, 1999, cap. 14).

Como no sistema implementado os sinais interferidos por ruído são de voz, portanto de frequências baixas, um filtro que atenue o efeito de altas frequências indesejadas se faz necessário. O filtro buscado é um filtro do tipo passa-baixas, que permita que as componentes com frequência dentro do espectro de voz humana não sejam cortadas ou atenuadas.

A topologia de filtros FIR que foi utilizada no projeto é a *Constrained Least-Squares*, baseada em diagonalização de matriz. É uma topologia bastante utilizada para filtragem de imagens de ultrassom, e é facilmente implementada através da operação de convolução. Para o projeto, esta topologia apresenta desempenho satisfatório com pouca utilização de recursos.

3.2.2 PROCESSAMENTO DE SINAIS

Operações envolvendo sinais de natureza elétrica são extensamente utilizadas, como técnicas de processamento de sinais. Tais técnicas podem ser caracterizadas como analógicos ou digitais.

A abordagem analógica foi a mais utilizada por muitos anos, baseada em componentes como resistores, capacitores, indutores, transistores e diodos. O atributo principal dessa abordagem é a capacidade de solucionar equações que descrevem sistemas físicos sem aproximações e em tempo real. Com o advento dos computadores e circuitos digitais, a abordagem digital passou a ser desenvolvida e hoje é a principal tática no processamento e análise de sinais. Três elementos digitais básicos são necessários no processamento digital de sinais: somadores, multiplicadores e memória.As operações demandam certo tempo para serem computadas, e o resultado é uma aproximação numérica. Devido a esses fatores, seria possível considerar as técnicas digitais como inferiores às analógicas; no entanto, a abordagem digital ao processamento de sinais apresenta vantagens importantes, como flexibilidade e repetibilidade. Apesar de mais complexos, os sistemas de PDS hoje se igualam em questões de custo aos analógicos. (HAYKIN; VAN VEEN, 1999, p. 14). Com razão, Proakis e Salehi (2002) citam que a aplicação é que define qual a melhor técnica a ser empregada, e muitas vezes ambas o são. Neste projeto a abordagem utilizada é a digital. É necessário definir e descrever alguns aspectos importantes em PDS, fundamentais para o algoritmo de processamento desenvolvido: quantização, amostragem e correlação.

QUANTIZAÇÃO

O termo quantizar se refere ao ato de dar um valor numérico a uma quantidade. No caso de sistemas eletrônicos, um valor de tensão ou corrente elétrica é quantizado em um número capaz de ser lido por um computador ou sistema digital. Tal quantização ocorre por meio de um ADC, convertendo a variável dependente (tensão) de contínua para discreta.

O funcionamento de um sistema de quantização baseia-se em escala, ou seja, o valor de entrada é escalado em um valor numérico na saída. Tal escala é definida através da resolução e da referência. A referência constitui a menor e a maior tensão a ser convertida em um valor. A precisão, dada em bits, determina a resolução. A resolução indica qual o valor de tensão entre os níveis discretos, calculado pela Equação (1):

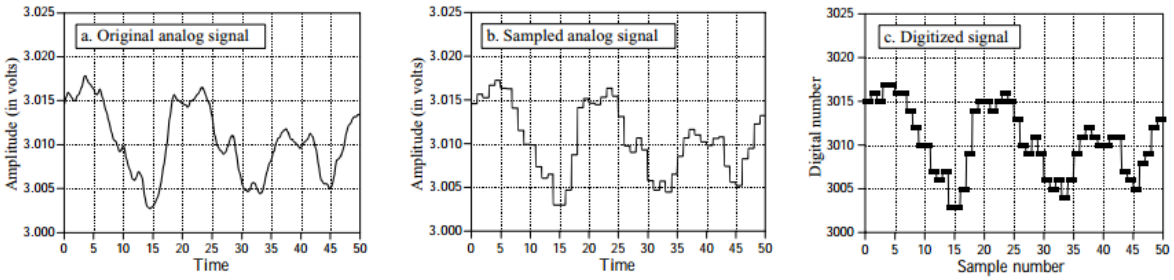
$$res = \frac{VREFP - VREFN}{2^{bits}}, \tag{1}$$

onde $VREFP$ indica o maior valor de referência, $VREFN$ indica o menor valor de referência, $bits$ indica a precisão do quantizador e res é a resolução, dada em unidades de tensão por nível discreto.

Por conseguinte, a resolução impõe uma característica aos níveis de tensão que podem assumir determinado valor inteiro. Variações menores que a resolução do sistema não variam o valor quantizado. Isto gera o chamado erro de quantização, presente em todos os sistemas de conversão analógico-digital. (SMITH, 1999, p. 35)

A Figura 1 ilustra a sequência de amostragem e quantização de um sinal analógico. É possível observar a "distorção" do sinal final em relação ao original.

Figura 1 – Sinal analógico, amostrado e quantizado



Fonte: Smith (1999)

Sistema digitais interpretam o valor do patamar estabelecido em cada instante amostral como o valor do sinal naquele instante de tempo.

AMOSTRAGEM

O Teorema da Amostragem, popularmente conhecido pelos nomes de Teorema de Nyquist ou Teorema da Amostragem de Shannon, em homenagem aos seus autores, define um valor empírico para a mínima frequência de amostragem de um sinal, sendo este valor o dobro da maior frequência presente no sinal a ser amostrado.

No processo de amostragem, é utilizado um trem de pulsos, de amplitude unitária e separados pelo período determinado pela taxa de Nyquist. Ocorre então a multiplicação desse trem de pulsos com o sinal de entrada, resultando em uma convolução no domínio da frequência. Observando-se os espectros do sinal amostrado poderá ser notado que a faixa do sinal original fica repetida a cada múltiplo da frequência de amostragem, e espelhada também. Isto ocorre devido à já citada operação de convolução entre os espectros do sinal de entrada e do trem de pulsos unitários.

Caso a ”regra”do teorema não seja respeitada, ocorre o efeito conhecido como *aliasing*, onde um sinal de frequência maior que a metade da frequência de amostragem ”assume”outro valor, menor que esta; podendo ainda ocorrer alterações na fase. Se o espectro resultante for analisado em um caso como esse, poderá ser observado a sobreposição das bandas a cada múltiplo da frequência de amostragem. (SMITH, 1999, cap. 3)

Não há um consenso sobre a definição de taxa de Nyquist ou frequência de Nyquist, dependendo de cada autor. Neste trabalho, atribuir-se-á a designação Frequência de Nyquist à metade da frequência de amostragem.

COMPRESSÃO

A compressão ou codificação é uma técnica bastante antiga, e diversos métodos foram desenvolvidos ao longo dos anos. Conforme o volume de dados aumenta, é mais custoso armazená-los ou transmiti-los, e portanto, foram realizadas inúmeras pesquisas para encontrar meios de reduzir esses custos através da compactação das informações. A compressão de dados é comumente encontrada nos dias de hoje; praticamente todos os computadores possuem ao menos cinco tipos diferentes de arquivos compactados, sendo os de mídia os mais comuns.

Em 1984, Welch publicou um algoritmo baseado em um trabalho anterior de Lempel e Ziv, o LZW. Este método de compressão é universal, se aplicando a diversos tipos de conjuntos de dados e é sem perdas, ou seja, nenhuma informação é retirada. É uma técnica extensivamente utilizada nos âmbitos computacionais e industriais, pois é bastante versátil e de fácil implementação. Seu funcionamento se dá através de uma tabela ou dicionário de dados.

O funcionamento do algoritmo é bastante simples. O conjunto de dados é analisado de forma que, se um padrão de repetição é encontrado, a sequência que o forma é substituída por uma representação indexada no dicionário. Em outras palavras, uma sequência de

caracteres é trocada por um único que os representa, através de uma tabela. Com isso, facilmente se obtém taxas de compressão de 2:1. Em casos como arquivos de sinais, ou outros conjuntos com muitas repetições, pode-se obter taxas de até 5:1.

Uma grande vantagem da compressão LZW é que a entidade que fará a descompressão não precisa do dicionário de dados utilizado para comprimir o conjunto. Ela cria um dicionário "invertido"a partir dos dados recebidos, repondo as representações diferenciadas com a sequência que originou a codificação, reconstruindo assim o conjunto original (SMITH, 1999, p. 488).

A compressão de dados é uma técnica valiosa, que possibilita a redução de custos de armazenamento e transmissão de dados. A LZW foi a técnica escolhida para comprimir os dados a serem enviados pela placa ao servidor, onde o mesmo faz a descompressão restaurando o sinal de áudio captado.

3.2.3 ALGORITMO DE CORRELAÇÃO

Como a proposta do projeto envolve o uso de um algoritmo baseado em correlação para o reconhecimento e validação da senha falada, aspectos importantes da teoria estatística e matemática que envolvem o processo foram pesquisados de modo a prover embasamento sólido para o desenvolvimento do algoritmo.

No caso de variáveis aleatórias e populações, estatisticamente define-se um coeficiente de correlação r, conhecido como coeficiente produto-momento ou simplesmente correlação total, dito por Kenney (1939, p. 162) como "a média aritmética dos produtos dos desvios dos valores correspondentes às suas respectivas médias, para dois grupos de amostras expressadas em seus respectivos desvios-padrão como unidades". Para dois grupos de N amostras x e y, matematicamente:

$$r = \frac{1}{N} \sum_{i=1}^{N} \frac{(x_i - \bar{x})(y_i - \bar{y})}{\sigma_x \sigma_y}. \tag{2}$$

Semelhantemente, Spiegel e Stephens (1999, p. 312) definem uma equação derivada de (2). No entanto, r é utilizado como medida de correlação entre dois grupos de variáveis que se acredita terem uma relação linear. Para fins de comparação posteriores, a equação apresentada é:

$$r = \frac{\sum xy}{\sqrt{(\sum x)^2 (\sum y)^2}}. \tag{3}$$

Todavia, a correlação entre sinais e não amostras populacionais deve ser empregada em processamento de sinais. Para tal, utiliza-se a cross-correlação (ou correlação cruzada) e a auto-correlação, operações matemáticas com variantes contínuas e discretas e cuja usabilidade será apresentada a seguir.

A convolução é uma operação bastante conhecida, mas a correlação não. Apesar de semelhantes ao olhar, têm características e aplicações diferentes. A correlação é de

extrema importância na área de comparação e detecção de sinais, se estendendo também às comunicações através da filtragem casada (SKLAR, 2001, p. 124). Inicialmente, o processo de correlação foi empregado em radares, e desde então as aplicações têm aumentado. No que diz respeito a processamento de voz, a correlação é a base do processo de codificação preditiva linear (LPC), importante em reconhecimento de palavras.

A base matemática, apesar de simples, é extensa. Antes dos sistemas discretos, o processo de correlação era aplicado a sinais e sistemas contínuos. No entanto, como outras operações com sinais, equivalentes discretos foram desenvolvidos. Alguns teoremas constituem o "manual" da comparação de sinais através da correlação. Nesta seção serão apresentados os pontos pertinentes ao sistema implementado, dando ênfase ao processo de correlação discreta.

Stein (2000, p. 349) define a operação de correlação r_{xy} entre dois sinais x e y para um atraso k como na Equação (4). Este caso é conhecido como cross-correlação, amplamente utilizado como medida de similaridade entre dois sinais:

$$r_{xy}(k) \equiv \sum_{n=-\infty}^{\infty} x(n)y(n-k). \tag{4}$$

Um caso especial da cross-correlação é a auto-correlação, onde realiza-se a operação de um sinal com ele mesmo, caso esse apresentado na Equação (5), utilizado para detectar periodicidade em um sinal e em processos estocásticos:

$$r_{xx}(k) \equiv \sum_{n=-\infty}^{\infty} x(n)x(n-k). \tag{5}$$

Para se determinar um parâmetro de similaridade entre dois sinais, realiza-se a cross-correlação entre eles, como anteriormente descrito. Como o resultado são as somas das multiplicações entre as amostras dos sinais deslocadas, necessita-se de um valor numérico único. Tal valor é obtido a partir da dedução a ser apresentada a seguir.

(STEIN, 2000, p. 351) Considerando-se r_n como o sinal de referência, s_n como o sinal recebido a ser comparado e n_n o ruído presente, e sabendo que o sinal recebido é o sinal de referência multiplicado por um fator qualquer A somado ao ruído, tem-se:

$$s_n = A.r_n + n_n. \tag{6}$$

O critério de equivalência é dado pela menor diferença entre o sinal de entrada e o de referência, sendo que um fator de ganho g é o que escala o sinal recebido. Para se obter o valor de g considera-se que em determinado momento não há ruído, assim:

$$g = \frac{r_n}{s_n} = \frac{1}{A}. \tag{7}$$

Como o sinal de ruído é nulo, sua energia também o é, deste modo:

$$\sum_n (r_n - g s_n)^2 = 0. \tag{8}$$

Abrindo o produto notável:

$$\sum_n r_n^2 - 2g \sum_n r_n s_n + g^2 \sum_n s_n^2 = 0. \tag{9}$$

Como definido anteriormente, a cross-correlação entre os dois sinais r e s, aqui denotada por C_{rs}, é dada como:

$$C_{rs} = \sum_{n=-\infty}^{\infty} r(n)s(n). \tag{10}$$

Sabendo-se que a energia de um sinal discreto é dada pela soma de cada amostra ao quadrado, define-se E_r como a energia do sinal de referência, e E_s como a energia do sinal de entrada:

$$E_r = \sum_n r_n^2 \tag{11}$$

$$E_s = \sum_n s_n^2. \tag{12}$$

Substituindo as equações 10, 11 e 12 em 9:

$$E_r - 2gC_{rs} + g^2 E_s = 0. \tag{13}$$

Da equação 7 pode-se deduzir que:

$$g^2 = \frac{\sum_n r_n^2}{\sum_n s_n^2} = \frac{E_r}{E_s}. \tag{14}$$

Substituindo a equivalência de g em (13) conclui-se finalmente que:

$$C_{rs} = \sqrt{E_r E_s}. \tag{15}$$

Assim, considerando-se as possíveis distorções e ruídos no sinal recebido, tem-se:

$$|C_{rs}| \leq \sqrt{E_r E_s}. \tag{16}$$

No entanto, toda a demonstração acima não considera o caso de diferença de fase entre sinal de entrada e de referência, para o qual necessitar-se-á apenas calcular as cross-correlações considerando os intervalos relevantes de atraso (deslocar as amostras), para mais ou para menos, e utilizando o maior valor resultante das operações. É imediato que a auto-correlação de um sinal com intervalo de atraso nulo, ou seja, sinais exatamente

sobrepostos no tempo, é numericamente igual ao valor da energia média do sinal. Assim, tem-se que:

$$max(|C_{rs}|) \leq \sqrt{r_{rr} r_{ss}}. \tag{17}$$

Comparando com o caso estatístico de populações e amostras, a equação 17 tem estrutura bastante próxima à da equação 3, o que indica a conformidade da demonstração apresentada.

Como a equação 17 apresenta a comparação que precisa ser feita mas não uma quantidade para a similaridade entre os sinais, determina-se um coeficiente de correlação ρ:

$$\rho = \frac{max(Crs)}{\sqrt{r_{rr} r_{ss}}}. \tag{18}$$

Definindo um valor mínimo de referência, pode-se utilizar enfim o coeficiente ρ para se determinar o quão similar um sinal é em relação a um padrão de referência. Muitas técnicas de processamento de voz e predição linear se baseiam neste método, assim como o algoritmo a ser empregado pelo sistema descrito neste trabalho.

3.2.4 COMUNICAÇÕES

Atualmente é imprescindível a presença de algum tipo de comunicação nos sistemas eletrônicos. Este é um campo amplo que engloba diversas teorias relacionadas aos canais de comunicação e à informação que será transmitida por eles. Como os conhecimentos relacionados à área são vastos, apenas alguns detalhes mais importantes serão abordados.

Os protocolos de comunicação utilizados no projeto são descritos nesta subseção, as especificações, o funcionamento e detalhes de implementação para cada um também.

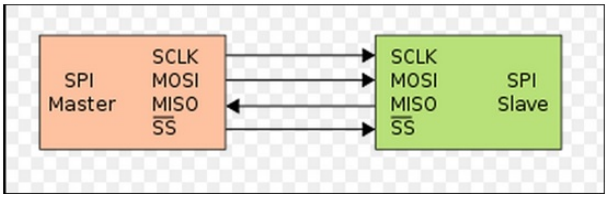
PROTOCOLO SPI

Desenvolvido pela Motorola em 1972 para comunicação entre seus equipamentos, o Serial Peripheral Interface, ou simplesmente SPI, é um protocolo de comunicação que permite a comunicação síncrona de dados seriais entre microcontroladores e dispositivos periféricos, ou até mesmo entre microcontroladores, dispostos em uma curta distância. Neste protocolo, dois ou mais dispositivos são conectados de modo full-duplex, ou seja, os dados são transmitidos e recebidos simultaneamente, fazendo com que a velocidade de troca de dados seja maior.

O protocolo SPI é single-master, ou seja, sempre um único dispositivo central (master) será responsável por iniciar a comunicação. Sendo assim, é dever deste dispositivo fornecer o clock para o sincronismo da comunicação com os escravos (slaves).

O barramento SPI consiste de 4 pinos para a comunicação master/slave: MOSI, MISO, CLK e SS. Tais pinos podem ser vistos na Figura 2 para uma comunicação SPI com um único slave:

Figura 2 – Barramento SPI Single-Slave



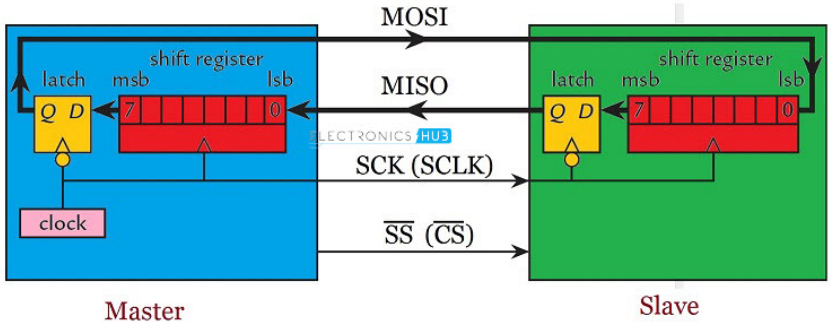
Fonte: Malik (2016)

O sincronismo na comunicação master/slave é obtido através de um clock enviado pelo pino SCLK do barramento do SPI master. Os pinos MOSI (Master Out Slave In) e MISO (Master In Slave Out) referem-se à transferência de dados. Logo, a saída de dados do master é conectada à entrada de dados do slave e, vice-versa.

Para habilitar o slave com o qual o master deseja se comunicar utiliza-se o pino SS. O master pode então gerar o sinal de clock e enviar/receber os dados, e assim pode haver a comunicação simultânea. O pino SS é usado para selecionar com qual ou quais slaves o master está se comunicando. A cada pulso de clock um bit de dado é transmitido do master para o slave e um bit de dado é transmitido do slave para o master.

Fisicamente, um dispositivo slave consiste de um shift register e um data latch. Um dispositivo master possui o mesmo hardware, porém acrescentando um gerador de clock (ANUSHA, 2017).

Figura 3 – SPI-Hardware

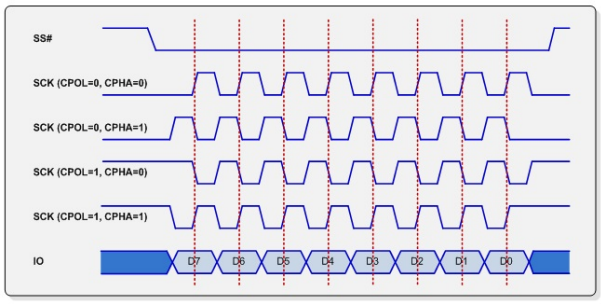


Fonte: Anusha (2017)

Pode-se observar na Figura 3 que ambos os shift registers estão conectados formando um loop. Sendo assim, os bits são deslocados do slave para o master e do master para o slave a cada sinal de clock.

O sinal de clock no SPI pode ser modificado utilizando as propriedades de fase (CPHA) e polaridade (CPOL) do clock para formar quatro únicos modos, a fim de fornecer flexibilidade na comunicação entre master e slave. Tais propriedades definem, respectivamente, quando os bits são amostrados/capturados e o valor do clock quando o SPI está em modo ocioso.

Figura 4 – SPI-Bus-Timing



Fonte: Corelis (2017)

Como pode ser visto na Figura 4, a polaridade do clock irá determinar que a amostra/captura dos bits será na borda de subida ou descida. Já a fase determinará o atraso em que será feito a amostragem/captura dos bits: primeira borda do clock ou segunda borda do clock.

PROTOCOLO TCP/IP

A essência do projeto é a construção de um sistema conectado via rede a um servidor de modo a permitir a escalabilidade, e portanto um meio de comunicação com a internet se faz necessário. Para isso, através da interface Ethernet, foi escolhido o protocolo TCP/IP, capaz de garantir entrega de pacotes e que possui um nível de segurança grande para esta aplicação.

Apesar da existência de outras alternativas, como o protocolo UDP, o TCP/IP se mostra a melhor solução em termos de aplicação e custo, além de possuir grande volume de material disponível para consulta e ser o principal protocolo utilizado para acesso a web.

O modelo TCP/IP é composto por dois principais protocolos que definem seu nome, TCP (Transmission Control Protocol) e IP (Internet Protocol).

O TCP faz parte da chamada camada de transporte, responsável por realizar a comunicação de dados entre a aplicação e o serviço de envio e recebimento de dados. Especificamente, provê um serviço de comunicações confiável, orientado à conexão. O serviço é responsável por reconhecer os pacotes recebidos, sequenciá-los e recuperar eventuais pacotes perdidos durante a transmissão. O protocolo TCP não foi projetado originalmente para ter como prioridade a segurança, já que a aplicação e o número de usuários não requeriam tal característica. Com o crescimento da Internet e de diversas aplicações em conjunto, o requisito de segurança se tornou algo indispensável para qualquer aplicação envolvendo esta comunicação. Para um cenário em que há um grande congestionamento de dados, o que poderá acontecer com a implementação do projeto em uma empresa de grande porte, o protocolo TCP possui a solução de diminuir a taxa de transmissão de

dados. (TANENBAUM, 2011, p. 556).

O IP é um dos protocolos que compõem a camada de rede. É responsável por endereçar, rotear, fragmentar e reconstruir pacotes de dados, tarefa realizada pelo serviço do protocolo IP.

3.2.5 SISTEMA

A escolha da arquitetura do sistema e a plataforma de desenvolvimento são importantes, pois refletem nos requisitos técnicos e dependem dos requisitos funcionais. A questão da afinidade dos desenvolvedores também é levada em conta nesta decisão. Considerando as diversas opções presentes no mercado, a mais comum e que possui as funcionalidades necessárias para implementação de um sistema como o descrito neste trabalho é a arquitetura ARM.

ARQUITETURA ARM

A arquitetura ARM incorpora algumas funcionalidades da arquitetura RISC, sendo semelhante à mesma, como registro uniforme de carregamento e armazenamento, onde as operações são realizadas apenas entre registradores e não entre conteúdos de memória, e modos de endereçamento simples, onde os endereços são determinados pelos registradores e campos de instruções.

Com o passar do tempo, a arquitetura ARM vem agregando mais funcionalidades para suprir a necessidade do mercado, em termos de performance e possibilidades, e é em muitos mercados a arquitetura computacional mais utilizada. Os atributos principais desta arquitetura são a dimensão reduzida, performance e baixo consumo, sendo então uma alternativa excelente para a implementação de sistemas avançados de forma eficiente.

A família de processadores ARM é divida em três segmentos: A, voltada para sistemas de alta performance; R, voltada para sistemas de tempo real; e M, para sistemas microcontrolados. (ARM, 2017)

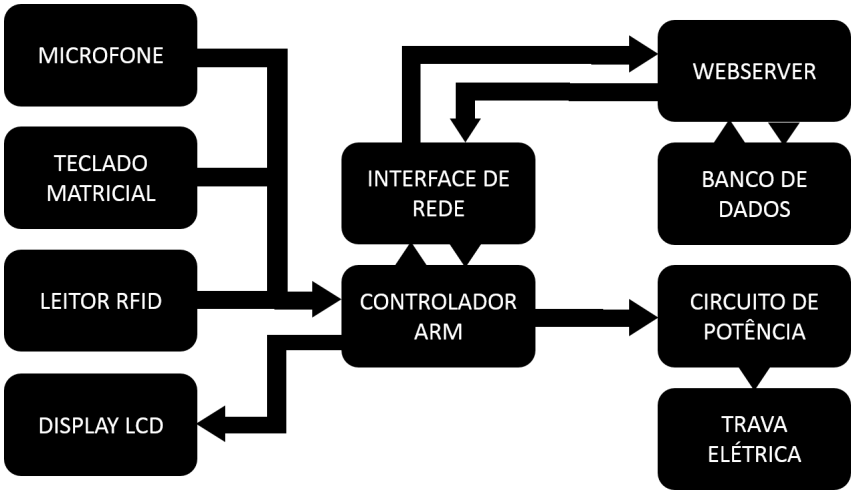
Os processadores da família M apresentam baixa latência e operação altamente determinística, o que é ideal para sistemas embarcados. Os conjuntos de instruções permitem implementações limpas e códigos reduzidos. As extensões arquiteturais incluem processamento digital de sinais e operações com ponto flutuante, o que melhora significativamente a performance do dispositivo.

O processador Cortex M4 é próprio para o mercado de controle e processamento de sinais, oferecendo eficiência, baixo consumo e baixo custo, além da facilidade de uso. Consegue-se simplicidade de implementação com instruções integradas para PDS, conexão com a rede e operações matemáticas e ponto flutuante. Os conjuntos de instruções Thumb/Thumb2 são bastante conhecidos e também facilitam o suporte e implementações com o processador.

3.3 MODELAMENTO DO SISTEMA

Os conceitos e teorias, juntamente com pesquisas de disponibilidade de componentes no mercado e de soluções existentes, foram de grande importância para que se pudesse modelar o sistema, cujo diagrama de componentes é apresentado na Figura 5. Tal modelo foi fundamental para realizar a separação de atividades, como descrito anteriormente, além de guiar a estruturação do desenvolvimento de código e interfaces entre os componentes previstos.

Figura 5 – Diagrama do sistema



Fonte: Autoria Própria

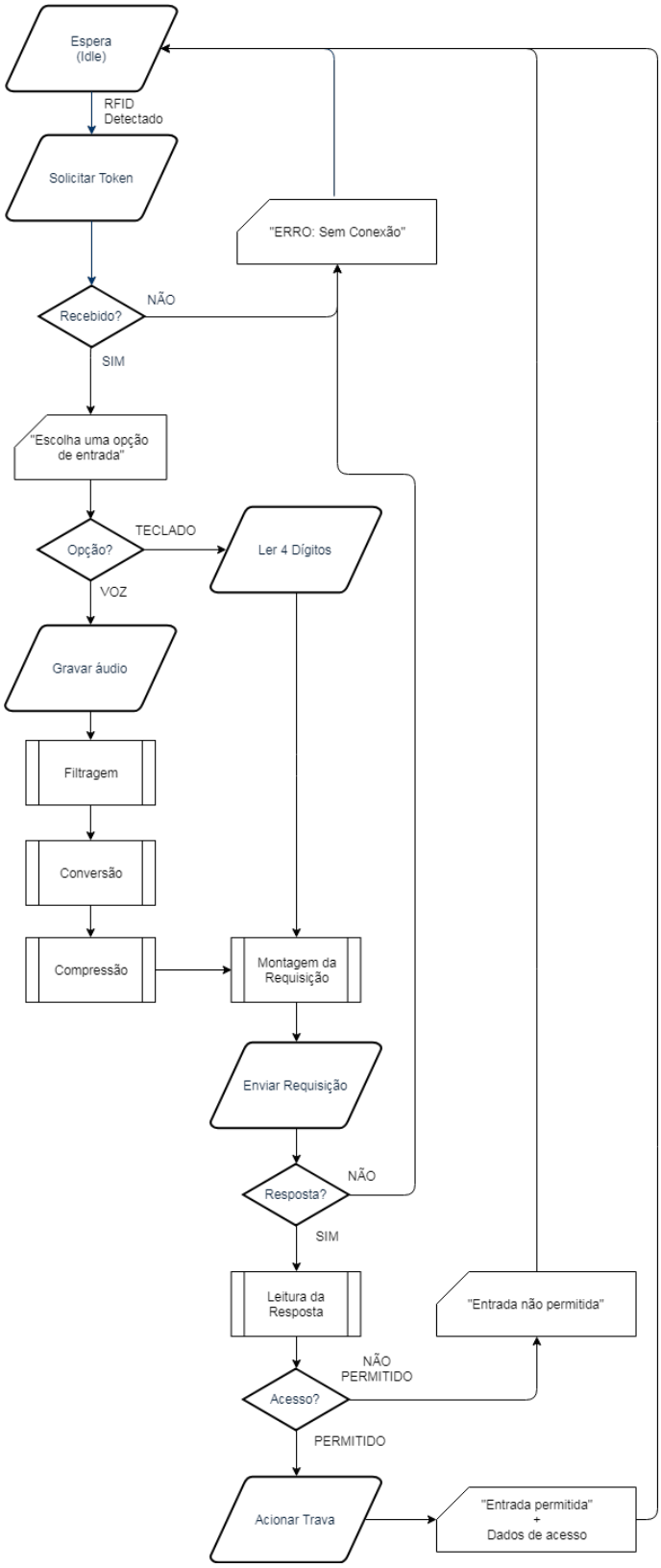
3.3.1 SEQUÊNCIA DE FUNCIONAMENTO

A definição da ordem de execução dos processos necessários é um procedimento importante na definição dos requisitos e para o desenvolvimento direcionado do sistema.

Como o controle de acesso é baseado em senhas, estas precisam ser armazenadas em um banco de dados, associadas a seus respectivos usuários, tanto a numérica como a de voz. No processo de cadastro, em um computador, um leitor de RFID é utilizado para cadastrar o cartão ou tag do usuário. Os dados do mesmo são inseridos através de uma página web e a voz é captada com auxílio de um microfone, gerando o arquivo a ser armazenado como senha falada. A senha digitada é inserida em um campo a parte, com verificação dupla.

A sequência de funcionamento do sistema, na visão do controlador, é apresentada na Figura 6 em forma de fluxograma simplificado. Apenas as etapas e processos mais importantes foram incluídos.

Figura 6 – Fluxograma sequencial na visão do controlador



Fonte: Autoria Própria

3.3.2 CENÁRIOS

Aqui serão apresentados alguns possíveis cenários no decorrer do uso do sistema. As opções mais prováveis de acontecer foram elencadas, e é descrito o comportamento do sistema em cada uma, aqui listadas:

USUÁRIO CADASTRADO

Caso um usuário cadastrado deseje ter acesso a determinada área, o mesmo se identificará através da sua tag RFID. O equipamento deve enviar uma requisição de acesso para o servidor com a senha e código de equipamento. Ao receber essas informações, o servidor irá retornar uma mensagem de confirmação de recebimento, juntamente com um token, confirmando acesso ao servidor. Com o token, o fuso horário do país em que se encontra o equipamento e a tag de RFID, o equipamento fará uma requisição de acesso do usuário. O servidor, ao receber esta mensagem, irá retornar uma confirmação de recebimento, juntamente com o áudio e o nome do usuário. O equipamento, por sua vez, irá fazer o processo de captação da voz e a liberação caso a resposta do servidor seja positiva. Um log será enviado para o servidor, tanto em caso de sucesso como de fracasso, que será registrado no servidor.

USUÁRIO NÃO CADASTRADO

Caso um usuário não cadastrado tente acessar, ao não encontrar uma entrada com a identificação RFID, o servidor envia uma mensagem de acesso proibido e irá registrar em log do servidor. O mesmo ocorre caso o usuário digite ou fale de forma incorreta a senha.

USUÁRIO SEM CADASTRO DA VOZ

Caso o usuário não esteja com o cadastramento de sua voz, será possível a opção de acesso pela digitação da senha pelo teclado numérico do equipamento. Neste caso, o equipamento deverá enviar para o servidor a tag do RFID e a senha digitada. O servidor deverá responder ao equipamento a confirmação de recebimento da mensagem e com a autorização ou não do acesso.

ACESSO NÃO PERMITIDO

Caso um usuário que não tenha acesso a determinada área ou seja temporário e o tempo esteja fora do permitido tente realizar um acesso, o servidor deverá enviar uma mensagem de acesso proibido e registrar em log.

3.4 REQUISITOS DO PROJETO

A partir das teorias bases para o desenvolvimento dos componentes do projeto em conjunto com a sequência de funcionamento previamente descrita, os requisitos necessários para o funcionamento do sistema de acordo com a proposta, para garantir a qualidade e eficiência do sistema e para o funcionamento e operação dos componentes foram definidos e serão apresentados nesta seção.

3.4.1 REQUISITOS FUNCIONAIS

Considerando os procedimentos de operação definidos na seção anterior, os requisitos funcionais necessários para que essas etapas se concretizassem e fossem implementadas da melhor maneira possível foram definidos.

Para o cadastro é utilizado um computador. No mesmo, a página web do sistema deve ser acessada, e realizado então o cadastramento de um novo usuário, contendo os dados pertinentes, como nome, data de nascimento, e-mail, etc. É também captada e armazenada a senha falada através de um microfone no próprio computador, devendo ser configurado para realizar amostragem em mono e amostragem de 48kHz, fazendo posteriormente o downsampling para 16kHz.

Como o início do processo de requisição de acesso se dá através do RFID, um leitor, no caso um módulo conectado à placa, está disponível para o usuário. Complementarmente, um teclado matricial é empregado como forma de entrada de alguns comandos. São usados LEDs como dispositivos indicadores, para sucesso ou fracasso nas etapas de verificação de RFID e senha. As mensagens e informações referentes à tentativa de acesso devem ser mostradas de maneira clara e objetiva ao usuário, usando para tanto um display LCD de 20 colunas por 4 linhas.

3.4.2 REQUISITOS NÃO-FUNCIONAIS

Como forma de garantir um sistema eficiente e de qualidade, alguns requisitos não-funcionais foram levantados, de modo a guiar o desenvolvimento do projeto levando em consideração também a questão prática do sistema, não apenas a técnica. Alguns requisitos aqui apresentados são comumente incluídos em sistemas comerciais de diversas aplicações, sendo caracterizados e reconhecidos como requisitos importantes para garantir uma boa experiência com o produto ou sistema na visão do usuário.

TEMPO DE ATENDIMENTO

Como modo de evitar esperas desnecessárias, é definido um tempo máximo de atendimento da requisição dos dados do servidor a serem analisados. Caso os pacotes solicitados não sejam entregues em um prazo de 10 segundos após a captura da senha falada, o sistema deve indicar falha por *timeout*, e uma nova tentativa deve ser feita.

QUALIDADE DE SERVIÇO (QoS)

Com a finalidade de medir, fornecer serviços melhores e mais previsíveis, largura de banda dedicada, jitter controlado e latência de uma rede de comunicação foi criado o conceito de Qualidade de Serviço (Quality of Service - QoS). Este conceito é caracterizado através de quatro parâmetros principais: confiabilidade, retardo, flutuação e largura de banda.

Para a aplicação deste projeto, em que será necessário uma comunicação para envio e recebimento de amostras de um sinal de áudio de um microcontrolador para um servidor, o sistema deve ter tolerância a falhas quase nula. No que diz respeito à largura de banda e retardo, não se faz crítico o requisito de funcionamento, desde que sejam recebidos os dados.

SEGURANÇA

Por se tratar de um sistema de controle de acesso, a segurança do mesmo é obviamente um requisito importante.

A segurança neste projeto está em garantir que, ao longo do percurso da comunicação, as informações não sejam lidas por mais ninguém além do destinatário. Para isso, todas as camadas da rede contribuem para a segurança, mas na camada de transporte é onde será possível criptografar conexões inteiras, mantendo a segurança máxima exigida pelo projeto.

CONFIABILIDADE

Devido aos requisitos de funcionamento e à necessidade de uma camada de transporte confiável, ou seja, com a garantia de entrega de envio dos pacotes, um protocolo que possua essas características deveria ser utilizado.

DISPONIBILIDADE

Novamente, por se tratar de um sistema de controle de acesso, o mesmo deve estar disponível sempre, para que não haja limitações no ir e vir devido à falhas evitáveis, como as causadas por congestionamento de dados.

3.4.3 REQUISITOS TÉCNICOS

Com base nos manuais (TI USER'S GUIDE, 2016), (MANUAL TI, 2014), relativos à componentes do sistema, foi necessário definir alguns requisitos técnicos para o projeto. Os principais requisitos dizem respeito à configurações dos módulos da plataforma e seus periféricos.

CAPTAÇÃO DE ÁUDIO

O sistema é baseado em senha de voz, para tanto, uma senha falada deve ser adquirida e utilizada como objeto de validação. Esta senha falada é gravada por um microcontrolador, dispositivo digital, e armazenada para envio posterior. Para tanto, o Teorema da Amostragem define uma frequência mínima de amostragem para o sinal. Considerando que a frequência da voz humana dificilmente passa de 2kHz, uma frequência de amostragem de 4kHz já seria suficiente para garantir, pelo Teorema da Amostragem, uma representação correta do sinal capturado. Frequências de amostragem maiores melhorariam a representação do áudio, pois mais pontos por ciclo seriam armazenados.

O sinal de áudio a ser captado passa por um conversor analógico-digital, que requer uma frequência de operação entre 16MHz e 32MHz. O dispositivo da placa possui um sistema de *sample and hold*, que ”segura” o valor de uma amostra convertida por um número de ciclos, variando com um valor programado entre os possíveis, sendo no mínimo 16 ciclos e no máximo 268 ciclos. O componente também possui restrições quanto ao sinal de entrada, que não deve ser negativo e deve ter magnitude dentro dos limites especificados, que são de 0V a 3,3V.

4 DESENVOLVIMENTO

Este capítulo trata dos aspectos que envolvem o desenvolvimento e implementação do projeto. Três partes constituem o sistema: hardware, firmware e software, cada qual tratada mais especificamente em sua seção. Uma apresentação geral de estudos feitos sobre a plataforma de modo a viabilizar a implementação eficiente também é apresentada, incluindo conceitos e requisitos referentes ao microcontrolador e periféricos utilizados.

As três partes foram inicialmente desenvolvidas quase em paralelo, uma vez que a implementação de cada uma é independente num primeiro momento. Após os componentes essenciais finalizados, deu-se início à integração dos mesmos, fazendo a ligação entre hardware, firmware e software, o que resulta no funcionamento do projeto como sistema completo e não mais em partes.

4.1 ESTUDO DA PLATAFORMA

Os estudos necessários para o correto desenvolvimento do projeto serão apresentados de maneira breve nesta seção, focando nos conceitos teóricos atrelados aos requisitos técnicos e funcionais discutidos no capítulo anterior, com as limitações e possibilidades encontradas na fase inicial da implementação e de estudo.

Com a definição dos requisitos do projeto, iniciou-se a busca por uma plataforma capaz de atender às necessidades do sistema ou pelo menos prover meios de fazê-lo. As soluções da Texas Instruments são bastante conhecidas por oferecer bom custo-benefício com bastante funcionalidade e suporte. Uma linha é a Tiva, utilizada para diversos projetos com microcontroladores e sistemas embarcados.

A Tiva C, especificamente o modelo TM4C129EXL Crypto Connected, é uma placa que contém os recursos necessários. Para a conexão com a rede e acesso ao servidor/banco de dados, a placa possui interface Ethernet MAC e PHY. Para realizar a captação de voz, dois ADC de 12 bits estão integrados à placa, com taxas de até 2Msps. Oito timers de 32 bits podem ser utilizados para fazer temporização. Diversos pinos de entrada e saída estão disponíveis em 15 blocos de GPIO para uso com os mais variados periféricos, como o display LCD e teclado matricial. Também é preparada para comunicação SPI com o RFID.

Em suma, a plataforma escolhida possui recursos para suprir as necessidades do sistema e assim cumprir os requisitos do projeto. O custo da placa está dentro do previsto, tendo uma excelente relação custo-benefício, sendo a melhor entre as concorrentes pesquisadas.

Detalhes técnicos relativos às implementações de cada uma das interfaces e funcionalidades foram pesquisados e elencados com auxílio do *datasheet* do microcontrolador (MANUAL TI, 2014) e também do guia do usuário da placa (TI USER'S GUIDE, 2016).

Também foram consultadas referências da internet na solução de dúvidas e problemas que surgiram durante a implementação. Uma delas é o fórum E2E (TEXAS INSTRUMENTS INC, 2018), da própria Texas.

4.2 HARDWARE

A seção trata dos elementos físicos, componentes e dispositivos eletrônicos, presentes no projeto, divididos em sensores, atuadores e os relativos à interface, além da placa de desenvolvimento.

A maioria dos elementos empregados no sistema foram adquiridos já prontos, como teclado matricial e display. Todavia, circuitaria de apoio foi desenvolvida para viabilizar a utilização dos componentes e fazer uma melhor integração física no protótipo.

Especificações dos componentes, bem como aspectos lógicos e computacionais quando pertinente são descritos nas subseções de cada elemento.

4.2.1 INTERFACE

A interface é um aspecto do projeto responsável pela interação com o usuário. O sistema implementado conta com uma interface simples mas amigável, composta por teclado, display, LEDs indicadores e sinalização sonora. Nesta subseção, as especificações relativas a cada item da interface são apresentadas, em conjunto com os detalhes das implementações.

TECLADO

Devido a problemas que podem ocorrer que impeçam a aquisição da amostra de voz, tais como queima do microfone ou indisponibilidade do usuário em pronunciar a senha falada na fechadura, o teclado surge como uma alternativa à senha falada até que tal exceção seja corrigida.

O modelo utilizado no projeto é um teclado matricial de 16 teclas dispostas em 4 linhas por 4 colunas, e um conector de 8 pinos para ligação com a placa.

A leitura das teclas é feita a partir de uma multiplexação das chaves (teclas) com um arranjo matricial. Com isso pode-se ler as 16 teclas com apenas 8 terminais.

Dispondo-se de um grupo de chaves separado em linhas, aciona-se uma linha por vez de modo que apenas uma linha se ligue as colunas. Deste modo configura-as linhas e colunas como saída e entrada, respectivamente. Assim, para acionar apenas uma linha, e desativar as outras, coloca-se um nível lógico baixo na respectiva linha e alto nas linhas a serem desativadas.

Com a linha desejada acionada, basta verificar se houve alguma mudança na leitura das colunas. Isso é feito verificando qual coluna apresenta um nível lógico baixo. Logo tem-se a linha e coluna acionadas, podendo assim determinar qual tecla foi pressionada.

Devido a baixa segurança da senha digitada, em comparação com a senha falada, a opção de digitar a senha pelo teclado será liberada apenas na ocorrência das exceções citadas anteriormente. O sistema reconhecerá qual usuário necessitará desse atendimento a partir da verificação do RFID.

DISPLAY

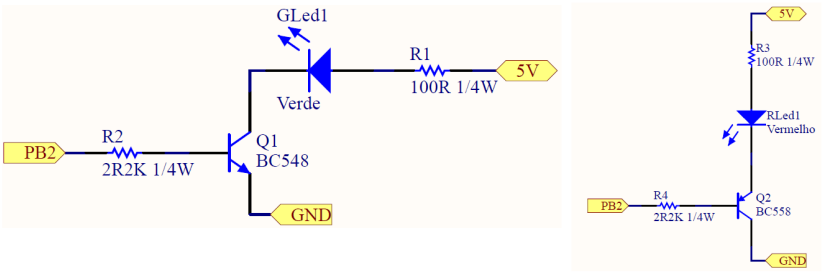
Para uma melhor interface com o usuário haverá um display LCD 20x4 (FILIPEFLOP, 2017), o qual apresentará algumas informações importantes tais como tempo até o início da gravação da voz, tempo de duração da gravação, usuário liberado ou não liberado, usuário cadastrado ou não cadastrado, dentre outras. A interface entre display e a placa é de forma paralela, com as conexões entre os pinos do display e os pinos da placa contidos na Tabela 1.

INDICADORES

Com o intuito de mostrar ao usuário se a permissão de entrada dele a determinado local foi aceita ou não, utiliza-se de indicadores sonoros (buzzer) e visuais (leds). Para o primeiro utilizou-se de um módulo buzzer cujo acionamento é feito enviando um sinal PWM para alterar a frequência do sinal sonoro ou apenas um sinal de nível alto/baixo para emitir um som. Já para o segundo usa-se o sinal padronizado para permissão concedida, no caso o led verde, e permissão negada, led vermelho.

Como a placa apenas controla os leds, sem fazer a alimentação dos mesmos, optou-se por utilizar transistores para acionamento deles. Além disso, evita que uma corrente excessiva seja necessitada da placa Tiva C. Para esse fim utilizou-se de dois transistores: um NPN (BC548) e um PNP (BC558) para acionamento dos leds verde e vermelho em níveis lógicos alto e baixo, respectivamente (Figura 7).

Figura 7 – Esquemático do circuito de acionamento dos Leds



Fonte: Autoria Própria

4.2.2 SENSORES

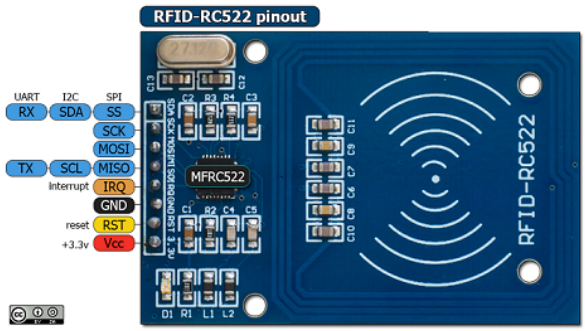
Os sensores utilizados são especificados e descritos nesta subseção, expondo também as implementações e configurações realizadas com os mesmos. Os sensores são uma parte importante do projeto, pois são o meio de entrada de dados do ambiente externo, como poderá ser observado a seguir.

RFID

Para habilitar a captação da voz, cada usuário tem um cartão, ou tag, com um determinado código de identificação que é armazenado em um banco de dados juntamente com a senha de voz. Tal código será utilizado para indexar o arquivo armazenado.

A técnica utilizada para a comunicação com o cartão/tag é a identificação por rádio-frequência. Para isso, necessita-se de um leitor RFID que consiga detectar o sinal emitido pelo cartão/tag e os envie para o microcontrolador. Para a leitura desse código no momento da requisição de abertura da porta utiliza-se o módulo leitor RFID baseado no chip MFRC522 da NXP Semiconductors. O módulo RC522 contendo o CI MFRC522 é mostrado na Figura 8.

Figura 8 – RFID-RC522



Fonte: $http://fritzing.org/projects/control-acess-rfid-rc522$

O MFRC522 é utilizado para comunicação sem contato com cartões ou tags MIFARE na frequência de 13,56MHz e suporta a ISO 14443 A/MIFARE, utilizando taxas de transmissão de até 848kBd em ambas as direções. Para a comunicação com o host são fornecidas as interfaces SPI, serial UART ou I2C. (NXP MFRC522, 2016).

Neste projeto utilizou-se a interface SPI para a comunicação da placa Tiva com o MRC522. Com esta interface suporta-se troca de dados com o host com uma velocidade de até 10 Mbit/s. Quando comunicando com um host, o MFRC522 atua como slave recebendo dados do host para configuração dos registradores, e enviando e recebendo dados da interface de comunicação RF (NXP MFRC522, 2016). A interface implementada segue o padrão SPI. Sendo assim o sinal de clock do SPI é gerado pelo master (microcontrolador).

O MFRC522 utiliza um buffer FIFO 8x64 bit para armazenar o fluxo de dados de entrada e saída entre ele e o host. Isto torna possível gerenciar fluxos de dados de até 64 bytes sem a necessidade de se levar em consideração restrições de tempo. Os cartões/tags escolhidos seguem o padrão Mifare S50 com memória EEPROM de 1K bytes, frequência de operação de 13,56MHz e padrão ISO 14443/14443A (MF1S50YYX/V1, 2014). Ambos são compatíveis com o módulo leitor RC522.

Os cartões/tags Mifare Classic 1k S50 são compostos por um microcontrolador e uma antena. O primeiro contém uma EEPROM de leitura e escrita onde as informações do usuário são armazenadas. Já a antena, que consiste em uma bobina com um pequeno número de voltas diretamente conectada ao cartão/tag, é utilizada para a transmissão e recepção de dados na frequência de 13,56MHz. Como os cartões/tags não possuem sua própria fonte de alimentação, eles são energizados pelo campo eletromagnético gerado pela antena do leitor, estabelecendo uma conexão via rádio.

Seus dados são organizados em 16 setores com 4 blocos de dados e estes possuem 16 bytes cada (MF1S50YYX/V1, 2014). Nesses endereços podem ser armazenados dados pessoais do usuário, bem como uma senha para validação de acesso a informações e/ou locais protegidos. Porém, no projeto utiliza-se apenas os 4 bytes iniciais na memória do cartão como senha, sendo os pré-configurados de fábrica. Utiliza-se desses bytes pois estes são capazes de atender a demanda inicial de usuários. Além disso, como há outra verificação para o acesso do usuário, a senha falada, não há como um cartão configurado com a mesma senha tenha acesso.

Os cartões Mifare Classic S50 utilizam um algoritmo de criptografia de fluxo da própria NXP, o CRYPTO1, para fornecer confidencialidade e autenticação mútua entre leitor e cartão/tag. As chaves utilizadas nesta criptografia são as armazenadas no Sector Trailer, que nos caso dos cartões são simétricas. Ainda, faz uso do protocolo de autenticação mútuo de três passos baseados na ISO 9798-2 (MF1S50YYX/V1, 2014).

A comunicação sempre é iniciada pelo leitor e controlada pela Unidade Digital de Controle do cartão. A resposta do cartão vai depender das condições de acesso e da autenticação. Após Power-On Reset, o cartão responde à um comando de requisição REQA ou à um comando *wake-up* WUPA com um valor ATQA: 0044h para o MF1S500 e 0004h para o MF1S503 (Padrão ISO/IEC 14443) (MF1S50YYX/V1, 2014).

No laço de anticolisão o identificador do cartão é lido. Caso haja vários cartões no campo de leitura ao mesmo tempo, tal identificador os distingue e um deles pode ser selecionado e pode efetuar a comunicação. Já os outros cartões são retornados ao estado inativo, ou ocioso, aguardando um próximo comando de requisição (INTERNATIONAL STANDARD ISO/IEC, 1999).

Após o identificador do cartão ser lido, o sistema informará se a próxima operação de verificação será a senha por voz ou pelo teclado.

CAPTAÇÃO DE ÁUDIO

Para a captação da voz do usuário no momento da tentativa de autenticação, a utilização de microfone de eletreto foi estabelecida. Inicialmente, houve a tentativa de ligar apenas um pequeno circuito de apoio ao componente, constituído de um resistor de pull-up e um capacitor de desacoplamento.

Por questão de praticidade, optou-se por utilizar um módulo comercial de captação com microfone de eletreto, o Keyes KY-308, como o da Figura 9. Este componente possui uma saída analógica de áudio, onde o nível médio é controlável via um resistor variável. Tal nível foi estabelecido em 1,65V, metade do valor de alimentação do mesmo, para que a modulação seja efetuada corretamente, uma vez que o ADC não permite entrada de tensões negativas.

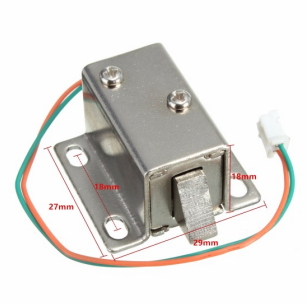
Figura 9 – Módulo de Microfone Keyes KY-038

Fonte: $https://i.ebayimg.com/images/g/XxEAAOSwofxUcpcM/s-l300.jpg$

4.2.3 ATUADORES

Na construção da fechadura eletrônica utilizou-se uma trava elétrica solenoide de 12V (Figura 10). Aplicando uma tensão de 12V em seus terminais, o pino da trava é recolhido (porta aberta), mantendo nesta posição até esta tensão ser retirada. Não havendo tensão em seus terminais o pino da trava volta ao seu estado normal (porta fechada).

Figura 10 – Trava elétrica solenoide 12V



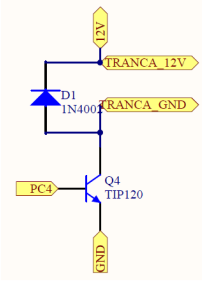
Fonte: $https://www.filipeflop.com/produto/mini-trava-eletrica-solenoide-12v/$

Quando a entrada do usuário é permitida, um sinal de 5V é enviado ao relé que libera uma tensão 12V nos terminais da trava, abrindo a porta. Caso contrário, nenhum

sinal é enviado ao relé resultando em uma tensão 0V nos terminais da trava, mantendo a porta fechada. A trava necessita de uma tensão de 12V e consome uma corrente de até 600mA para funcionar corretamente. Como a Tiva trabalha com uma tensão máxima de 5V e corrente máxima de 64mA em seus pinos, houve a necessidade de utilizar um gatilho para acionamento (transistor) e uma fonte externa. Com relação ao primeiro, optou-se por utilizar um transistor Darlington de média potência, TIP 120, pois devido a seu alto ganho de corrente não exige alta corrente da placa para o acionamento da trava. Além disso, por conseguir dissipar até 65W (ON SEMICONDUCTOR, 2014), o acionamento da tranca, que consome 7.2W, não o esquentaria em excesso, evitando assim a necessidade de se utilizar um dissipador.

Deve-se ainda colocar um diodo polarizado inversamente entre os terminais da trava (*snubber diode*, Figura 11). Estes ajudam a eliminar transientes de tensão que ocorrem quando bobinas magnéticas param de conduzir. Tal tensão ocorre no momento em que a bobina (solenoide) que estava energizada é desligada, já que as linhas de força do campo magnético gerado pela bobina, que se encontravam em expansão máxima, se contraem. Nessa contração, há uma indução de corrente elétrica no sentido oposto ao que estava estava criando o campo magnético, podendo atingir valores elevados de tensão. Sendo assim, quando a trava solenoide é desligada, a alta tensão gerada nos extremos da bobina no momento da interrupção de corrente irá polarizar diretamente o diodo, fazendo com que este apresente uma resistência baixa, absorvendo esta energia. Sem tal diodo, os picos dessa tensão podem danificar os componentes do circuito como o próprio transistor de acionamento (PETRUZELLA, 2011).

Figura 11 – Esquemático do circuito de acionamento da trava solenoide.



Fonte: Autoria Própria

4.2.4 CONTROLADOR

Para o uso dos diversos periféricos e dispositivos necessários ao projeto, foram feitas as devidas conexões à placa, como na Tabela 1. A relação apresentada não leva em consideração os pinos de alimentação de nenhum periférico. Os pinos foram escolhidos de

acordo com a funcionalidade embutida descrita no TI User's Guide (2016, p. 12) ou por praticidade para fazer as conexões.

O RFID foi conectado ao Port de GPIO preparado para comunicação SPI, enquanto que a saída do captador de áudio foi conectado a um pino ligado à uma das entradas do ADC contido na placa. Os pinos dos demais periféricos foram associados à Ports de GPIO com pinos afins disponíveis.

Tabela 1 – Conexões aos pinos da placa Tiva.

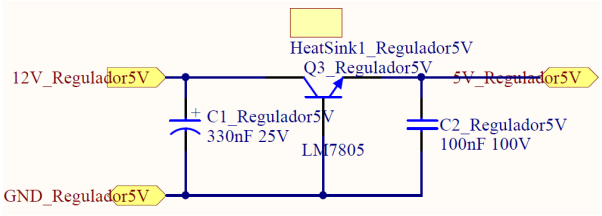
Periférico	Função	Pino
Teclado Matricial	Linha 1	PL0
	Linha 2	PL1
	Linha 3	PL2
	Linha 4	PL3
	Coluna 1	PE0
	Coluna 2	PE1
	Coluna 3	PE2
	Coluna 4	PE3
Display LCD	Enable	PM0
	R/W	PM1
	RS	PM2
	Data 0	PK0
	Data 1	PK1
	Data 2	PK2
	Data 3	PK3
	Data 4	PK4
	Data 5	PK5
	Data 6	PK6
	Data 7	PK7
RFID	MOSI	PD1
	MISO	PD0
	SCK	PD3
	NSS	PD2
	RST	PG0
Buzzer	In	PB3
LEDS	VM	PB2
	VD	PB2
Microfone	Out	PE5
Trava	In	PC4

Fonte: Autoria Própria

Em conjunto com a Tiva, uma segunda placa foi desenvolvida para apoiar o controle dos periféricos, e com esses compor o protótipo físico. Esta placa secundária tem a função de prover alimentação para os periféricos externos, como o display LCD e a trava, além de ser um agente de centralização, para todas as partes estarem conectadas em um ponto comum. Ou seja, essa segunda placa serve para realizar a interface física entre a Tiva e os diversos periféricos.

A alimentação do protótipo foi feita com uma fonte chaveada externa de 12V 3A. No entanto, precisa-se de tensões de 5V para alimentar os demais componentes e utilizou-se o regulador de tensão L7805 que fornece em sua saída 5V 1,5A para isso. Este foi utilizado em conjunto com dois capacitores, 330nF e 100nF, conforme sugere o datasheet do L7805 (STMICROELECTRONICS, 2014). O primeiro capacitor, eletrolítico, desacopla a entrada do estabilizador enquanto que o segundo, cerâmico, desacopla a saída e evita oscilações em altas frequências (Figura 12).

Figura 12 – Esquemático do regulador 5V



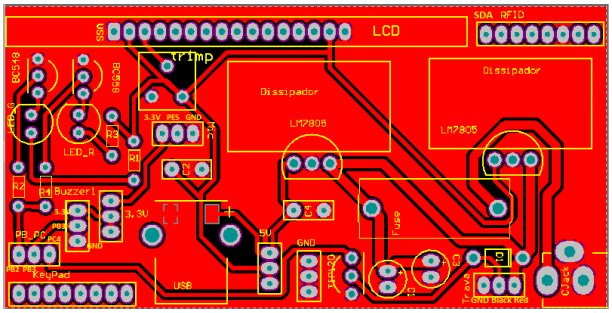
Fonte: Autoria Própria

Porém, como a corrente necessitada da saída do regulador para a alimentação do circuito é próxima a corrente máxima do L7805, este precisaria de um dissipador muito grande, o que aumentaria o tamanho da placa. Por isso optou-se por utilizar dois reguladores de 5V e dividir a alimentação dos componentes entre os dois. Com isso, pôde-se usar dois dissipadores menores.

Todo o esquemático e o layout da placa de alimentação e controle foram desenvolvidos com o auxilio do Multisim para os testes, e do Altium para a prototipagem.

Com o circuito pronto e testado, partiu-se para a confecção da placa. Primeiramente repassou o circuito testado para o Altium e criou-se um layout para placa (Figura 13). Depois este foi impresso termicamente sobre uma placa cobreada de fenolite 5x10cm. Após um processo de corrosão com percloreto de ferro e a soldagem dos componentes, obteve-se o protótipo final.

Figura 13 – Layout da placa de alimentação e controle



Fonte: Autoria Própria

4.3 FIRMWARE

Esta seção trata dos componentes do firmware do projeto, especificamente drivers, configurações e funções referentes ao algoritmo de compressão, filtragem, interface, controle e periféricos. Para a implementação em código, a linguagem C foi empregada em conjunto com a IDE própria da Texas, o Code Composer Studio versão 6.

No que diz respeito ao desenvolvimento de programas e drivers para a plataforma ARM utilizada, inicialmente foram criadas as bibliotecas de funções específicas para o ADC, Timer, GPIOs e controle da CPU. Contudo, nos testes iniciais destas partes isoladas, foram identificados problemas de configuração que não puderam ser resolvidos, e como o foco do projeto não é o desenvolvimento das interfaces de comunicação com os periféricos, a implementação de tais funções foi suspensa.

Tomou-se então a decisão de se utilizar as bibliotecas de drivers disponibilizadas pela Texas Instruments, contidas no software TivaWare, versão 2.1.4 (TIVAWARE USER'S GUIDE, 2016). As funções e definições contidas nos arquivos não foram modificadas, e os devidos direitos autorais são respeitados.

Outras funções necessárias para o sistema, tais como rotinas de serviço de interrupção, inicialização e configuração de periféricos, foram propriamente desenvolvidas, contendo referências às bibliotecas usadas.

4.3.1 CONTROLE DO SISTEMA

Para a unidade de processamento do sistema, considerando os requisitos técnicos anteriormente apresentados, configurações foram efetuadas para a correta operação da mesma.

A frequência de operação do microcontrolador foi definida em 120MHz, utilizando o circuito PLL presente na plataforma. Somente os periféricos que são utilizados no sistema foram habilitados, visando economia de energia. O controlador de interrupções também foi configurado de modo a permitir que os devidos periféricos gerassem interrupções de maneira apropriada e que suas rotinas de serviço fossem mapeadas corretamente.

4.3.2 TIMERS

Quatro timers foram utilizados para propósitos distintos, por isso configurados de maneira ligeiramente diferente. Os módulos escolhidos foram os módulos 0, 1, 2 e 3, todos operando com a frequência base de 16MHz do oscilador interno. O bloco Timer A de cada módulo foi escolhido para receber a carga de contagem.

O Timer do módulo 0 foi utilizado para realizar a temporização do disparo de conversão no ADC, por necessidade de ser uma frequência de amostragem fixa e específica. O contador do Timer A foi carregado com o valor respectivo a um intervalo de disparo de 62,5547us, o que resulta em um frequência de aproximadamente 15,986kHz, valor mais próximo que se obtém de 16kHz. Como configuração, o contador reinicia automaticamente quando a contagem chega ao valor pré-carregado, disparando assim um sinal para o ADC iniciar a conversão do dado na entrada. O contador deste módulo é ativado quando o usuário pressiona a tecla para habilitar a captação de voz, e é desativado após as amostras serem adquiridas.

O Timer do módulo 1 foi utilizado para temporizar a espera para retorno ao estado inicial (*idle*) do hardware, no qual o sistema está pronto esperando um usuário. É configurado para um disparo único após 4, 5 ou 11 segundos. O primeiro intervalo é carregado/ativado quando o usuário tem seu acesso liberado ou não. O segundo é carregado/ativado quando o usuário é inquerido sobre a escolha de senha: voz ou senha digitada. Já o último intervalo é carregado/ativado para o processo de digitação da senha pelo usuário. Para ambos os casos, quando o disparo ocorre, uma rotina de interrupção vinculado ao Timer 1 tranca a porta, retorna o display LCD à mensagem inicial, apaga o led verde, acende o vermelho e atualiza algumas flags de auxílio.

Já o Timer do módulo 2, que também é configurado para um disparo único, é utilizado como temporização de utilização do teclado. Serve para limitar o tempo que o usuário tem para terminar a rotina de utilização do teclado, como a escolha de senha digitada/voz ou mesmo para digitar a senha. Para o primeiro, ocorre sempre que o usuário passa o cartão RFID e o mesmo está cadastrado. Em seguida é requisitado que o usuário digite sua opção: voz ou senha. Nesta primeira ocasião o Timer 2 é carregado para contar 5 segundos antes do disparo. Já o segundo caso ocorre quando o usuário escolhe a opção de senha digitada e é requisitado para digitar a mesma. Neste caso o Timer 2 é carregado para contar 10 segundos antes de disparar, tempo limite que o usuário tem para digitar a senha. Em ambos os casos uma rotina de interrupção vinculada a este Timer irá salvar a opção como vazia (”none”, nem voz nem senha digitada), e também irá salvar uma senha ”default” que impedirá o acesso do usuário, caso a contagem chegue ao fim. Nestes dois casos este Timer é carregado/acionado juntamente com o Timer 1, com a diferença que o Timer 2 é utilizado para tratar rotinas específicas do teclado.

Por último, o Timer do módulo 3, também configurado para disparo único, é utilizado apenas para desacionar o buzzer após um tempo de 0,5 segundos quando a

entrada do usuário é permitida, ou após um tempo de 2 segundos, quando sua entrada não é permitida.

O emprego dos módulos timers facilita muito a implementação de sistemas e programas que demandem exatidão de tempo ou que dependam de tempo para certos procedimentos. Do mesmo modo, no sistema implementado, os pontos críticos em relação à tempo foram corretamente sustentados com o emprego destes módulos.

4.3.3 CONVERSOR A/D

Apenas um dos módulos conversores analógico-digital da plataforma foi utilizado, sendo o módulo 0. O mesmo foi configurado para amostrar o canal 8, ligado ao pino 5 da porta E, e a amostragem acontece quando o Timer 0 citado na subseção anterior dispara, em uma frequência de 7,993kHz.

A resolução do ADC é 12 bits, mas as amostras são armazenadas no formato de inteiros de 8 bits. De maneira semelhante, os sinais de áudio captados via computador são amostrados a 48kHz, e *downsampled* para 8kHz. Isto foi necessário devido à limitações na memória da placa, que é de apenas 256KB.

Nos sistemas de telefonia, a frequência de voz considerada varia entre 300Hz e 3400Hz, deste modo, amostragem a 8kHz já assegura, pelo Teorema de Nyquist, que todas frequências são corretamente amostradas. No projeto, a frequência escolhida é satisfatória para a correta representação dos mesmos, além de permitir maior eficiência na utilização da memória por outros processos.

O armazenamento das amostras na memória se dá na ISR do ADC, através de funções disponibilizadas na biblioteca (TIVAWARE USER'S GUIDE, 2016). O módulo ADC é ativado apenas quando a requisição para início da captação da voz acontece, e é desativado após as amostras serem captadas. Estas são armazenadas no formato inteiro sem sinal, de 8 bits, variando portanto de 0 a 255.

4.3.4 FILTRO DIGITAL

Para reduzir a interferência de ruídos de altas frequências relativamente aos sinais de áudio a serem adquiridos, um filtro passa-baixa digital foi implementado. A topologia escolhida foi a *Constrained Least-Squares* de ordem 30, um filtro tipo FIR (resposta finita ao impulso) com frequência de corte em 2kHz. Este filtro foi escolhido por ser de fácil implementação, resposta rápida e performance relativamente boa. Os coeficientes do filtro foram obtidos através da ferramenta FDATool do MATLAB. A implementação se deu utilizando um vetor para armazenamento dos coeficientes e um vetor auxiliar para salvar uma certa quantidade de amostras para não comprometer muita memória. O resultado do filtro é sobrescrito no buffer de amostras adquiridas, gradativamente.

Pode-se observar na Figura 14 a curva de resposta em frequência do filtro, obtida experimentalmente, onde nota-se a frequência de corte próxima de 2kHz. Novamente,

só foram plotados valores para frequências de até 10kHz pelo fato de o microfone não responder além.

Figura 14 – Curva de resposta em frequência do filtro FIR

Fonte: Autoria Própria

Após a filtragem, os valores numéricos das amostras são convertidos em pares de caracteres ASCII que os representam na forma hexadecimal. Por exemplo, uma amostra de valor 127 é armazenada com os caracteres 7 e F. Isto é feito para que se possa realizar o envio utilizando um *charset* compatível com a plataforma Tiva.

4.3.5 COMPRESSÃO LZW

Com a transformação dos valores das amostras de inteiros numéricos para pares de caracteres ASCII, há um aumento significativo na quantidade de dados a serem enviados; opta-se então por comprimir esses dados.

O algoritmo LZW é bastante simples de ser implementado. Comumente utiliza-se dicionários de 12bits, permitindo 4096 entradas, mas, como a transmissão dos dados é feita via caracteres ASCII, optou-se por utilizar um dicionário de 8 bits. O número de entradas é bastante reduzido, restringindo-se apenas aos caracteres imprimíveis entre 0 e 127. Excluindo-se os que já são utilizados para representar valores não codificados, obtém-se 60 entradas disponíveis. Apesar de não se ter muitas possibilidades de substituição de sequências, a implementação provê taxa média de compressão de 1,45:1, sendo suficiente para realizar a transmissão dos dados.

Apesar de haver certo custo computacional relacionado à implementação do algoritmo de compressão e sua execução, não houve impacto perceptível na utilização do sistema, sendo comprovada a eficiência do algoritmo LZW.

A descompressão, realizada no servidor, consiste no processo inverso, de implementação igualmente simples. Nos testes realizados, não houve casos de erros na descompressão.

4.3.6 ETHERNET

A placa de desenvolvimento EK-TM4C129EXL usada no projeto possui um módulo Ethernet, 10/100 Mbits/s MAC + PHY. O padrão Ethernet originalmente foi desenvolvido para 10 Mbits/s, mas este já possui conexão para 100 Mb/s, também chamada de Fast Ethernet, uma forma de comunicação mais rápida e que ao mesmo tempo mantém a compatibilidade e características básicas do antigo padrão Ethernet 10 Mbit/s.

Este foi um fator considerado na escolha da placa de desenvolvimento na fase inicial, com a tecnologia com melhor custo/benefício e economicamente mais viável de rede de computadores por garantir compatibilidade com as redes mais existentes e pelo custo do cabo. Tal módulo é essencial para a comunicação cliente/servidor.

4.4 SOFTWARE

Esta seção apresentará os desenvolvimentos realizados no aspecto de software do projeto, como a implementação de páginas e serviço web, banco de dados, algoritmo e comunicações. Estas partes são de extrema importância para o correto funcionamento e atendimento a alguns dos requisitos estabelecidos.

4.4.1 ALGORITMO

Como apresentado no capítulo 3, a base teórica envolvida no processo de desenvolvimento do algoritmo é razoavelmente extensa, no entanto, simples. As equações (4), (5) e (18) foram implementadas no servidor.

O coeficiente ρ de correlação previamente determinado necessita dos parâmetros: maior valor de cross-correlação e o valor das auto-correlações dos sinais com deslocamento zero (o que corresponde à energia do sinal). No momento dos cálculos das correlações, um laço *for* multiplica cada amostra do buffer por ela mesma, dividindo por 255 (o valor máximo) para diminuir drasticamente a magnitude dos números a serem calculados, evitando assim possíveis extrapolações dos limites do tipo de variável, e soma progressivamente até chegar ao resultado. Para a cross-correlação, leva-se em consideração ainda o valor de atraso máximo, definido previamente no código. Considera-se diferenças de até 100ms, um intervalo pequeno mas relevante para que o sistema seja flexível à pequenas variações e ainda assim seguro. Com isso, um laço de repetição, também do tipo *for*, calcula a soma dos produtos das amostras correspondentes entre os dois vetores armazenados, dividindo por 255 e resultando em (2 * número de amostras de atraso) + 1 valores de cross-correlação. Busca-se então o maior desses valores, que é utilizado no cálculo do coeficiente final. O valor de ρ é calculado como na equação (18), simplesmente dividindo o maior valor de cross-correlação pela raiz do produto das auto-correlações. O resultado é um valor entre 0 e 1, e é comparado com o mínimo requisitado, também previamente definido no código

como parâmetro alterável no banco de dados. Caso o coeficiente de correlação seja igual ou maior ao valor mínimo definido, a senha é reconhecida como válida, do contrário, não.

Para o armazenamento dos valores utilizados no algoritmo, dois buffers de amostras foram definidos, com tipo vetores de inteiros, além de variáveis tipo ponto flutuante para os valores das auto e cross-correlações e o coeficiente final. Funções para encontrar o valor máximo em um buffer, bem como as de cálculo das correlações foram implementadas. Uma função de validação é responsável por realizar a chamada para essas outras, tendo como resultado final um *booleano* correspondente à validade da senha falada.

4.4.2 COMUNICAÇÃO ENTRE DISPOSITIVO E SERVIDOR

PROTOCOLO HTTP 1.1

Em conjunto ao protocolo TCP/IP, o protocolo HTTP 1.1 (*HyperText Transfer Protocol*) foi escolhido para este projeto como a forma de comunicação entre cliente servidor, baseado no paradigma de requisição e resposta.

A escolha do protocolo foi baseada na segurança e garantia de entrega dos pacotes, fatores essenciais para o projeto. Concentrando sempre a resposta dos métodos ao servidor. Garantindo assim que o servidor apenas responda equipamentos que enviem requisições corretas, incluindo senhas e identificações.

MÉTODOS IMPLEMENTADOS

O HTTP 1.1 é composto no total por oito métodos, mas para este projeto, foram usados apenas métodos POST. Para está aplicação, apenas este método seria de utilidade, devido ao equipamento (cliente) não poder realizar cadastramento pelo próprio dispositivo, concentrando o controle para o servidor, evitando assim os outros métodos oferecidos no HTTP.

A comunicação é realizada por duas diferentes sequências de métodos HTTP. A primeira forma é utilizando o método POST, enviando a identificação da placa e a senha, ambos cadastrados pelo cliente no servidor. O servidor por duas vez irá responder um token (JWT) e código 200. Ao final disto, o equipamento terá armazenado em sua memória o token. A segunda requisição será usando o método POST também, enviando este token no header da mensagem com a tag RFID e a senha ou áudio do usuário, dependendo do tipo de acesso que o usuário irá escolher. O servidor irá processar está mensagem e irá responder com uma mensagem de autorização ou não, dependendo do áudio ou senha enviado serem corretos ao cadastrado no servidor.

Concentrando o processamento da senha e voz ao servidor teremos maior rapidez e segurança ao sistema, sendo o equipamento apenas um módulo do servidor. O dispositivo só irá se conectar e enviar mensagens para o servidor e irá apenas processar as respostas

do servidor apenas após o envio de requisições, evitando requisições mal intencionadas vindas de outros dispositivos não pertencentes ao sistema.

CÓDIGOS DE RETORNO

Por motivos de tratamento dos erros na comunicação, foram implementados ao sistema três tipos de código de retorno para as requisições. O código 200 é usado para informar do servidor para o equipamento que a mensagem foi recebida e bem interpretada. Enquanto para o código 404, a mensagem foi recebida com erro, com erros na formação da mensagem, informando ao equipamento estes códigos após o envio. O código 400 também avisa um erro, mas o erro será referente ao conteúdo dos itens enviado, como por exemplo senhas e identificados errados, evitando o acesso deste usuário.

FORMATO DE ENVIO DAS MENSAGENS EM JSON

Além de seguir o protocolo HTTP para a comunicação, deve-se usar um formato que seja aceito tanto no transmissor como no receptor de mensagens. O formato usado neste projeto foi o JSON (JavaScript Object Notation), formato padrão, simples e amplamente utilizado em vários sistemas. Além disso, o formato em questão é de interpretação e geração pelas máquinas, além de ser independente da linguagem de programação usada e dos endpoints. O formato se concentra no uso de tag e seus conteúdos, podendo estes serem tanto em formato de texto, entre aspas, como também em números.

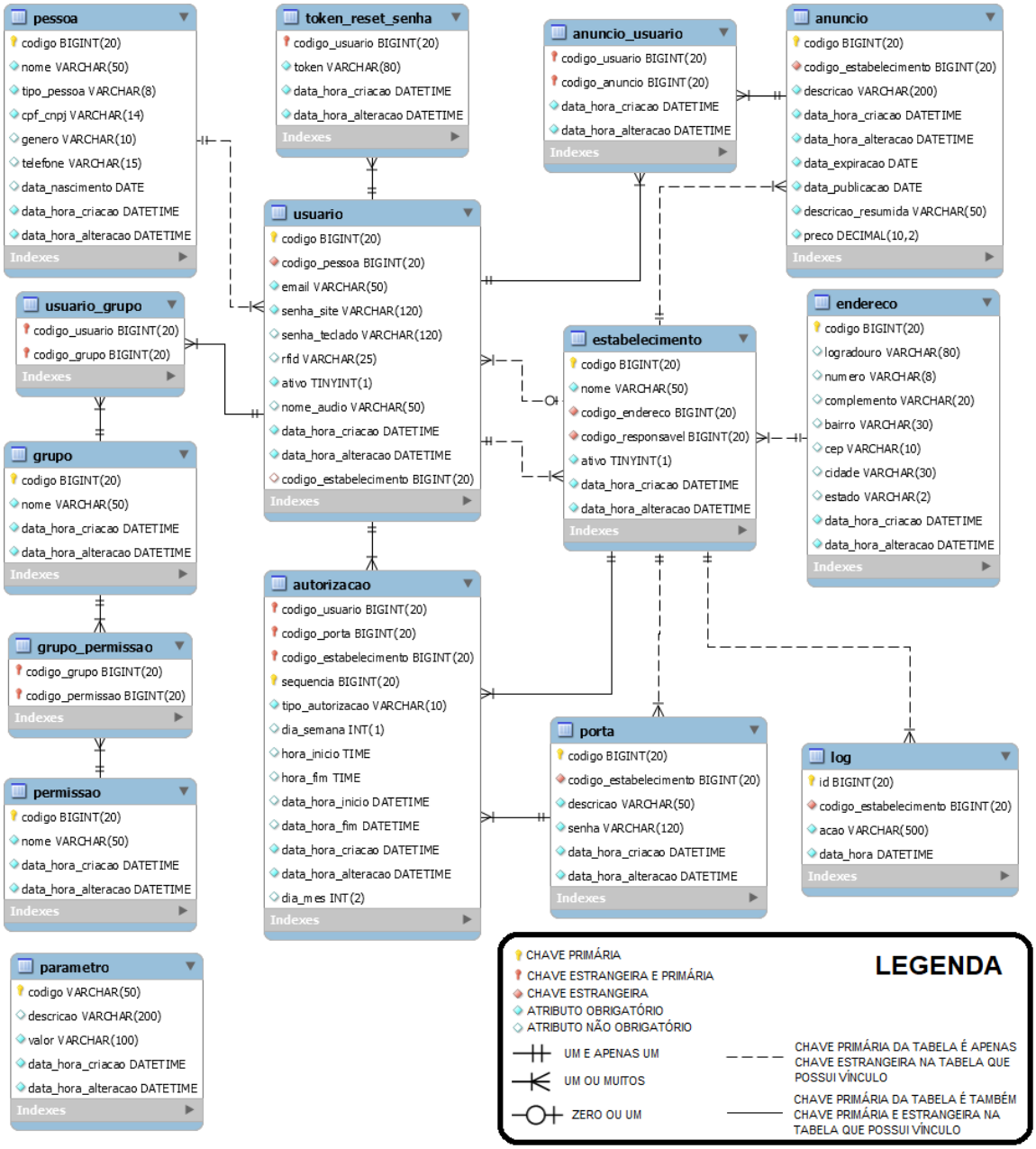
JSON WEB TOKEN

Por ser um projeto que faz parte da área de segurança, houve grande preocupação também na segurança dos dados, impedindo que outros equipamentos não autorizados entre em comunicação com o servidor para roubo de dados ou para conseguir acesso. Uma das formas implementadas na comunicação para aumenta a segurança, foi o uso do JSON WEB Token (JWT). Está forma de segurança é baseada por token, em que o cliente que gostaria de se comunicar com o servidor envia por formato JSON por método POST um identificador e uma senha, caso estes estejam de acordo, o servidor retorna uma mensagem confirmando com o token. Esta chave será usada para o acesso, de forma o cliente enviar o token em formato JSON pelo método POST, e em seguida o servidor retornar ao cliente autorização ou não do acesso do cliente. Para cada acesso ao servidor a aplicação de JWT é realizada, sendo obtido um token diferente para cada envio de identificador e senha.

4.4.3 BANCO DE DADOS

Para o armazenamento das informações coletadas via página web foi escolhido o banco de dados MySQL, a versão *Community* 6.2. Foi escolhido esse banco de dados por conta de ser um banco de dados relacional, característica que atende as necessidades do projeto, além de possuir grande notoriedade no mercado de tecnologia da informação. Segue abaixo o esquemático com as tabelas do banco de dados com suas relações.

Figura 15 – Diagrama de relacionamento das tabelas do banco de dados



Fonte: Autoria própria

ENTIDADES

Nessa seção serão descritas todas as entidades mostradas no diagrama do banco de dados.

Todas as tabelas possuem os campos: código, data hora criação e data hora alteração, com exceção das tabelas grupo permissão e usuário grupo, pois essas tabelas representam o vínculo de N:N (muitos para muitos) entre as tabelas grupo e permissão e entre as tabelas usuário e grupo. O campo código é uma chave primária, ou seja, é um valor único presente em toda a tabela e deve ser sempre preenchido. Na tabela log esse campo assumiu o nome id, mas desempenha essa mesma função. O campo data hora criação nunca pode ser modificado, pois esse campo só é informado no momento que nova informação é inserida no banco de dados. O campo data hora alteração é atualizada para a data e hora atual do sistema a cada momento que qualquer informação é alterada.

A tabela pessoa tem a função de armazenar os dados pessoais dos usuários, podendo ser informações referentes a pessoa física ou jurídica. Essa indicação é armazenada no campo tipo pessoa, onde pode assumir o valor FISICA ou JURIDICA. Caso o tipo pessoa for física, o campo gênero pode assumir três opções: MASCULINO, FEMININO ou OUTRO.

Outra tabela é a de usuário que possui vínculos com as tabelas estabelecimento e pessoa. A relação que a tabela usuário tem com a tabela pessoa é de 1:1 (um para um), ou seja, os dados pessoais do usuário ficam guardados na tabela pessoa. A outra chave estrangeira é a de relação 1:1 com a tabela estabelecimento, mas essa informação é apenas preenchida quando o usuário assume o tipo de usuário "anfitrião", mais informações sobre tipo de usuário será descrito no tópico 4.4.4.

Outro detalhe a respeito dessa tabela de usuário é com relação aos campos senha site e senha teclado. Ambas as informações são criptografadas pelo método *bcrypt*. Esse método de criptografia foi escolhido, pois apresenta maior resistência à ataques do tipo "força-bruta", onde é usado o processamento de uma máquina para inúmeras vezes tentar violar a informação que fora criptografada. Com isso as senhas mantem o seu sigilo, no qual apenas o usuário que as cadastrou saberá a sua verdadeira informação.

Ao ser cadastrada pelo usuário, a senha do site deve ter tamanho de no mínimo seis e no máximo doze caracteres alfanuméricos, deve conter pelo menos uma letra maiúscula, uma letra minúscula, um carácter especial e um número. Com esse padrão de senha, força o usuário criar senhas "fortes" e assim, essas senhas, serão mais difíceis de serem violadas.

A senha do teclado deve ter tamanho de quatro dígitos, pois essa informação é referente ao acesso alternativo as portas, podendo o usuário se autenticar usando o teclado contido na porta. O campo nome áudio é com relação ao nome dado ao arquivo de áudio. Esse nome será um identificar único universal de 128 bits e poderá ser preenchido caso o usuário for do tipo usuário.

A tabela estabelecimento armazenará as informações referentes ao local que conterá

posteriormente as portas vinculadas. Terá uma relação de 1:1 com a tabela usuário, para assim haver um responsável a ser o gestor de cada estabelecimento cadastrado. Nessa tabela também faz vinculo obrigatório de 1:1 com a tabela endereço, que tem como objetivo armazenar as informações de localidade do estabelecimento.

Outra tabela apresentada no diagrama é a porta. Nessa tabela armazena as informações de código, código do estabelecimento, descrição e senha. Os campos código e senha são inalteráveis, ou seja, a partir do momento que elas são inseridas no banco de dados não poderão mais ser alteradas pois essas mesmas informações estarão registradas em cada placa que estará nas trancas das portas.

Apenas os usuários do tipo suporte poderão criar novas portas e apenas os usuários do tipo anfitrião poderão alocar essas portas aos estabelecimentos no qual são gestores, onde nesse processo é preciso informar o código e a senha da porta. O código de estabelecimento da tabela porta faz um vínculo de 1:N com a tabela estabelecimento, deixando registrado assim que determinada porta pertence a um determinado estabelecimento, mas um estabelecimento pode possuir mais de uma porta. A descrição deve ser um breve texto informado pelo usuário, no qual pode ser alterado a qualquer momento. A senha segue os mesmos critérios de segurança das senhas contidas na tabela usuário, onde a informação é criptografada pelo método bcrypt.

A tabela autorização tem vínculo de 1:N com as tabelas: usuário, estabelecimento e porta. É a partir dessa tabela que um usuário assume autorização de acessar a uma determinada porta. Existem quatro diferentes tipos de autorização: permanente, temporária, semanal e mensal. Caso a autorização for do tipo permanente quer dizer que o usuário pode acessar a porta a qualquer dia e horário. Mas se o tipo for temporário, significa que um usuário terá acesso a uma porta em um determinado período. Assim sendo, os campos data hora início e data hora fim devem ser informados, onde a data inicial deve ser anterior à data final.

É importante salientar aqui, que existe um serviço de rotina implementado dentro do sistema, que efetua a exclusão de autorizações do tipo temporária que já foram vencidas, ou seja, onde a data final do período de uso é posterior a data e hora atual do sistema. Com isso ocorre uma "limpeza" na base de dados de informações desnecessárias.

Caso o tipo de autorização for semanal, isso permite que o usuário tenha acesso a porta apenas a um determinado dia da semana em um determinado horário, ou seja, deverá ser informado um dia da semana que poderá ser segunda-feira ou terça-feira ou quarta-feira ou quinta-feira ou sexta-feira ou sábado ou domingo. No banco de dados a coluna que corresponde ao dia da semana armazenará um número inteiro entre 1 (um) à 7 (sete), corresponde respectivamente aos dias da semana mencionados. Mas se a autorização for do tipo mensal, o usuário deverá escolher um dia no mês no valor de 1 (um) à 31 (trinta e um). Para ambos os casos, semanal e mensal, os campos hora início e hora fim devem ser preenchidos. O campo hora início deve ser anterior à hora final.

Existe uma validação que ocorre antes da gravação de cada autorização no banco de dados, onde verifica se o usuário já possui autorização permanente a porta selecionada. Caso o usuário já possua uma autorização desse tipo não será possível gravar outro tipo de autorização, seja ela temporária, semanal ou mensal.

Na tabela anúncio é gravado os dados referentes a divulgação dos lugares que poderão ser visualizados pelos usuários. Os anúncios serão inseridos através do usuário do tipo anfitrião, no qual deverá informar uma descrição resumida, descrição mais completa, um preço e uma data de expiração. Essa tabela possui vincula de 1:N com a tabela estabelecimento, ou seja, o anúncio pertence a um único estabelecimento, mas um estabelecimento pode possuir vários anúncios.

Como foi dito, esses anúncios cadastrados serão vistos pelos usuários. Quando o usuário mostrar interesse a algum desses anúncios, será então gravado na tabela anuncio usuário o código do usuário e o código do anúncio, os demais campos, data hora criação e data hora alteração, será armazenado a data e hora atual do sistema. Por meio dessa tabela, os anfitriões, responsáveis pelos estabelecimentos, poderão visualizar os usuários interessados pelos anúncios.

A tabela log conterá os registros dos acessos dos usuários as portas no qual possuem permissão, contendo a data e hora que isso ocorreu, vinculado de 1:N com a tabela de estabelecimento e no campo descrição dizendo se o acesso do usuário foi feito por senha falada ou pela senha do teclado da porta.

Na tabela parâmetro conterá os principais parâmetros do sistema para que este funcione adequadamente. Parâmetros esses que são: TOLERANCIA (erro relativo máximo permitido na comparação dos áudios), URL-RESET-SENHA (endereço de URL encaminhado para o usuário que deseja alterar a senha do site), COD-GRP-SUPORTE (código do grupo de permissões do tipo de usuário suporte), COD-GRP-ANFITRIAO (código do grupo de permissões do tipo de usuário anfitrião), COD-GRP-USUARIO (código do grupo de permissões do tipo usuário). O grupo de permissões dizem respeito aos privilégios de acesso que cada tipo de usuário possui as páginas web.

A tabela *token reset* senha terá o propósito de armazenar os *tokens* gerados que possibilitarão que os usuários que esqueceram a senha do site alterem-nas. Os *tokens* são gerados aleatoriamente com 65 caracteres, para que a possibilidade de repetição do valor desses seja a menor possível. Essa tabela possui vínculo de um para um com a tabela usuário, pois a partir desse relacionamento é que se saberá qual usuário terá a senha do site alterada. Os registros são mantidos por três dias, contados a partir da data de inserção dos mesmos, sendo excluídos após esse período. Os registros também podem ser excluídos quando os mesmos são utilizados no processo de alteração de senha do site.

As próximas tabelas descritas aqui serão a respeito da permissão de acesso que os usuários terão dentro da página web. As diferentes rotas URL que dão acesso as páginas web dentro do site seguem determinadas permissões, nomeadas de regras, que dão privilegio

de acesso a um determinado grupo de usuário. Existem três diferentes tipos de grupo que são: suporte, anfitrião e usuário. Esses três registros ficam gravados na tabela grupo, no qual tem relação de N:N, por meio da tabela usuário grupo, com a tabela usuário. Também possui vinculo de N:N com a tabela grupo permissão, no qual tem guardado os registros de todas as regras de acesso as páginas web.

Assim os usuários cadastrados são vinculados, por meio da tabela usuário grupo , a um determinado tipo de grupo, no qual permitirá a eles acessar as páginas web de acordo com as permissões vinculadas aos grupos, por meio da tabela grupo permissão.

4.4.4 PÁGINA WEB

Para construção do sítio eletrônico foi utilizado a linguagem de programação Java, versão 8, juntamente com o *framework* Spring, versão 4.3, na parte do *backend* da aplicação, onde essa parte é referente a validação e persistência dos dados no banco de dados. A parte visual da página web foi utilizado a linguagem de marcação HTML versão 5, juntamente com CSS, para gerenciar a adição de estilos. Foi utilizado também, a linguagem de programação JavaScript e o *framework* Bootstrap, versão 3.3, no qual auxiliou no desenvolvimento da construção visual do projeto, o *frontend*.

BACKEND

Essa parte do projeto diz respeito ao tratamento das informações vindas do usuário por meio da página web, onde essas informações serão validadas por regras de negócio para então serem inseridas ou alteradas ou excluídas do banco de dados. O código fonte está disponível no repositório do GitHub pelo seguinte endereço eletrônico: https://github.com/tiagompalte/tcc-porta-servico.

A linguagem de programação escolhida foi a Java na sua versão 8. Ela surgiu no ano de 1995 e possui o atributo de ser orientada a objetos, no qual contribuiu na modelagem das entidades envolvidas no projeto. O Java é compilado para o formato *bytecode* Java, que são arquivos no formato (.class), e então é interpretado pela sua máquina virtual, a JVM. Isso possibilita que essa linguagem opere em várias plataformas, ou seja, atue em diferentes sistemas operacionais.

Complementando essa parte do projeto foi utilizado o *framework open source* Spring. Essa ferramenta da programação em linguagem Java contribuiu para a construção do sistema de acesso da aplicação ao banco de dados, a segurança da página web, gerenciando as autenticações e autorizações de cada usuário, além das respostas as requisições HTTP realizadas dentro do site.

FRONTEND

Para o desenvolvimento da parte visual das páginas do site foi utilizado os recursos disponibilizados pelo *framework* Bootstrap. Nele foi disponibilizado diversos estilos em CSS e vários códigos em JavaScript, no qual possibilitaram que todas as páginas do site fossem responsivas e seguissem um template padrão. O código fonte dessa parte do projeto está disponível no seguinte endereço eletrônico: https://github.com/tiagompalte/tcc-porta-web.

Através da linguagem de marcação HTML versão 5, foi possível alocar os diferentes componentes (caixas de texto, legendas, caixas de seleção e etc), de forma ordenada nas páginas web, com a intenção de tornar a usabilidade do site fácil de ser compreendida pelo usuário.

Para que o site tenha um carregamento dinâmico dos seus componentes, dependendo da ação do usuário, foi utilizado o JQuery, para fazer requisições GET e POST, onde essas requisições são assíncronas, ou seja, não provocam o travamento da página web. Como por exemplo, na página de cadastramento de novo estabelecimento, quando o usuário digitar o CEP é enviado uma requisição GET a um serviço online de busca de endereço por CEP. Quando é retornado a resposta, os campos referentes a endereço do cadastramento de estabelecimento são sobrescritos com as informações contidas nessa resposta.

Outra ferramenta essencial na construção da página web é a atuação do *thymeleaf* na sua versão 3. Ele promove o preenchimento dos campos do HTML com os dados obtidos do servidor e constrói a página web final, na qual será entregue ao usuário.

Todas as imagens contidas no site foram obtidas pelo Pixabay (https://pixabay.com). São imagens gratuitas e livres de indicação de autoria.

GRAVADOR DE VOZ

Para que o usuário possa cadastrar a sua senha falada foi disponibilizado na página web de cadastro de usuário um gravador de voz utilizando recursos do HTML 5 juntamente com a biblioteca de JavaScript p5.js. Essa biblioteca disponibilizou funções aos quais puderam ser usadas na construção do gravador de voz presente na página de cadastro de usuário.

Para que o usuário cadastre a sua voz é necessário que o usuário acesse o site por meio de um computador que possua um microfone, e também, ao acessar a página de cadastro de usuário, libere o acesso do site a captação de áudio do microfone da máquina.

Outro requisito é que o usuário acesse a página web por meio de um dos seguintes navegadores: Chrome a partir da versão 4.0, Firefox a partir da versão 3.5, Safari a partir da versão 4.0 e o Opera a partir da versão 10.5. O navegador Internet Explorer não pode ser utilizado pois não possui suporte ao recurso áudio do HTML 5 para arquivos do formato WAV, pois esse é o formato no qual as senhas faladas são armazenadas.

Como citado no final do capítulo anterior, as senhas faladas dos usuários são armazenadas no formato WAV. Esses arquivos são salvos no serviço de nuvem S3 da Amazon. Esse serviço oferece recursos abrangentes de segurança e conformidade que cumprem até os requisitos normativos mais rigorosos, além de oferecer resiliência de 99,999999999% e armazena dados para milhões de aplicativos usados por líderes de mercado em todos os setores.

No banco de dados, na tabela de usuário, é armazenado a referência ao arquivo, ou seja, o nome dado ao arquivo de áudio armazenado no serviço de nuvem. O usuário poderá gravar apenas uma senha falada, podendo altera-la a qualquer momento via página web, realizando a sua identificação através do seu *login*, informando e-mail e senha do site.

SEGURANÇA

Para manter protegido as informações contidas no banco de dados e controlar o acesso a elas pelos usuários cadastrados no site, foi utilizado um recurso contido no *framework* Spring, chamado de Spring Security. Esse recurso permite configurações que asseguram a correta aplicação de autenticação e autorização dentro das páginas web do site.

A autenticação diz respeito a identificação dos usuários, a partir da página de login, onde o usuário deve informar o seu devido e-mail e senha, para então ter acesso ás informações do sistema. A partir do momento que ocorre a identificação do usuário é entregue a ele um código chamado de *token*, que é um conjunto de caracteres que dá acesso as respostas das requisições enviadas ao servidor, invés de ser necessário que o usuário informe e-mail e senha do site a todo momento.

Com essa barreira de segurança, o site se protege de ataques como o CSRF, onde através de *cookies*, sites maliciosos enviam requisições, não desejadas pelo usuário, ao servidor.

Outro passo de segurança presente no site é com relação a autorização. Ela diz respeito ao controle de acesso das informações pelos usuários. Ou seja, um definido tipo de usuário poderá acessar um conjunto de informações e não a sua totalidade.

Os usuários são distribuídos em três tipos diferentes: suporte, anfitrião e usuário. Esses três tipos de usuários estão contidos na tabela do banco de dados chamado grupo e possui relação com a tabela usuário, através da tabela usuário grupo. Outro vinculo que a tabela grupo possui é com a tabela permissão, através da tabela grupo permissão. Esses três tipos de conjuntos de usuários possuem permissões diferentes de acesso as páginas do site, e com isso acesso a diferentes informações contidas no banco de dados.

Mais informações referentes a permissões dadas aos três tipos de usuários serão descritas na subseção seguinte.

A senha do site pode ser alterada pelo usuário quando este não se lembra mais da mesma. Após uma tentativa inválida de *login* no sistema Web, é apresentado ao usuário

um *link*, na própria página de *login*, no qual redireciona-o a um endereço URL no qual é necessário informar apenas o e-mail cadastrado. A partir desse ponto é iniciado o processo de alteração da senha do site, no qual consiste em gravar na tabela *token reset* senha um *token* vinculado com o usuário referente ao e-mail informado. A esse e-mail é enviado o caminho URL para alterar a senha do site concatenado com o *token* gravado na base de dados. Acessando esse endereço, o usuário poderá alterar a senha do site, informando no campo indicado uma nova senha e confirmando-a.

REGRAS DE NEGÓCIO

Para que o projeto web funcionasse de forma esperada foram definidas algumas regras de negócio. Regras essas que validam as informações antes de serem inseridas no banco de dados, bem como também, permitem ou não que elas sejam acessadas de acordo com o tipo de cada usuário do sistema.

Os tipos possíveis de usuário são: suporte, anfitrião e usuário.

O tipo de usuário suporte, tem a permissão de acessar quaisquer dados de estabelecimentos, usuários, autorizações, anúncios, portas, logs e parâmetros. Ele tem a permissão de inserir, alterar, excluir, ativar e inativar estabelecimento e usuário. Além dessas funções, o usuário do tipo suporte pode também cadastrar novas portas, criando uma nova descrição e senha que serão posteriormente usadas pelos usuários do tipo anfitrião, para cadastrar em seu estabelecimento e vincular os usuários as portas por meio das autorizações. Um detalhe que é necessário ser dito é que ao ser implementado o sistema, já é inserido na tabela de dados um usuário do tipo suporte chamado de administrador.

Outro tipo de usuário, anfitrião, tem a permissão de acessar apenas os seus dados de cadastrado, onde ele pode modificar tais informações, cadastrar novas portas ao seu estabelecimento, informando corretamente o código e a senha da porta. O anfitrião pode também inserir, editar e excluir as autorizações que estão vinculadas ao seu estabelecimento e visualizar a lista de usuários cadastrados no sistema. Também pode ser feito o cadastro de anúncio, como forma de divulgação do seu estabelecimento aos usuários e verificar quais destes mostrou algum interesse. Por fim, esse tipo de usuário pode visualizar a lista de logs, que é referente ao acesso de usuários nas portas do seu estabelecimento.

O tipo usuário pode editar os seus dados cadastrados e visualizar a lista completa de usuários do mesmo tipo que estão cadastrados no sistema. Além disso, o usuário também pode verificar em quais estabelecimentos ele possui permissão de acesso. Pode visualizar os anúncios cadastrados pelos responsáveis pelos estabelecimentos, e assim, se lhe interessar algum desses, deixar marcado o seu interesse.

Veremos a seguir um tutorial com o passo a passo que os usuários do sistema devem seguir.

Primeiramente será descrito o passo a passo que os usuários devem seguir caso queiram se cadastrar como usuário do sistema. Pela página web inicial do sistema é possível

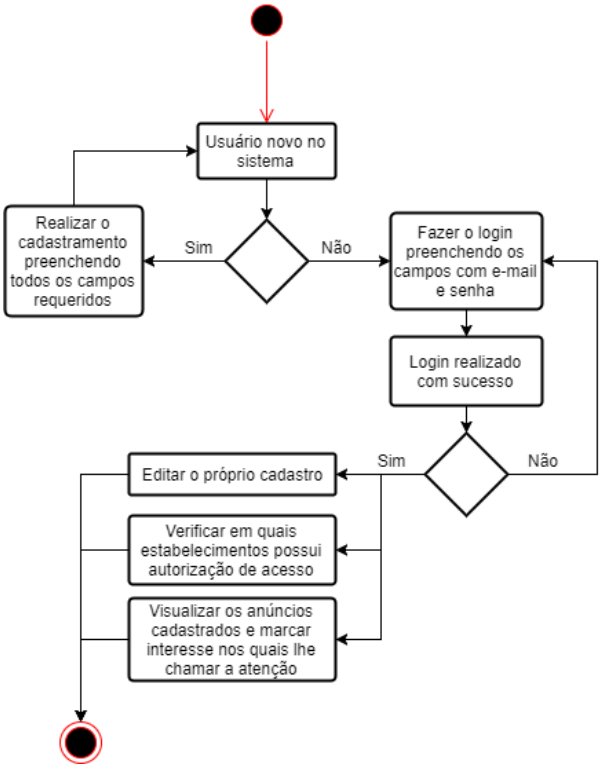
o usuário acessar o *link* chamado “Novo Usuário”, que no qual corresponde ao cadastro de novos usuários, localizado no topo da página web. Clicando nesse *link*, o usuário será redirecionado a uma outra página web, onde ele poderá se cadastrar informando os campos que estão sinalizados por asterisco (*), sendo obrigatórios os seus preenchimentos.

Após isso o usuário poderá se logar no sistema informando e-mail e senha anteriormente cadastrados e então este poderá editar o seu cadastro quantas vezes quiser e se informar a respeito dos estabelecimentos que ele possui autorização de acesso.

O usuário poderá também visualizar os anúncios cadastrados pelos responsáveis pelos estabelecimentos, e através da própria página web de anúncios marcar o seu interesse no ícone em forma de estrela. Onde posteriormente, o responsável no qual cadastrou o anúncio poderá visualizar os usuários interessados.

Segue abaixo o diagrama no qual esquematiza as ações anteriormente mencionadas.

Figura 16 – Rotinas do usuário



Fonte: Autoria própria

A seguir será descrito as ações que os usuários devem tomar caso queiram cadastrar-se como anfitrião. Pela página web inicial do sistema, no topo superior da mesma, é possui acessar o *link* correspondente a “Novo Estabelecimento”. Esse *link* redirecionará o usuário a uma outra página web que conterá os campos referentes ao cadastro do estabelecimento e dos dados do responsável pelo mesmo. Todos os campos indicados por asterisco (*) devem ser obrigatoriamente preenchidos.

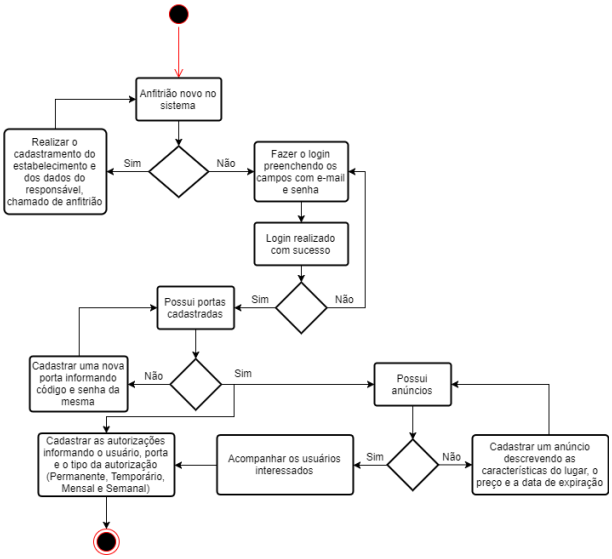
Após realizado corretamente o cadastramento do estabelecimento e dos dados

do responsável pelo estabelecimento, que será chamado aqui de anfitrião, este poderá então efetuar o login no sistema, informando o e-mail e a senha. Esse usuário, do tipo anfitrião, poderá então cadastrar as portas, informando código e senha das mesmas, e também cadastrar as autorizações, informando o usuário, a porta e o tipo de autorização, se é permanente ou temporário ou mensal ou semanal.

O responsável pelo estabelecimento poderá também cadastrar anúncios para divulgar o lugar, informando uma descrição resumida, uma descrição mais completa, o preço e a data de expiração. Após esse cadastro o responsável pelo estabelecimento poderá acompanhar os usuários, que notificaram através do site, o interesse de visitar tal estabelecimento. A partir da lista dos usuários interessados, o responsável pelo estabelecimento poderá escolher a qual deles dará permissão de acesso, cadastrando a cada um destes uma autorização.

Segue abaixo o esquemático com as ações, do usuário do tipo anfitrião, descritas anteriormente.

Figura 17 – Rotinas do anfitrião



Fonte: Autoria própria

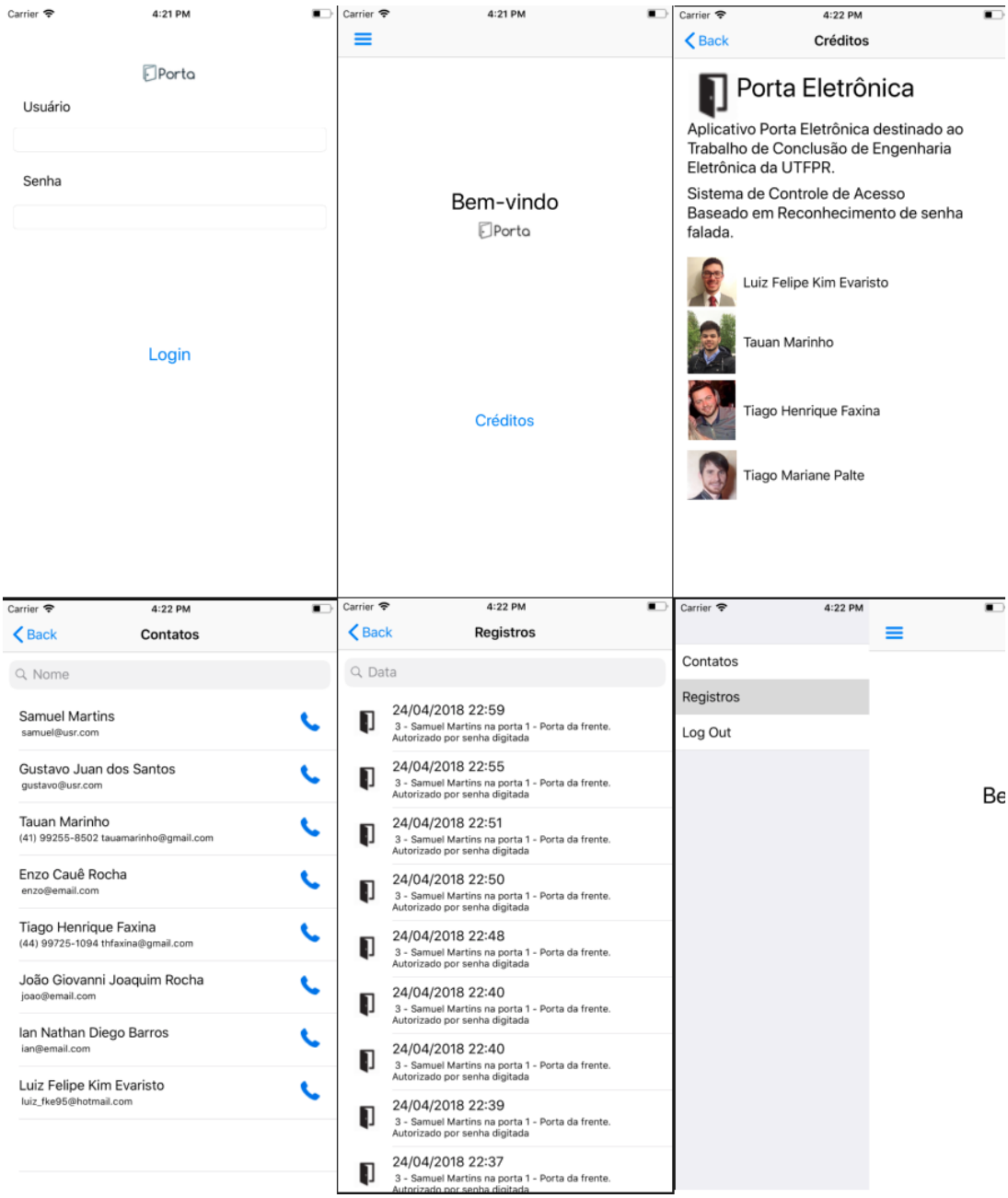
4.4.5 APLICATIVO

Com o objetivo de aumentar a interatividade e o monitoramento constante de forma fácil, foi inserido junto do sistema um aplicativo para plataformas com sistema operacional iOS. O aplicativo é direcionado apenas ao administrador do sistema. Através do e-mail e senha do administrador, o mesmo poderá fazer o login.

Após inserir o e-mail e senha corretamente, o usuário do aplicativo terá acesso as informações de registro e contatos. Em registro será possível saber o horário e data que algum usuário teve autorização, em qual porta cadastrada e se o acesso foi por senha

digita ou por voz. Nesta lista, para facilitar a pesquisa, ela é mostrada da data mais atual até a mais antiga; assim como um campo de procura, em que os registros são filtrados por data. Na área de contatos, será disponibilizado ao administrador uma lista com todos os usuários cadastrados, assim como os respectivos telefones e e-mails. Para facilitar a procura pelo usuário, há um campo de procura por nome. Abaixo segue uma imagem representando todas as telas do aplicativo.

Figura 18 – Telas do Aplicativo



Fonte: Autoria própria

COMUNICAÇÃO SERVIDOR-APLICATIVO

Seguindo os processos de segurança como no dispositivo, nenhum dados é armazenado no aplicativo, incluindo a senha do administrador. Sendo assim, todos os dados estão concentrados no banco de dados do servidor. Para as validações e obtenção desses dados, foi usado, assim como no dispositivo, o protocolo de transporte HTTP 1.1 por TCP/IP e o formato JSON.

Para a validação da senha do usuário do aplicativo, este deve inserir no campo e-mail e senha conforme, e ao pressionar o botão login, o aplicativo irá enviar uma requisição POST com os respectivos dados do cliente. Caso estes dados estejam corretos, o servidor irá responder com o JWT correspondente, caso contrário será respondido erro 401. O token recebido será importante para que o usuário se mantenha logado no aplicativo e faça as próximas requisições.

Usando o token recebido através do login, ao clicar em contatos, o aplicativo irá enviar uma requisição GET para o servidor, e caso este token esteja correto, o servidor irá responder com a lista de usuários cadastrados no estabelecimento, em JSON. Nesta lista de dados, constará o nome, telefone e e-mail de cada usuário. Da mesma forma, ao clicar na aba de registros, o aplicativo enviará uma requisição GET com o token, caso este esteja correto, o servidor enviará uma lista em JSON de data, horário e nome do usuário que acessou determinada porta por ordem de data, do mais recente ao mais antigo. O número do registros irá variar de acordo com o pedido pelo cliente, mas por padrão foi adotado 30 registros diferentes.

CASOS PARA ERROS

Por haver uma comunicação entre dois dispositivos diferentes e a parte de acesso, o aplicativo foi preparado para lidar com alguns tipos de erros. O erro mais comum será no momento do login, caso o usuário digite no campo e-mail algo diferente do padrão de um e-mail, o software irá identificar e lançará um erro, mostrando ao usuário por um pop-up que se deve inserir o e-mail. Na mesma tela de login, ao digitar a senha errada, será mostrado da mesma forma ao usuário que a senha está incorreta.

O uso de pop-up também foi adotado na parte de comunicação. Caso a conexão à internet do celular/tablet não esteja funcionando conforme, e/ou ao enviar a requisição a resposta não chegue do servidor ao aplicativo, será mostrado ao usuário que há problemas com conexão. O aplicativo é totalmente dependente de uma conexão à internet.

Para todas essas situações o usuário será informado dos problemas, evitando pensamentos equívocos, afinal, os erros não estão relacionados ao aplicativos, e sim a fatores externos.

BIBLIOTECAS UTILIZADAS

As plataformas iOS estão fortemente difundidas no mercado internacional, e devido a isso a comunidade de criação de aplicativos iOS vem crescendo. Nisto surgiu a comunidade de gerenciamento de dependências Cocoapods. É amplamente utilizado em projetos em Swift e Objective-C, com mais de 46 mil bibliotecas e sendo usado em mais de 4 milhões de aplicativos. A Cocoapods vem ajudando a tornar os softwares mais robustos e com melhor performance.

Devido aos benefícios, no projeto foram usadas as dependências Alamofire para a comunicação HTTP entre o servidor e o aplicativo. Através desta dependência, é possível enviar uma requisição com os parâmetros no header e body em JSON. A resposta do servidor é responsabilidade também. A grande vantagem de utilização de Alamofire é no momento da resposta. Caso o servidor não responda ou ocorra um problema de comunicação, o aplicativo não irá entrar em estado de erro. Em conjunto com o *pod* Alamofire, foi usado a dependência SwiftyJSON, responsável pelo parceamento do JSON, recebido com bastante facilidade. O parceamento das informações é feito não importando o tipo da variável; se adapta a todos os campos existentes em JSON.

SwiftKeychainWrapper é usada para a passagem de valores entre diferentes telas. No aplicativo em questão foi usada para gravar o JWT. Este foi amplamente usado nas telas de contato e registro, e também para manter o usuário logado através do token.

4.5 TESTES

O teste do algoritmo foi realizado em primeiro momento no software Excel, inicialmente com 200 amostras arbitrárias. Para sinais exatamente iguais, o valor obtido ao final do processo foi 1, como esperado. Testou-se então atrasos de até 5 amostras, obtendo resultados entre 0,95 e 0,98, indicando a capacidade do algoritmo de detectar sinais periódicos com atraso. Inserindo-se distorções em alguns valores, o valor do coeficiente diminuiu como esperado, mostrando que o algoritmo funciona, dependendo apenas de um limite mínimo na comparação para a determinação do índice de segurança. Posteriormente, utilizou-se amostras captadas pelo microfone associado à placa. Para pronúncias e timbres diferentes, obteve-se resultados condizentes com o esperado, indicando que o sistema funciona razoavelmente bem em situação real. Os testes com o algoritmo na placa indicaram resultados condizentes, já que os procedimentos realizados em Excel foram os mesmos a serem utilizados no servidor.

Inicialmente a ideia do projeto era incluir o algoritmo de processamento na própria placa, sendo o servidor responsável apenas por armazenar dados. No entanto, na etapa de integração das partes foi detectado o problema de falta de memória, pois o algoritmo e a comunicação necessitavam de uma quantidade maior que a disponível na plataforma, e não foi possível aumentá-la.

Assim, na tentativa de reduzir a quantidade de memória utilizada, implementou-se uma Lei de Compressão para formato WAV, conhecida como $\mu - Law$ do Codec G.711. A operação era realizada na placa, e reduziu a quantidade de memória empregada pelo armazenamento do algoritmo, no entanto, ainda não foi suficiente e piorou também o desempenho do sistema. Investiu-se na implementação do algoritmo de compressão LZW após a identificação de problemas com o volume de dados transmitidos. Os testes realizados indicaram taxa média de compressão razoável, e que permitiriam o envio de dados sem problemas.

Alternativamente, reduziu-se o tempo máximo para a senha falada, de 3 segundos para 1,5 segundos, e baixou-se a taxa de amostragem inicialmente definida em 48kHz para 8kHz, o que liberou bastante espaço em memória prejudicando pouco a performance e a eficiência do sistema. Ainda assim, trabalharia-se no limite de 256KB de RAM da placa. Por isso, finalmente, tomou-se a decisão de transferir o processamento realizado pelo algoritmo para o servidor, fazendo com que a placa ficasse responsável pelo momento inicial de sensoriamento e interface e pelo momento final de liberação de acesso. Em suma, o servidor passou a armazenar as informações de cadastros em banco, processar as requisições enviadas pela placa e também executar o algoritmo de correlação sobre o sinal captado e o sinal armazenado, e a placa tem a responsabilidade de interagir com os periféricos atrelados à plataforma e realizar o interfaceamento com o usuário.

Testes comparando sinais captados em PC com captados na placa também foram efetuados, utilizando o módulo JUnit na IDE Eclipse, já que o algoritmo foi transferido para o servidor. Resultados bastante satisfatórios foram obtidos, com coeficientes acima de 0,35 para detecção de senha correta e valores menores para senhas erradas. Tal valor é reduzido devido à interferências não resolvíveis.

Extensivamente foram realizados testes seguindo a rotina de utilização padrão do sistema, inclusive testando os diversos casos de erro previstos. Pôde-se observar a usabilidade e fácil interação de um usuário com o sistema, concluindo-se que as premissas do projeto que dizem respeito à interface e usabilidade foram cumpridas.

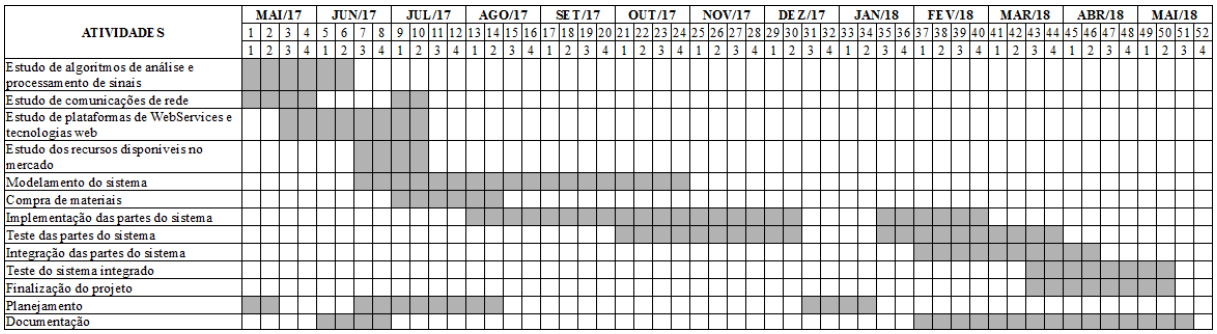
4.6 GERENCIAMENTO

A gestão do projeto foi realizada com auxílio de ferramentas e metodologias da área. Todas as operações de compra e desenvolvimento de código e hardware foram inicialmente planejadas de modo a reduzir o tempo com correções e custos adicionais. Após a execução do que foi planejado em cada procedimento, uma revisão sobre as premissas e resultados foi realizada, como forma de auditar o desenvolvimento, e quando necessário, ações de correções foram tomadas.

O sequenciamento do cronograma seguiu o que foi apresentado na proposta do trabalho. Iniciou-se com o estudo dos conceitos e aspectos para um bom embasamento teórico. Após a coleção dos conhecimentos pertinentes, as implementações iniciaram

em separado. Com as partes prontas, deu-se início à integração para a realização dos testes de validação e assim a finalização após o refino do sistema. No entanto, os prazos do cronograma não foram inteiramente cumpridos, havendo atrasos principalmente nas etapas de implementação e integração. Algumas dificuldades encontradas demoraram a ser resolvidas, majoritariamente por indisponibilidade de algum membro da equipe devido às outras disciplinas em curso, todavia não houve sobrecarga significativa. O cronograma final do projeto pode ser observado na Figura 19.

Figura 19 – Cronograma do projeto



Fonte: Autoria própria

O gerenciamento de um projeto é importante, pois apresenta uma visão ampla de tudo o que foi feito e tudo o que pode ser feito, além de prover a redução de custos financeiro e de tempo. A eficiência na implementação de um sistema só pode ser obtida com um bom planejamento e gerenciamento, como pôde ser observado no emprego prático das metodologias citadas em nosso projeto.

5 PLANO DE NEGÓCIOS

5.1 RESUMO EXECUTIVO

A segurança patrimonial é uma questão primordial e vêm ganhando força nos últimos tempos. O mercado cada vez mais pede por soluções tecnológicas que possibilitem maior controle sobre a proteção de bens, tanto materiais quanto intelectuais, além da segurança pessoal, crescendo cerca de 20% nos últimos 5 anos.

O sistema desenvolvido supre essas necessidades, através de um moderno processo de reconhecimento por voz aliado à um serviço de nuvem que permite o gerenciamento de acesso. Assim, a premissa de se possuir maior controle é cumprida, bem como o alto nível de segurança exigido pelo mercado. O segmento de controle de acesso é o segundo maior do ramo de segurança eletrônica, com 20,8%, atrás apenas da videovigilância.

O fornecimento do sistema como produto através de uma fechadura eletrônica carrega tecnologia embarcada. Já os serviços atrelados ao sistema são componentes importantes para a integração da parte física com a rede. Os parceiros e fornecedores, já consolidados e com nome no mercado, agregam ainda mais valor intrínseco ao produto e aos serviços oferecidos, permitindo receita estimada em 3,5 vezes sobre as despesas e custos. As mensalidades cobradas sobre os serviços de manutenção comporiam um fator considerável, cerca de 40% das receitas mensais projetadas.

A tecnologia à serviço das necessidades do mercado é observada no produto proposto, que provê a segurança desejada pelos consumidores aliada à uma alta capacidade de gerenciamento e controle. O sistema vem para ser um marco no segmento de segurança patrimonial, com o diferencial de ser um dos primeiros a utilizar biometria de voz como recurso.

5.2 ANÁLISE DE MERCADO

Em termos de mercado, o alvo do produto é o mercado de segurança, dentro do segmento de edificações e proteção de patrimônio. Neste mesmo segmento estão os portões com identificação via RFID, impressão digital, reconhecimento de íris, entre outros sistemas de controle de acesso. Atualmente, ainda não é comum, tampouco difundido o emprego de biometria de voz em sistemas de controle de acesso, apenas em bancos e aplicações não físicas. No Brasil, alvo primário do produto, é mais difícil encontrar concorrência com premissas parecidas, pois o mercado de tecnologia nacional ainda está em desenvolvimento.

O investimento no mercado de segurança e sua aliança com a tecnologia vêm crescendo nos últimos anos, 20,6% desde 2011, e com projeção de crescer mais 15% nos próximos 2 anos; a projeção de receitas esperadas ultrapassa os R$ 3,5 bilhões. Atualmente, os sistemas de videovigilância são responsáveis pela maior parcela do mercado de segurança,

cerca de 40%, seguidos dos sistemas de controle de acesso, com 20%, o que mostra o grande potencial de evolução do produto dentro do segmento ao qual ele foi projetado para atuar.

A clientela de um negócio como esse é composta de pessoas físicas, de classes média e alta, que desejam a segurança de suas propriedades, mas também pessoas jurídicas, públicas e privadas que necessitem de proteção de patrimônio, tal como bancos, tribunais, instituições que lidam com recursos de alto valor financeiro e intelectual. Secundariamente, o setor hoteleiro e de hospedagem é um potencial cliente para o sistema, pois empresas como o AirBnB procuram por soluções de controle de acesso gerenciável.

5.3 PROPOSTA DE NEGÓCIO

O projeto é constituído de duas partes: o sistema físico (hardware) e o sistema de serviços (software). O primeiro engloba uma plataforma eletrônica de processamento e entrada/saída de dados, uma fechadura e os sistemas de interface, todos associados à uma placa da Texas, com um microcontrolador ARM. Cada unidade possui um de cada desses componentes. Já os serviços em software contém uma página web para administração e cadastro do sistema, além do sistema de armazenamento em nuvem e servidor. A proposição de negócio construída sobre o projeto consiste na venda do sistema eletrônico componente e também o fornecimento e manutenção dos serviços de armazenamento em nuvem, sistema web e suporte técnico.

As vendas de uma ou mais unidades seriam feitas via internet, com pacotes e conjuntos, a serem pagas à vista ou parceladas. Já a manutenção e serviços de suporte possuem mensalidade ou anuidade, pois a hospedagem por parte da empresa também deve ser paga continuamente. Os serviços de entrega, instalação e manutenção deverão ser feitos por pessoal especializado, com conhecimentos técnicos do sistema, o que pode ser resolvido através de treinamentos. O atendimento de suporte e pós-venda planeja-se fazer através de chat online, principalmente, e também por telefone. A avaliação da empresa e dos serviços oferecidos, bem como a divulgação de novidades, atualizações, melhorias e promoções serão feitas via internet, que é o principal meio de comunicação da atualidade.

O negócio, por se tratar de tecnologia e inovação, tem como clientes principalmente pessoas com conhecimento da área. No segmento de segurança, é difícil encontrar oposição ao consumo, uma vez que é uma necessidade comum, individual mas mútua também.

5.4 MODELO CANVAS

Figura 20 – Modelo Canvas para o Projeto

<table>
<tr>
<td rowspan="2">Parcerias Chave
• Texas Instruments
• NXP

Fornecedores
• Amazon</td>
<td rowspan="2">Atividades Chave
• Montagem da plataforma
• Instalação e manutenção dos serviços associados
• Suporte técnico

Recursos Chave
• Equipe capacitada
• Know-how técnico</td>
<td rowspan="2">Proposta de valor
• Oferecer um sistema de controle de acesso moderno, escalável, prático e seguro.
• Uso de biometria de voz, recurso altamente diferenciado em termos de unicidade (muito difícil de copiar).
• Emprego de sistema embarcado confiável e eficiente, com a conhecida arquitetura ARM.</td>
<td rowspan="2">Relações com clientes
• SAC on-line / chat
• Avaliação periódica do sistema
• Assistência técnica
• Disponibilização de atualizações

Canais
• Canal de comunicação principal: Internet
• Secundário: Telefone
• Distribuição: Transportadora e revendedor</td>
<td rowspan="2">Segmentos de mercado
• Alvo inicial: Região Sul
• Pessoas físicas: Classes média e alta, interessadas em reforçar a segurança de seu patrimônio ou que necessitam de uma solução confiável e gerenciável.
• Pessoas jurídicas:
- Bancos
- Hotéis
- AirBnB</td>
</tr>
<tr></tr>
<tr>
<td colspan="3">Estrutura de custos
• Produção de Hardware (desenvolvimento, matéria-prima)
• Serviço Web (manutenção)
• Funcionários (P&D, técnicos, SAC, RH, Fin, Adm)
• Estrutura (Custos e contas fixas)</td>
<td colspan="2">Fontes de renda
• Venda da plataforma eletrônica (por quantidade)
• Mensalidades do serviço web (plano de pagamento variável)</td>
</tr>
<tr>
<td colspan="3">2</td>
<td colspan="2">7</td>
</tr>
</table>

Fonte: Autoria Própria

5.5 ANÁLISE ESTRATÉGICA

Na definição de possíveis estratégias comerciais para o produto, alguns aspectos de mercado e de produto foram levados em conta, apresentados nos tópicos a seguir:

- Necessidade Social:
  O projeto engloba a questão de segurança e proteção de patrimônio, necessidades primordiais para o bem-estar.
- Sistema Tecnológico Local:
  O sistema é dependente de serviço de hospedagem em nuvem, não local e dependente de fornecedores de hardware não locais.
- Capacidade de Saturação:
  Média-alta, uma vez que existem diversos outros sistemas de segurança, embora cada um com seu diferencial.
- Acesso:
  A equipe de desenvolvimento é um grupo da mesma instituição de ensino. Com relação aos fornecedores, suas operações são não-restritas no Brasil.
- Competitividade:
  Basicamente vertical (especialização e competências em processamento de voz e sistemas eletrônicos embarcados).

- Tempo de Vida:
  Alguns anos, até atualização de tecnologias de processamento e armazenamento, no entanto, o recurso primordial de análise, a voz, continua sendo único e terá cada vez mais enfoque na questão de segurança e biometria.
- Escalabilidade:
  O produto é escalável mundialmente, onde for possível ter a operação do sistema de servidor e fornecedores possam entregar os componentes.
- Legislação:
  Conformidades com o Inmetro, mas livre de regulamentação da Anatel pois não possui emissão de radiação eletromagnética ou comunicação sem fio.
- Produto de Futuro:
  Não, pois a segurança é uma necessidade básica, presente e crescente.
- Competências da Equipe:
  Sistemas eletrônicos e processamento de dados são pontos fortes da equipe, já a questão de marketing e vendas não.
- Capital e Custo de Risco: Risco médio, capital inicial moderado, porém necessidade é "constante" (existirá quando houver demanda).

5.6 AVALIAÇÃO

Com base na análise do mercado e nas premissas do produto, além da análise estratégica, conclui-se que o sistema é uma opção válida e viável para ser agregada ao segmento de segurança. Através de ferramentas foi possível verificar que o negócio proposto explora lacunas ainda não aparentes no mercado, mas que poderão no futuro ser aproveitadas.

Os potenciais clientes possuem a necessidade de um serviço como o negócio proposto. Avanços nas tecnologias permitem atender ao chamado do mercado com soluções modernas, seguras e eficientes. Acredita-se que cada vez mais sistemas como o proposto vão explorar as oportunidades presentes no mercado brasileiro contemporâneo.

6 CONSIDERAÇÕES FINAIS

Durante e após o desenvolvimento do projeto, alguns *insights* e conclusões foram gerados, atrelados aos resultados obtidos ou ao processo de desenvolvimento em si, além das relações dos mesmos com disciplinas e conteúdos pertencentes ao curso de Engenharia Eletrônica. Tais ideias são uma importante auto-avaliação a respeito do tempo e do esforço investidos na formação dos alunos envolvidos no projeto, e, a caráter informativo, servem como sumarização do trabalho realizado.

6.1 RESULTADOS

O sistema finalizado foi extensivamente avaliado em seus diversos aspectos sobre suas funcionalidades e atendimento aos requisitos previamente determinados. Algumas características de comportamento foram alteradas no decorrer da implementação do projeto, pois surgiram alguns problemas, majoritariamente técnicos, que não foram possíveis de resolver, e portanto a decisão de contorná-los com outras soluções para o sistema foi tomada, o que não comprometeu o funcionamento do sistema. Pode-se apontar que o comportamento dinâmico do sistema quando operado é intuitivo e amigável ao usuário, atendendo às imposições feitas. Tal feito foi alcançado através de um processo de melhoria contínua, reavaliando durante as implementações o desempenho e a funcionalidade de cada uma das partes do sistema, de forma a ter eficiência máxima dentro da capacidade dos desenvolvedores e das plataformas.

No âmbito funcional, o projeto teve a completa implementação de todas as funcionalidades previstas, como indexação de usuário via RFID, senha falada como objeto de validação e toda a estruturação do sistema web.

A respeito dos requisitos não-funcionais, fez-se o possível para que fossem atendidos, muito embora sejam difíceis de quantizar, sendo a avaliação de seu desempenho muito mais observacional e dependente da visão do usuário, que foi simulada pela equipe, obtendo assim resultados satisfatórios dentro do aspecto. Estima-se que o algoritmo de reconhecimento de senha falada identifique corretamente o acesso até 70% das vezes, o que indica certa robustez com relação à controle de acessos, mas ainda com espaço para melhoria. Também, nos testes finais realizados, observou-se os tempos de espera moderados e, pelo fato de o sistema estar instalado em ambiente de rede controlado, nenhum caso de perda de conexão ou *timeout* por demora de reposta do servidor. Ainda, o serviço escolhido para hospedar a parte de software do projeto esteve disponível todas as vezes em que o projeto foi testado. Assim, avalia-se finalmente que o sistema possui desempenho razoável, todas as funcionalidades propostas e atende aos diversos requisitos sugeridos.

6.2 DISCIPLINAS ENVOLVIDAS

Diversos conteúdos do curso de Engenharia Eletrônica foram de grande valia na elaboração, implementação e avaliação do projeto. Pode-se elencar as disciplinas mais relevantes no âmbito do desenvolvimento deste trabalho, observando a Tabela 2. Nota-se que boa parte das disciplinas estão contempladas, e é interessante que variam do primeiro ao último período, incluindo as optativas.

Tabela 2 – Disciplinas relevantes no âmbito do projeto e o período.

Disciplina	Período
Fundamentos de Programação 1	1
Fundamentos de Programação 2	2
Estruturas de Dados 1	3
Probabilidade e Estatística	3
Circuitos Elétricos	4
Circuitos Digitais	5
Eletrônica Básica	5
Sinais e Sistemas	5
Sensores e Atuadores	5
Microcontroladores	6
Processamento Digital de Sinais	6
Fundamentos de Comunicações	7
Semicondutores de Potência	7
Comunicações Digitais	8
Sistemas Embarcados	8
Redes de Computadores 1	9
Laboratório de PDS	9/10
Tópicos em Comunicações	9/10
Fabricação Eletrônica	9/10

Fonte: Autoria Própria

É afirmativo que muitos outros assuntos não previstos no planejamento didático-pedagógico do programa apareceram no decorrer do desenvolvimento do projeto, e nesses casos o conhecimento foi buscado em outras fontes, provando que, embora a universidade e o curso forneçam sólidos conhecimentos em muitos aspectos, estes não são suficientes por si só para o desenvolvimento de um sistema real, como o implementado.

6.3 CONCLUSÃO

Os resultados obtidos em testes e também na avaliação final do projeto mostram que o mesmo foi concebido e implementado com sucesso. Apesar do afronte causado por dificuldades principalmente técnicas, a realização do trabalho se deu de maneira satisfatória.

O desenvolvimento deste projeto foi de grande valia para a consolidação dos diversos conhecimentos adquiridos no decorrer do curso. A equipe teve a chance de realizar na prática um projeto de engenharia, com seus diversos riscos, prazos e especificações. A grande gama de conteúdos reunidos foi um fator decisivo na escolha do número de integrantes do grupo, pois áreas não relacionadas diretamente com o curso também tiveram parte no sistema. Apesar de a equipe ser incomumente maior do que a maioria dos trabalhos desse tipo, a carga de tarefas não foi pouca para nenhum dos membros, dado a vastidão de funcionalidades e requisitos a serem atendidos pelo sistema.

A dedicação dos alunos e mais ainda a dedicação dos professores é recompensada com o sucesso de um trabalho como o desenvolvido, onde pode-se observar que a essência da educação é coroada com a aplicação prática e honesta de suas premissas. As abordagens do aprendizado no decorrer do curso hoje são vistas como maneiras distintas de apresentar os diferentes aspectos da função de um engenheiro, que é variada e múltipla, mas que no seu cerne é projetar, desenvolver, implementar e acompanhar soluções para os mais distintos problemas, sejam simples ou complexos, e assim levar a sociedade a uma patamar mais tecnologicamente e humanamente desenvolvido . A engenharia é uma arte que exige investimento e atualização contínuos, e é fundamental para o progresso.

Como o intuito de um Trabalho de Conclusão de Curso de Engenharia é a concretização dos inúmeros aspectos educacionais componentes do programa de formação, pode-se inferir que este objetivo foi alcançado. Não apenas como mero requisito para obtenção de diploma, o trabalho desenvolvido foi de importância sumária para a observação prática dos conhecimentos teóricos adquiridos no decorrer da formação da equipe. Finalmente, é impossível discordar que este trabalho foi a contribuição majoritária e essencial à esta etapa do contínuo processo de aprendizado dos alunos envolvidos.

Referências

ANUSHA. **Basics of Serial Peripheral Interface (SPI)**. 2017. Disponível em: <http://www.electronicshub.org/basics-serial-peripheral-interface-spi>. Acesso em: 8 de Agosto de 2017. Citado na página 15.

ARM. **ARM Architecture**. 2017. Disponível em: <https://developer.arm.com/products/architecture>. Acesso em: 12 de Setembro de 2017. Citado na página 17.

BOKER, S. M. et al. **Windowed Cross-Correlation and Peak Picking for the Analysis of Variability in the Association Between Behavioral Time Series**. Psychological Methods Vol. 7 No. 3, Estados Unidos, p. 338–355, 2002. Citado na página 4.

CANDYHOUSE. **Sesame**. 2015. Disponível em: <https://candyhouse.co/apps/help-center>. Acesso em: 7 de junho de 2017. Citado na página 3.

CORELIS. **SPI Interface**. 2017. Disponível em: <https://www.corelis.com/education/SPI_Tutorial.htm>. Acesso em: 8 de Agosto de 2017. Citado na página 16.

FILIPEFLOP. **Display LCD 20x4 com Backlight Azul**. 2017. Disponível em: <https://www.filipeflop.com/produto/display-lcd-20x4-backlight-azul>. Acesso em: 26 de Janeiro de 2018. Citado na página 26.

HAYKIN, S.; VAN VEEN, B. **Signals and Systems**. 1. ed. New York: John Wiley and Sons, 1999. Citado na página 8.

INTERNATIONAL STANDARD ISO/IEC. **ISO/IEC 14443-3**: Identification cards, contactless integrated circuit(s) cards, proximity cards: Initialization and anticollision. Austin, 1999. 48 p. Disponível em: <https://nfc-wisp.wikispaces.com/file/view/fcd-14443-3.pdf>. Citado na página 28.

KENNEY, J. F. **Mathematics of Statistics Part One**. 4. ed. London: Chapman and Hall Ltd., 1939. Citado na página 11.

KRASHENINNIKOV, V. R. et al. **Cross-Correlation Portraits of Voice Signals in the Problem of Recognizing Voice Commands According to Patterns**. Pattern Recognition and Image Analysis Vol. 21 No. 2, Rússia, p. 193–194, 2011. Citado na página 4.

LACANETTE, K. **A Basic Indroduction to Filters**. National Semiconductor Application Note 779, Estados Unidos, p. 1–22, 1991. Citado na página 7.

MALIK, B. **SPI Communication Using PIC Microcontroller**. 2016. Disponível em: <http://microcontrollerslab.com/spi-communication-pic-microcontroller>. Acesso em: 8 de Agosto de 2017. Citado na página 15.

MONTALVÃO FILHO, J. R. et al. **Desenvolvimento de Uma Fechadura Eletrônica Baseada em Reconhecimento Vocal de Usuário (via Redes Neurais Artificiais)**. Laboratório de Automação e Controle, Universidade Tiradentes - UNIT, Aracaju, SE, 2003. Citado na página 3.

NXP SEMICONDUCTORS N.V. **MF1S50yyX/V1**: Mifare classic ev1 1k: Mainstream contactless smart card ic for fast and easy solution development. Austin, 2014. 40 p. Disponível em: <https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf>. Citado na página 28.

NXP SEMICONDUCTORS N.V. **MFRC522**: Standard performance mifare and ntag frontend. Austin, 2016. 95 p. Disponível em: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>. Citado na página 27.

ON SEMICONDUCTOR. **Plastic Medium-Power Complementary Silicon Transistors**: Datasheet. Arizona, 2014. 12 p. Disponível em: <https://www.onsemi.com/pub/Collateral/TIP120-D.PDF>. Citado na página 30.

PETRUZELLA, F. D. **Controladores Lógicos Programáveis**. 4. ed. New York: Niagara University, 2011. Citado na página 30.

PROAKIS, J. G.; SALEHI, M. **Communication Systems Engineering**. 2. ed. New Jersey: Prentice Hall, 2002. Citado na página 8.

PUTH, M.; NEUHÄUSER, M.; RUXTON, G. D. **Effective Use of Pearson's Product-Moment Correlation Coefficient**. Animal Behaviour 93, Grã-Bretanha, p. 183–189, 2014. Citado na página 4.

SAVULEA, D.; CONSTANTINESCU, N. **Statistical Correlation Study**. Annals of the University of Craiova Vol. 37, Romênia, p. 35–51, 2010. Citado na página 4.

SEGRETTI, R. **A expressão "abre-te Sésamo" realmente poderá abrir portas**. TecMundo Software, 2015. Disponível em: <https://www.tecmundo.com.br/apps/75865-expressao-abre-te-sesamo-realmente-abrir-portas.htm>. Acesso em: 31 de maio de 2017. Citado na página 3.

SKLAR, B. **Digital Communications: Fundamentals and Applications**. 2. ed. New Jersey: Prentice Hall, 2001. Citado na página 12.

SMITH III, J. O. **Introduction to Digital Filter Theory**. Digital Audio Signal Processing: An Anthology, Estados Unidos, p. 1–59, 1985. Citado na página 8.

SMITH, S. W. **The Scientist and Engineer's Guide to Digital Signal Processing**. 2. ed. San Diego: California Technical Publishing, 1999. Citado 5 vezes nas páginas 3, 8, 9, 10 e 11.

SPIEGEL, M. R.; STEPHENS, L. J. **Theory and Problems of Statistics**. 3. ed. New York: Schaum's Outline, McGraw-Hill, 1999. Citado na página 11.

STEIN, J. Y. **Digital Signal Processing: A Computer Science Perspective**. 2. ed. New York: John Wiley and Sons, 2000. Citado 2 vezes nas páginas 3 e 12.

STMICROELECTRONICS. **Positive voltage regulator ICs**: Datasheet. Genebra, 2014. 57 p. Disponível em: <http://users.ece.utexas.edu/~valvano/Datasheets/L7805.pdf>. Citado na página 32.

TANENBAUM, A. S. **Computer Networks**. 4. ed. Amsterdam: Prentice Hall, 2011. Citado na página 17.

TEXAS INSTRUMENTS INC. **Tiva TM4C129ENCPDT Microcontroller**: Datasheet. Austin, 2014. 2011 p. Disponível em: <http://www.ti.com/lit/ds/symlink/tm4c129encpdt.pdf>. Citado 2 vezes nas páginas 22 e 24.

TEXAS INSTRUMENTS INC. **TivaWare Peripheral Driver Library**: User's guide. Austin, 2016. 704 p. Disponível em: <http://www.ti.com/lit/ug/spmu298d/spmu298d.pdf>. Citado 2 vezes nas páginas 33 e 35.

TEXAS INSTRUMENTS INC. **TM4C Series TM4C129E Crypto Connected LaunchPad Evaluation Kit**: User's guide. Austin, 2016. 32 p. Disponível em: <http://www.ti.com/lit/ug/spmu372a/spmu372a.pdf>. Citado 3 vezes nas páginas 22, 24 e 31.

TEXAS INSTRUMENTS INC. **TI E2E Community**. 2018. Disponível em: <https://e2e.ti.com/>. Acesso em: 04. Citado na página 25.

TUBBS, J. D. **A Note on Binary Template Matching**. Pattern Recognition Vol. 22 No. 4, Grã-Bretanha, p. 359–365, 1989. Citado na página 4.

VILLA REAL, L. C.; HEINEN, F. J.; DE OLIVEIRA, L. P. L. **Autenticação de Senhas Faladas Dependente de Usuário**. IV Workshop sobre Software Livre, São Leopoldo, RS, p. 99–102, 2003. Citado na página 4.