UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA ELECTRÓNICA

PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E *INTERFACE WEB*

José Catine Munguambe Júnior

Supervisores:

Supervisor da Faculdade: Eng.º Edson Camilo Fortes

Supervisor da Instituição: Sr. Celso Langa

Maputo, Abril de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E INTERFACE WEB

José Catine Munguambe Júnior

Supervisores:

Supervisor da Faculdade: Eng.º Edson Camilo Fortes

Supervisor da Instituição: Sr. Celso Langa

Maputo, Abril de 2022

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

AVALIAÇÃO DOS SUPERVISORES

Autor: José Catine Munguambe Júnior

PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E *INTERFACE WEB*

Supervisor da Faculdade **Nota**

_____ _____

(Eng.º Edson Camilo Fortes)

Supervisor da Instituição **Nota**

_____ _____

(Sr. Celso Langa)

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉNICA

TERMO DE ENTREGA DE RELATÓRIO DO ESTÁGIO PROFISSIONAL

Declaro que o estudante: José Catine Munguambe Júnior

Entregou no dia ___/___/20__ as __ cópias do relatório do seu relatório do estágio profissional com a referência: _____

Intitulado: PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E *INTERFACE WEB*

Maputo, ____ de _____ de 20__

O Chefe de Secretaria

_____

DEDICATÒRIA

A Melta Munguambe e José Munguambe, meus pais que conduziram e incentivaram a minha educação formal.

AGRADECIMENTOS

Agradeço à Melta Munguambe e José Munguambe, meus pais, que me deram apoio e incentivo nas horas difíceis. Sou grato também ao meu amigo Nilton Madade e meu tio Manuel Munguambe, que não me deixaram ser vencido pelo cansaço. Meus agradecimentos aos irmãos, sobrinhos, tios e avos, que de alguma forma também contribuíram para que o sonho da faculdade se tornasse realidade. Por fim, agradeço imensamente à Deus, por ter - me concedido saúde, força e disposição para fazer a faculdade e o trabalho de final de curso. Sem Ele, nada disso seria possível. Sou grato também ao senhor por ter dado saúde aos meus familiares e tranquilizado o meu espirito nos momentos mais difíceis da minha trajectória académica ate então.

EPIGRAFE

“Aquele que não é capaz de governar a si mesmo, jamais governará os outros”

Samora Machel

RESUMO

Nos últimos anos, tem sido uma tendência a utilização de tecnologias de segurança electrónica no dia-a-dia do ser humano, em diversos sectores e áreas da sua vida. Este projecto tem como objectivo desenvolver um sistema de controlo de acesso por RFID com recursos avançados a um custo reduzido (Custo de material 1879,00 Mtn e custo de instalação 700,00Mtn) no Bloco Operatório do HCM, como a capacidade de controlar vários sectores por Wi-Fi, facilitar actualização de dados de usuários no banco de dados, possuir um servidor, interface baseada em página web. A maioria dos sistemas disponíveis no mercado carecem desses recursos avançados. Este sistema é indispensável, pois bloqueia o acesso de pessoas não autorizadas, regista e organiza no banco de dados todas as operações realizadas no sistema (identificação, tipo de operação, permitida ou negada, data e hora), facilita a entrada e saídas e auxiliar o sector de Recursos Humanos por trazer informações sobre a jornada de trabalho de cada colaborador. O protótipo foi submetido a testes e verificou-se a eficácia dos algoritmos propostos no sistema.

Palavras-chave: Controlo, RFID, Dados, HCM

ABSTRACT

In recent years, there has been a trend towards the use of electronic security technologies in the daily life of human beings, in different sectors and areas of their lives. This project aims to develop an RFID access control system with advanced features at a reduced cost (material cost 1879.00 Mtn and installation cost 700.00 Mtn) in the HCM Operating Block, such as the ability to control various sectors via Wi-Fi, facilitate updating of user data in the database, have a server, web page-based interface. Most systems available on the market lack these advanced features. This system is essential, as it blocks the access of unauthorized persons, registers and organizes in the database all operations carried out in the system (identification, type of operation, allowed or denied, date and time), facilitates entry and exits and assists the Human Resources sector for providing information on the working hours of each employee. The prototype was tested and the effectiveness of the algorithms proposed in the system was verified.

Keywords: Control, RFID, Data, HCM

Índice

Índice de Figuras

Índice de Tabelas

Listas de Abreviaturas

API	*Application Programming Interface* (Interface de Programação de Aplicativos);
HCM	Hospital Central de Maputo;
RFID	*Radio Frequency Identification* (Identificação por Radio Frequência);
IoT	Internet of Things (Internet das Coisas);
PHP	*Hypertext Preprocessor* (pré-processador de hipertexto);
IHM	Interface Homem Máquina;
UTL	Universal Tecnologies Limitada;
CCTV	*Closed – circuit television* (Circuito Fechado de Televisão);
HTML	*HyperText Markup Language* (linguagem de Marcação de Hipertexto);
DHTML	*Dynamic HTML* (HTML Dinâmico);
CSS	*Cascading Style Sheet* (Folhas de estilos de cascatas);
LCD	*Liquid Crystal Display* (Tela de Cristal Liquido);
XML	*EXtensible Markup Language;*
CGI	*Interface de Gateway comum;*
SSI	*O Server Side Includes;*
ASP	*Active Server Pages;*
PHP	*Hypertext Preprocessor;*
ISAPI/NSAPI	*Information Server Application Programming Interface;*
JSP	*Java Server Pages;*
SPI	*Serial Peripheral Interface;*
I2C	*Inter – integrated Circuits* (Circuito Inter – intregado).
SQL	*Standard Query Language*

Capitulo I

1. Introdução

1.1. Contextualização

Sempre foi problema da sociedade a necessidade de ter segurança no meio em que se vive, não somente em relação à segurança pessoal, mas também de manter um local seguro quando não se está nele ou próximo o suficiente para tê-lo em vista (Cardoso, 2014 *apud* Gonçalves, 2019).

Além da necessidade de manter um local seguro também é necessário ter o controlo sobre determinados sectores, sendo possível o acesso somente por pessoas com autorização previamente declarada (Gonçalves, 2019).

“Estas soluções já conhecidas como portas e fechaduras resolvem o problema de manter um local seguro, mas elas não fornecem a solução do controle de acesso”. (Cardoso, 2014 *apud* Gonçalves, 2019).

Nos dias actuais para identificação automática de objectos ou pessoas a tecnologia RFID é mais usado devido ao seu custo reduzido e melhorias em seu funcionamento. RFID é uma tecnologia que permite a transferência de informações sem fio através de campos electromagnéticos, com um propósito de identificar ou rastrear objectos que possuam algum dispositivo RFID presente (Guimarães, 2013).

Com o avanço das tecnologias as informações que levavam horas, dias, meses ou até anos para chegar, são entregues em questões de milissegundos, com isso, surge a possibilidade de criar um sistema de controlo de acesso e monitoramento em tempo real, envolvendo grande fluxo de dados transferidos em milissegundos através da *internet* das coisas (*Internet Of things*).

O presente trabalho tem como objectivo desenvolver uma proposta de um sistema de controlo de acesso em áreas restritas do bloco operatório do hospital central de Maputo usando autenticação por RFID e gerenciamento por meio de *software web.* Será feita a integração de um sistema embarcado que será responsável por colectar a informação de um usuário e enviar essa informação para um *software* que realiza todo o gerenciamento do controlo de acesso de usuários, permitindo ou não o usuário ter o

acesso ao local e salvando todo seu histórico em banco de dados para que um supervisor tenha controlo sobre seus colaboradores.

1.2. Definição do Problema

A pandemia do novo Coronavírus Covid 19 impactou o mundo inteiro. Enquanto alguns locais fecham, outros vêem sua demanda aumentar significativamente (Intelbras, 2021).

Que é o caso do Hospital Central de Maputo. Desde aparição de Covid-19 (20 de Março de 2020) o Hospital tem visto o fluxo de pessoas aumentar, o que consequentemente requer um aumento da segurança.

O bloco operatório é um sector com acesso limitado e divido em três áreas nomeadamente área irrestrita (secretaria, vestiários, área de transferência, corredor de entrada), área semi - restrita (salas de estar, descanso e de preparo do material) e áreas restritas (salas cirúrgicas, de recuperação pós-anestésica e corredor interno), por conta disso necessita de um sistema de controlo de acesso físico que atenda o previsto no regulatório Nacional do Sistema de Saúde.

O monitoramento em tempo real de entradas e saídas nessas instituições é complexo, há áreas que a entrada é permitido a um determinado grupo (Funcionários e emergências). Isso faz com que cada área esteja protegida da forma mais adequada, resguardando equipamentos e dados críticos.

A falta de um controlo de acesso bem estruturado em hospitais os torna sujeitos a uma série riscos. Alguns exemplos são o roubo de medicamentos, saídas de pacientes sem autorização médica, entrada de pessoas não autorizadas.

1.3. Relevância da pesquisa

Nos últimos anos, tem sido uma tendência a utilização da tecnologia no dia-a-dia do ser humano, em diversos sectores e áreas da sua vida. No que diz respeito à tecnologia de Controlo de Acesso, a segurança Electrónica tem muito a somar neste segmento, pois disponibiliza soluções modernas e eficientes para uma rotina mais tranquila tanto para profissionais da saúde, quanto para pacientes e visitantes

O controlo de acesso no Bloco Operatório da HCM é indispensável, para evitar que certo grupo de pessoa tenha acesso a áreas restritas. Este sistema ira facilitar entradas

e saídas e auxiliar o sector de Recursos Humanos por trazer informações sobre a jornada de trabalho de cada colaborador.

1.4. Objectivos

1.4.1. Objectivo Geral

Desenvolver uma proposta de um Sistema de controlo de Acesso em Área restrita do Bloco Operatório do Hospital Central de Maputo usando autenticação por RFID e *Interface WEB*

1.4.2. Objectivos Específicos

- Desenvolver um protótipo de um sistema embarcado de fechaduras electrónicas integrado leitores de Rfid e Lcd;
- Desenvolver um Sistema *Web* para o monitoramento;
- Aplicar o *Servidor Microsoft SQL* para de Base de dados;
- Possibilitar o Registo permanente de Entradas e Saídas;
- Explicar o princípio de funcionamento do Sistema de controlo de Acesso.

1.5. Justificativa

O âmbito da escolha do tema surgiu numa experiência pratica no HCM que UTL presta serviços de automatização das portas do Banco de Socorro, que esta em reabilitação e requalificação total. O aspecto desmotivador para aquisição de um sistema de controlo de acesso é o seu alto preço, e alguns deles não dispõem de recursos avançados como permissões de agendamento, capacidade de controlar vários sectores *por Wi-Fi,* facilitar actualização de dados de usuários no banco de dados, possuir um *hardware* externo (como servidores), *interface* baseada em página web e muitos outros. Desta forma, pretende-se desenvolver um Sistema de Controlo de Acesso que contenha todas as funcionalidades mencionadas, mantendo um preço abaixo, com o uso da tecnologia *IoT* para permitir a integração com outros sistemas e baseado em *Wi-Fi.*

A tecnologia RFID se tornou uma maneira fácil e barata de identificar usuários. Além disso, a área de Sistemas de Controlo de Acesso tem grande importância na actualidade, quando questões envolvendo privacidade e segurança estão em alta. Para resolver esse problema de privacidade e segurança a maior parte das empresas tem adoptado esses tipos de sistemas de segurança.

1.6. Metodologia

Este projecto baseia - se numa pesquisa aplicada que visa a aplicar conhecimentos na área de Segurança Electrónica. Pretende – se fazer uma abordagem quantitativa de dados já existentes, pesquisa explicativa de como se beneficiar com uso do Sistema de controlo de Acesso. A técnica aplicada obedeceu o esquema abaixo.

- Pesquisa bibliográfica;
- Pesquisa documental;
- Observação;
- Estudo de Caso;
- Estudo de campo;
- Escolha de Materiais e Tecnologias Envolvida.

1.7. Estrutura do trabalho

A estrutura do trabalho se divide nos seguintes capítulos: O Capítulo I (Introdução) expõe uma breve Contextualização, Definição do Problema, Relevância da pesquisa, Objectivos, Justificativa, Metodologia e Estrutura do trabalho. No Capítulo II (Actividades realizadas no estágio) será apresentada a instituição em que o estágio profissional foi realizado, também as áreas onde o estágio foi realizado. No Capítulo III (revisão de literatura) apresenta-se tópicos importantes para a resolução do problema. O Capítulo IV (Caso de estudo) expõe os resultados de estudo de caso e fala-se de forma detalhada, sobre o Hospital Central de Maputo. O Capítulo V (Proposta de solução) propõe-se a solução para o problema estudado no presente trabalho. No Capítulo VI (Análise e discussão de resultados) procede-se a discussão dos resultados encontrados depois da resolução do problema. No Capítulo VII (Considerações finais) avalia-se o cumprimento dos objectivos do trabalho e propõe-se recomendações para trabalhos posteriores. Bibliografia nesta parte do trabalho estão apresentadas as obras bibliográficas citadas ou não no trabalho. Anexos, procede-se a apresentação de elementos adicionais que facilitem a compreensão do trabalho.

Capítulo II

2. Actividades realizadas no estágio

2.1. Considerações Iniciais

O estágio profissional teve duração de 5 meses, na Universal Technologies limitada, referir ainda que durante a sua estadia o estudante foi integrado nas equipas de trabalho presentes de diferentes obras onde a empresa desenvolve trabalho, a tabela 1 mostra de uma forma resumida as actividades realizadas pelo estudante na empresa.

Tabela 1: Cronograma de Actividades de Actividades do Estudante

Cronograma de Actividades			
Actividades	**Subáreas**	**Data de Início**	**Data de Conclusão**
Instalação e Manutenção de Sistemas	Vedação Eléctrica	16/08/2021	20/08/2021
	CCTV	23/08/2021	03/09/2021
	Incêndios/Extinção	06/09/2021	18/09/2021
	Alarme	20/09/2021	01/10/2021
	Controlo de Acesso	03/10/2021	23/10/2021
Consultoria	Análise e Gestão de Projectos	25/10/2021	26/11/2021
Instalação e Manutenção de Sistemas	Controlo de Acesso e Portões Automáticas	29/10/2021	14/01/2022

Fonte: Autor

2.2. Apresentação da Universal Technologies Limitada

A UTL é uma empresa Moçambicana especializada na concepção, gestão, consultoria, fornecimento, instalação e manutenção de sistemas avançados de segurança electrónica e informática. Localizada na avenida Eduardo Mondlane, bairro Central, nº. 1942, 1º Andar, Flat 2. Tem como missão busca de soluções electrónicas e informáticas para garantir a satisfação dos seus clientes.

A operar em Moçambique desde novembro de 2009, a *UTL* tem como principais fornecedores a *Elvey Security Technologies SA, Amco, Nemtek SA, Reditron SA, IDS e GE Security SA*, empresas que operam no mercado Sul-africano a mais de 35 anos.

As actividades da empresa Estão vocacionada para as obras de pequena, media e grande dimensão, como: Hospitais, Bombas, Bancos, Hotéis, Edifícios de Escritórios, Armazéns, Industrias, Lojas e Centro comercial.

A *UTL* possui uma equipe de consultores Seniores (Arquitectos, Engenheiros Electrónicos e de Informática), com elevada experiência na concepção e implementação de projectos e sistemas diversificados nas áreas de tecnologias de sistemas integrados de segurança electrónica. De salientar que estes sistemas permitem receber a qualquer momento novos recursos, integrando-os com os existentes para melhorar a sua qualidade de vida e tirar máximo proveito dos recursos disponíveis. Pode-se observar na figura 1 o organograma da empresa.

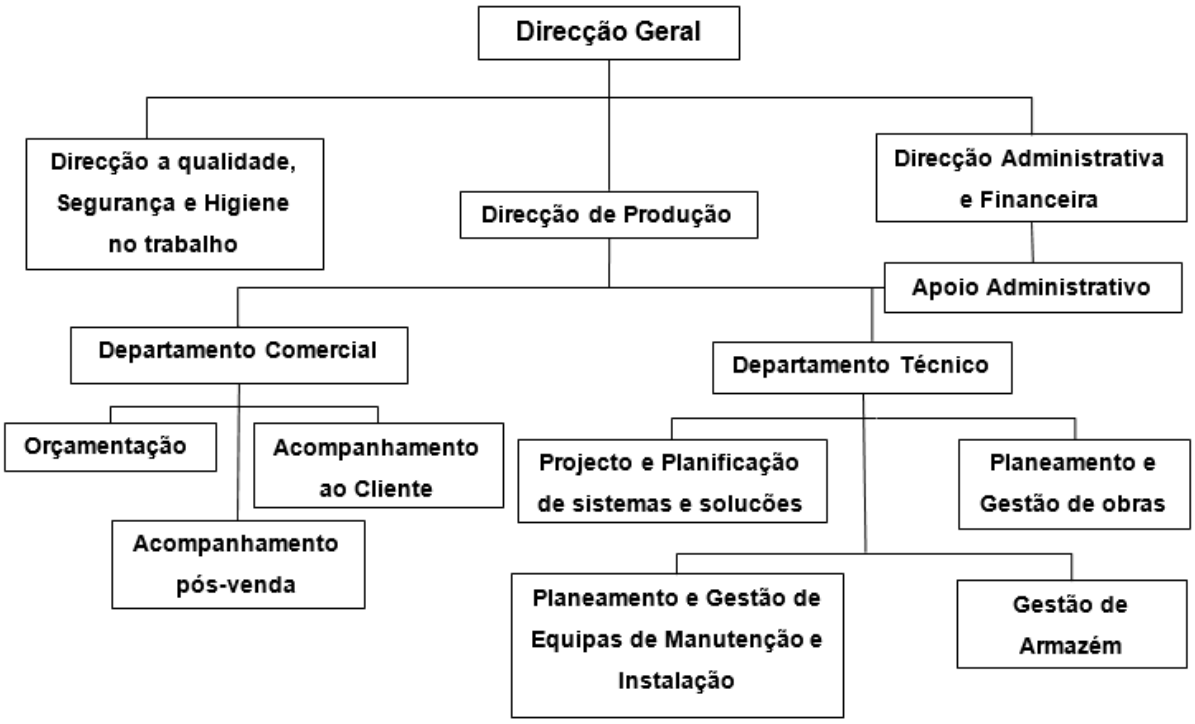


Figura 1: Organograma da Empresa

Fonte: Autor.

Capítulo III

3. Revisão de Literatura

3.1. Sistemas de Controlo de Acesso

Os sistemas de controlo de acesso electrónico são redes digitais que controlam o acesso aos portais de segurança. Um portal de segurança é uma entrada ou saída de um limite de segurança (Norman, 2017).

A maioria destes sistemas tem como funções principais o Registo automático de entradas e saídas, Alarme em caso de entrada forçada em zonas com acesso condicionado, Definição de áreas de acesso, Definição de direitos de acesso por área, Definição de horários de acesso, Definição de percursos de acesso, Seguimento e localização (Gomes, 2010).

Além das funções acima referidas oferece as seguintes vantagens: segurança, fiabilidade, conforto, flexibilidade e integração. A figura 1 mostra a arquitectura geral de um sistema de controlo de acesso.

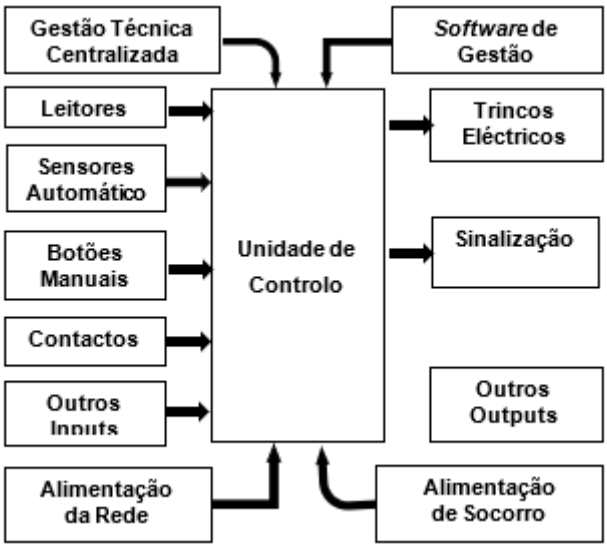


Figura 2: Constituição geral de sistema de controlo de acessos.

Fonte: *(Gomes, 2010)*

Unidade de Controlo

A Unidade de Controlo é o “cérebro” do sistema. É neste equipamento que são ligados todos os periféricos (leitores, sensores, botões, trincos eléctricos) e a partir do qual sairá, ou não, uma ordem de abertura, dependendo das definições de acessos e da

validade dos dados recebidos pelos elementos periféricos. Os sistemas de controlo de acessos dividem-se em dois grupos principais: Sistemas em Rede e Sistemas *Stand Alone* (Gomes, 2010).

Leitores

Os Leitores são o meio de interacção do utilizador com o sistema. Podem ser de diversos tipos: Teclado, Banda Magnética, Proximidade, Códigos de barras, Ópticos e Biométricos (leitura da íris, impressão digital) (Gomes, 2010).

A figura 3 mostra um exemplo de leitor de sistema de controlo de acesso, este leitor possui mais de duas tecnologias (Proximidade, Teclado e Biometria).

Figura 3: Leitor de sistema de Controlo de Acesso

Fonte: (Intelbras, 2021)

Proximidade: possuem uma antena que emite um sinal que é captado pelos dispositivos de proximidade. Em resposta ao sinal recebido, estes dispositivos enviam um código ao elemento receptor do leitor de proximidade que, por sua vez, o transmite ao sistema. Estes leitores utilizam tecnologia RFID para comunicar com as respectivas chaves de acesso. Existem dispositivos de proximidade que também podem alterar as informações contidas nas chaves de acesso, nos quais se incluem os leitores do tipo *MIFARE* (APSEI, 2018).

Cartões de Banda Magnética: possuem uma ranhura, para passagem do cartão, e uma cabeça de leitura apropriada que, durante a passagem do cartão, lê o código que está na banda magnética e o transmite ao sistema (APSEI, 2018).

Biométricos: dispositivos com capacidade de reconhecer as características referenciais que caracterizam os utilizadores (os dados biométricos mais utilizados são as impressões digitais, o padrão da íris, a geometria da mão, a voz e as características da face). O leitor biométrico mais conhecido é o leitor de impressões digitais. Este leitor é constituído por uma superfície, onde é colocado o dedo cuja impressão digital se quer analisar, que contém um sensor capacitivo ou óptico que consegue extrair os detalhes da impressão digital e processá-los internamente através de algoritmos apropriados (APSEI, 2018).

Teclados: servem para introduzir Códigos de Identificação Pessoal, podendo ser utilizados isoladamente ou em conjunto com outro tipo de leitor (APSEI, 2018).

Contactos

São os elementos de informação do estado do sistema. Podem ser de dois tipos: Magnéticos e Mecânicos (Gomes, 2010).

Botões Manuais

São utilizados normalmente como elementos de saída, quando não se justifique a utilização de leitores nos dois lados das portas. Estes botões quando pressionados, actuam um contacto que vai gerar o pedido de abertura à central de controlo de acesso (Gomes, 2010).

Trincos Eléctricos

São as fechaduras do sistema. Permitem, para utilizadores autorizados, a abertura das portas e o acesso aos espaços (Gomes, 2010).

Alimentação Do Sistema

A alimentação de energia eléctrica do sistema em condições normais de funcionamento deverá ser realizada através da rede de energia eléctrica devendo para o efeito ser prevista uma alimentação vinda do Quadro Eléctrico da instalação. O sistema deverá ainda ter uma alimentação própria de socorro que garanta o seu funcionamento em caso de falha da alimentação normal da rede (Gomes, 2010).

***Softwares* de Gestão**

Destinam-se, essencialmente, a controlar e gerir a totalidade do sistema de controlo de acessos a partir de um ou diversos postos. Através de interfaces gráficas, o utilizador, gere de uma forma simples e intuitiva a totalidade do (s) sistema (s) (Gomes, 2010).

Para além da gestão e supervisão de funcionamento dos sistemas que recebe, permitem a geração de relatórios com os eventos recebidos pelo sistema, tornando-se numa ferramenta muito útil para gestores e responsáveis de empresas e entidades (Gomes, 2010).

Gestão Técnica Centralizada

A Gestão Centralizada consiste na integração dos diversos sistemas existentes numa instalação para que o seu comando, controlo e operação possam ser realizados de uma forma centralizada num sistema de gestão (Gomes, 2010).

A gestão centralizada normalmente só é utilizada em instalações grandes e complexas, de forma a facilitar o comando, controlo e operação dos diversos sistemas (Gomes, 2010).

3.2. Tecnologia RFID

RFID é uma tecnologia baseada na autenticação/identificação de objectos ou pessoas, através de ondas electromagnéticas de radio. RFID é uma tecnologia de comunicação sem fio que é capaz de identificar objectos ou pessoas através da utilização de etiquetas de identificação única (Costa, 2018).

O sistema RFID é composto por três componentes nomeadamente Leitor, *Tags e Hosts.*

3.2.1. Componentes de um Sistema RFID

A Figura 4 mostra um sistema completo de RFID apresentando um *Hosts* ligado a um leitor e antena se comunicando com uma *tag* contendo um identificador. O leitor utiliza uma antena que emite ondas electromagnéticas a um raio de alcance definido de acordo com a frequência de operação utilizada. Essas ondas energizam a tag que emite um sinal com o conteúdo armazenado em sua memória que é captado de volta pelo leitor (Bhuptani; Maradpour et al 2005 *apud* Losi, 2015).

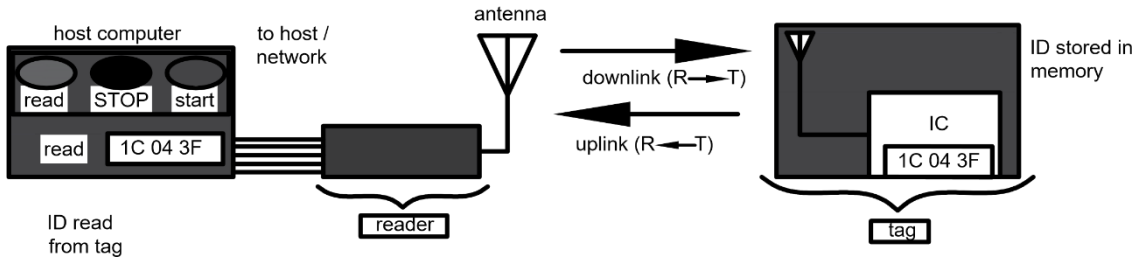


Figura 4: Sistema de Identificação por Radio Frequência.

Fonte: (Dobkin 2013 apud Losi, 2015)

Tags

Tag RFID é um pequeno dispositivo electrónico que recebe uma transmissão do leitor RFID e transmite um sinal contendo suas informações. *Tag* RFID é um pequeno dispositivo de transmissão de ondas de radio que também pode ser referido como transponder, *smart tag*, que é constituído de silício, muitas vezes menor que um milímetro, que por sua vez são conectados a uma antena geralmente em formato de bobina (Guimarães, 2013).

As tags RFID podem ser activas ou Passivas. A figura 5 mostra um exemplo de *Tag* RFID. As *Tags* passivas não precisam de uma fonte de alimentação própria para seu funcionamento, com isso possui um tamanho reduzido. As tags passivas são produzidas a um custo menor pois elas não necessitam de fonte de energia própria, já que utilizam energia electromagnética emitida pelo leitor e por isso também tem o alcance mais limitado, algo em torno de 10 centímetros (Losi, 2015).

As tags activas custam mais pois possuem sua própria fonte de energia interna o que permite alcances maiores, em torno de 10 a 30 metros, e podem transmitir o sinal a qualquer momento sem depender do leitor (Bhuptani; Maradpour et al 2005 *apud* por Losi 2015).

Figura 5: Exemplo de Tag RFID

Fonte: *(Losi, 2015)*

Leitor

O Leitor RFID é um dispositivo electrónico quando activado transmite um sinal que é reconhecido pela TAG e aguarda uma resposta da TAG RFID, após recebê-la, a decodifica e a transmite para o sistema.

Os Leitores são dispositivos capazes de enviar e receber sinais codificados em radio frequência que são emitidas pelas tags, um leitor pode chegar a ter múltiplas antenas acopladas que são responsáveis por emitir estas ondas de rádio (Guimarães, 2013).

As frequências de operação são classificadas em: baixa (LF de 125 kHz), alta (HF de 13,56 MHz) ou ultra alta (UHF de 840~960MHz), sendo as duas primeiras as frequências de trabalho comumente encontradas em tags passivas e a última em tags activas. (Bhuptani; Radpour et al 2005 apud Losi 2015).

Hosts

Hosts são os sistemas que irão controlar e processar os sinais enviados pelos leitores. Estes hosts podem ser um computador, smartphone, tablet ou qualquer outro dispositivo capaz de processamento. Cabe então ao engenheiro de controlo programar o host para realizar as leituras, processar os sinais e tomar uma acção com base nos dados colectados (Guimarães, 2013).

3.3. Tecnologias para o Interface

Para o desenvolvimento do Software Web usa-se uma página em HTML, interpretada pelo navegador de Internet (*Microsoft Edge, Google Chrome* e outros navegadores), para interagir com o usuário, formando a Camada de Apresentação. Outras tecnologias podem ser misturadas ao HTML para a construção de uma interface mais poderosa, com um visual mais adequado, além de proporcionar recursos que o HTML isoladamente não é capaz (Costa, 2001).

A tabela 2 apresenta os tipos e a descrição das tecnologias responsáveis pela construção da interface com o usuário.

Tabela 2: Tecnologias responsáveis pela construção da interface com usuário

Tecnologias	**Descrição**
HTML	É uma linguagem de Marcação padrão usada para construção de páginas WEB. O HTML Utiliza os conceitos do *HyperTexto* e da

	Hipermídia para apresentar num mesmo ambiente: dados, imagens e outros tipos de mídia, como vídeos, sons e gráficos. O HTML é um subconjunto do *Standard Generalized Markup Language* (SGML) e utiliza rótulos (tags) que definem a aparência e o formato dos dados, sendo padronizado *pelo Object Management Group* (OMG). É interpretado por qualquer navegador, em qualquer plataforma.
DHTML	É um conjunto de técnicas usadas para união das tecnologias HTML e *JavaScript* para tornar o HTML mais dinâmico. HTML é um termo utilizado para agrupar as tecnologias de script, cascatas de estilo e *applets*, as quais podem ser utilizadas em conjunto com o HTML tornando as páginas Web mais interactivas e animadas. O uso de tecnologias DHTML é possível graças à concepção do *Document Object Model* (DOM), que aplica os conceitos da orientação a objectos a todos os elementos de uma página HTML
Applet Java	A linguagem Java da *Sun Microsystems*, utilizada na forma de *applets*, é capaz de estender as funcionalidades dos navegadores, adicionando recursos antes impossíveis de serem construídos com o *HTML* puro. Os *applets* são miniprogramas executados sob o browser, através da *Java* Virtual Machine.
Active X	É uma estrutura de *software* da Microsoft (MSFT) que permite que os aplicativos compartilhem funcionalidades e dados uns com os outros por meio de navegadores da web, independentemente da linguagem de programação em que estão escritos
JavaScript	É uma linguagem de script que pode ser embutida na página HTML, oferecendo algumas formas de controlo da página, como a validação de campos. O *JavaScript* pode ser usado em quase todos os Navegadores, sendo que o Internet Explorer apresenta diferenças na sintaxe dos comandos, o que dificulta a capacidade multiplataforma das aplicações Web que utilizam o *JavaScript*.
VBScript	Possui a mesma filosofia do *JavaScript*, mas utiliza a sintaxe da linguagem Visual Basic da Microsoft, ao invés da sintaxe da linguagem Java
CSS	Permite que os estilos dos elementos da página (espaçamento, cores, fontes, margens, etc.) sejam especificados separadamente da estrutura do documento, facilitando dessa forma, uma futura modificação no estilo da página

XML	É uma linguagem de marcação, tal como o HTML. O XML lida com rótulos (tags) sendo possível definir conjuntos de *tags* próprios. A definição do padrão de *tags*, possibilita a criação de documentos num formato XML que podem ser facilmente interpretados pelo Navegador. Diferentemente do HTML, no XML não há tags para a aparência dos dados. O XML é também muito utilizado para padronizar a troca de informações entre sistemas.

Fonte: (Costa, 2001)

3.4. Tecnologias para o Processamento no Servidor

Na camada *middleware* (software intermediário), ocorre realmente o trabalho de programação do aplicativo Web, sendo esta camada a responsável por processar a informação enviada pelo cliente (navegador), processar a regra de negócio (que pode estar em outra camada), interagir com o banco de dados, preparar a resposta (quase sempre na forma de uma página HTML) e enviá-la ao cliente. Os componentes dessa camada estão no Web *Server* e são capazes de utilizar os recursos desses servidores e dos demais recursos conectados para realizar o processamento. É importante perceber que a forma com que todas essas tecnologias trabalham é similar: recebem uma solicitação do cliente, processam essa solicitação e respondem na forma de uma página HTML (Costa, 2001).

Tabela 3: As tecnologias responsáveis pela construção da camada *middleware*

Tecnologias	**Descrição**
CGI	É uma interface padrão de comunicação entre servidores Web e programas de gateway. “O CGI é a aplicação mais básica para a cessar os recursos do sistema no servidor, e foi também a primeira tecnologia para o desenvolvimento de aplicações Web; Pode ser escrito em diversas linguagens, sendo as principais o Perl e o C/C++.”
SSI	Utiliza rótulos especiais (tags), inseridos no documento HTML que são interpretados pelo *Web Server*, possibilitando assim que as tags sejam substituídas por conteúdo dinâmico, de acordo com o processamento realizado no servidor; As tags do SSI são específicas para cada *servidor Web*.
ASP	É uma tecnologia da *Microsoft* que utiliza os conceitos de SSI e CGI para a construção de conteúdo dinâmico, somente funcionando no *Internet Information Server* (IIS), o *software servidor Web* da *Microsoft,* ou seja, é exclusiva para a plataforma Windows. Código ASP é inserido no HTML e interpretado pelo servidor a cada requisição recebida. O ASP é a mais popular linguagem de script servidora actualmente em uso

PHP	PHP segue a mesma filosofia do ASP, porém pode ser executada por diferentes servidores, principalmente na plataforma *Unix (Solaris, Linux*, etc.). Diferentemente do ASP, o PHP utiliza sintaxe baseada em C, Java e Perl. É uma tecnologia não-proprietária.
ISAPI/NSAPI	A tecnologia ISAPI é baseada no acesso à *Application Programming Interface* (API) do *web server*, através do qual a aplicação servidora ISAPI ou NSAPI utiliza directamente a API do web server para executar a função desejada. A NSAPI é voltada para o *Netscape Server* e a ISAPI é a tecnologia para o servidor IIS da Microsoft. Algumas linguagens possibilitam o desenvolvimento de tais aplicativos, como é o caso do Delphi e C++
Servlets	É um tipo de aplicativo Java que executado no *Web Server* permitem um funcionamento similar ao CGI. Os *Servlets* Java são multiplataforma e oferecem bom desempenho.
JSP	É uma tecnologia baseada em Java que utiliza o mesmo princípio do ASP, com código Java embutido na página HTML, o qual é interpretado a cada requisição pelo *Web Server*. Tem - se mostrado uma tecnologia bastante promissora.
ColdFusion	É linguagem de *script server* que também utiliza uma filosofia similar ao ASP e JSP. Possui sintaxe própria e é uma tecnologia proprietária.

(Costa, 2001).

3.5. Banco de Dados

O banco de dados é a organização e armazenagem de informações sobre um domínio específico. De forma mais simples, é o agrupamento de dados que tratam do mesmo assunto, e que precisam ser armazenados para segurança ou conferência futura (Souza, 2020).

Existem diversos tipos de sistema de gerenciamento de banco de dados, e cada um é adequado para uma necessidade dos clientes. A tabela 4 mostra os tipos mais comuns.

Tabela 4: tipos de sistema de gerenciamento de banco de dados

Tipos de banco de dados	**Descrição**
O Oracle Database	É o sistema de gestão de banco de dados mais utilizados no mundo. Trabalha com a linguagem SQL, e garante a segurança e diversos recursos para seus clientes e usuários.

O SQL Server	Criado pela *Microsoft,* é muito conhecido e utilizado no mercado. A linguagem usada nessa ferramenta é o T-SQL, e oferece recursos avançados e diferenciados para facilitar a actualização de dados e o armazenamento das informações de forma segura e confiável
O MySQL	É um banco de dados relacional que pertence à Oracle. Uma das características mais marcantes desse modelo é o fato de se tratar de um Open Source. Utiliza a linguagem SQL e funciona com as licenças de *software* comercial e livre.
O PostgreSQL	Também é um gerenciador de banco de dados relacional Open Source, comumente utilizado para sistemas *online*, como *Skype, Apple*.
O NoSQL	É um sistema de banco de dados não relacionais. Hoje, esse termo é comumente utilizado por pessoas que produzem conteúdos por dispositivos, redes sociais e outros tipos de funcionalidades web, que exigem a gestão de dados em diferentes formatos.
O MongoDB	É um dos maiores destaques do mercado. Esse banco de dados é Open Source e é um dos mais utilizados por diversas empresas. Seu sistema gira em *Windows, Linux e OSX,* com linguagem de programação C++.
O Redis	Se tornou um banco de dados popular no mercado, e também funciona como *Open Source.* Através desse sistema, as informações são armazenadas no formato de chave-valor.

Fonte: (Souza, 2020).

Capítulo IV

4. Caso de Estudo

4.1. Hospital Central de Maputo (HCM)

O HCM é um hospital público de referência, elevado nível de competência, e oferece atendimento bem como campo de desenvolvimento de actividades assistenciais, de formação e investigação (HCM, s.d.).

Com mais de 100 anos de existência, o HCM tem actualmente uma capacidade de internamento de 1500 camas distribuídas por diversos departamentos clínicos e serviços de apoio e presta assistência nas mais diversas áreas médicas e cirúrgicas (HCM, s.d.).

Conta actualmente com aproximadamente 4000 funcionários e colaboradores distribuídos em categorias profissionais como, médicos, técnicos de saúde, administrativos, agentes de serviços e outras áreas de apoio. Além das actividades de rotina, o HCM vem desenvolvendo nos últimos anos actividades de excelência tais como dialise, Cirurgia Ortopédica de prótese da anca e joelho e Cirurgia de coração aberto com circulação extracorpórea. Tem ainda capacidade para realizar exames auxiliares de diagnóstico tais como a Tomografia axial computarizada (TAC), Ressonância Magnética, Mamografia entre outras (HCM, s.d.).

No HCM, são formados Médicos de Clínica Geral, Especialistas de diversas áreas, enfermeiros, técnicos médios e superiores de diversas áreas de saúde. É também um polo importante de pesquisa clínica, em parceria com outras instituições vocacionadas para a pesquisa, quer nacionais quer internacionais (HCM, s.d.).

Pelo seu tempo de existência o HCM necessita permanentemente de obras de manutenção e reabilitação para manter o seu padrão de qualidade e dignificar os seus utentes e trabalhadores. São também necessárias novas construções e obras de funcionalização para responder as necessidades do desenvolvimento da medicina neste seculo (HCM, s.d.).

Para a prossecução destas actividades o HCM dispõe de fundos maioritariamente alocados pelo orçamento Geral do Estado e em menor volume de fundos próprios gerados pelo “atendimento especial e personalizado” (HCM, s.d.).

De um modo geral, pode-se dizer que estes meios estão muito aquém das necessidades dum hospital com a dimensão do HCM. A exiguidade de fundos e meios compromete sobremaneira o funcionamento do último recurso público nacional na área da saúde (HCM, s.d.).

Os grandes desafios que o HCM tem neste momento e durante os próximos anos é de se adaptar as necessidades dos seus utentes, dotando-se de meios humanos e materiais suficientes e adequados para um desempenho que se pretende de excelência (HCM, s.d.).

A humanização e a qualidade nos procedimentos hospitalares constituem hoje elemento primordial e omnipresente a nível de qualquer unidade sanitária. Os hospitais de actualidade são convidados a abrir-se para que a comunidade participe na sua gestão (HCM, s.d.).

4.2. Dificuldades encontradas

Não foi possível ter informações sobre os sistemas actuais de controlo de acesso e de assiduidade disponível no hospital (vide o anexo 3), devido a falta da autorização do instituto de Bioética (Faculdade de Medicina – UEM). A direcção geral do hospital Central de Maputo disse que tinha que submeter a Credencial, Projecto e requerimento. Reuniu – se esses documento e foram submetido (vide o anexo 1 – Comprovativo de entrada), aguardou – se pela resposta, depois de 1 mês da entrada dos documentos no hospital obteve – se a seguinte resposta: falta autorização do Instituto de Bioética por conta disso tinha que se iniciar o processo (vide o anexo 2 – Documentos submetidos e pareceres da direcção geral de HCM), mas já não havia tempo suficiente para pedir a autorizar ao Instituto da Bioética.

Capítulo V

5. Desenvolvimento do Protótipo

A solução escolhida é de um sistema de controlo por RFID, servidor Apache e um banco de dados MySQL, por ser um sistema de baixo custo e de fácil manutenção. O objectivo do sistema é accionar um relé através de contactos, que controla o movimento da porta (fechada ou aberta), a mesma através do sinal envido por leitor RFID de *Tag* de usuário registado na base de dados, e caso o tag deste usuário tenha permissão ou não para realizar esta operação os dados de acesso são organizados e registados na base de dados (identificação, data, hora e tipo de operação permitida ou negada).

Para o funcionamento do sistema desenvolvido foi dividido em 5 classes sendo elas, a classe API, Relógio, RFID, Senha, Tela e Microcontrolador".

- API é responsável por se conectar ao servidor e fazer todas as requisições necessárias. Toda parte em que ocorre troca de dados entre sistema e o servidor é gerenciado por essa classe, os métodos de autenticação, cadastro, remoção de tags e actualizar o horário que é exibido no LCD;
- RFID é responsável por fazer a leitura da tag de um cartão e consequentemente de acordo com a opção desejada executar os métodos de autenticação, cadastro ou remoção de uma tag;
- Relógio é responsável por toda a lógica de funcionamento da data e hora que são exibidas no LCD. Mesmo sem conexão com o servidor é possível alterar a data e hora manualmente pelo dispositivo;
- Tela é onde exibe a data do sistema e os ícones de conexão com Wi-Fi e servidor;
- Microcontrolador é o cérebro do sistema. Ela é responsável por determinar o que acontece quando uma tecla é pressionada ou dispositivo de entrada.

5.1. Descrição do sistema

A falta de recursos avançados em alguns deles, como permissões de agendamento, capacidade de controlar vários sectores por Wi-Fi, facilitar actualização de dados de usuários no banco de dados, possuir um *hardware* externo (como servidores), interface baseada em página *web*. Desta surge a necessidade de projectar Sistema de Controlo

de Acesso que contenha todas as funcionalidades mencionadas, mantendo um preço abaixo, com o uso da tecnologia *IoT* para permitir a integração com outros sistemas e baseado em Wi-Fi. A figura 6 mostra o diagrama de bloco do sistema, que explica de uma forma resumida o funcionamento geral do sistema, o mesmo que será explicado detalhadamente nos passos subsequentes.

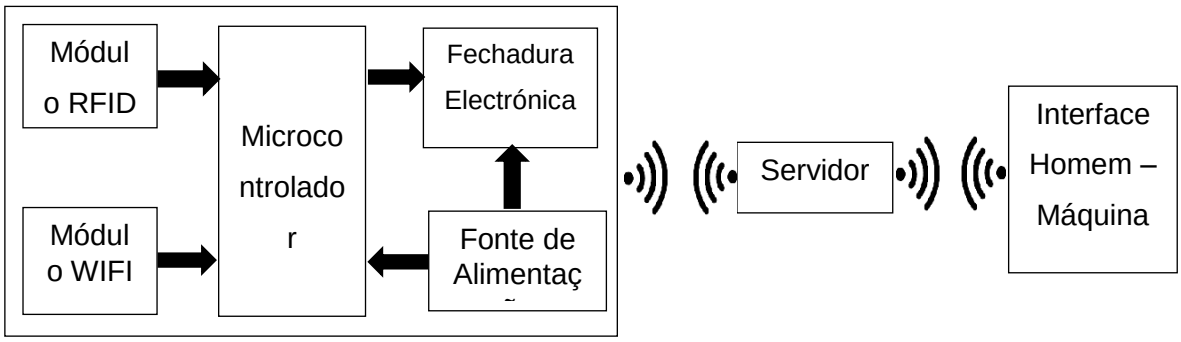


Figura 6: Diagrama de blocos do sistema

Fonte autor

Módulo RFID: são dispositivos de entrada do sistema, responsáveis pela leitura dos cartões ou tag e enviar os dados para o microcontrolador.

Fechadura Electrónica: são dispositivos de saída do sistema, responsáveis pelo bloqueio físico.

Módulo Wifi: é um dispositivo de entrada, responsável por conectar o microcontrolador a internet.

Microcontrolador: é o dispositivo controlador do sistema, que ira comparar os dados envidos por módulo RFID e dados armazenados no banco de dados. E ele acciona o relé da fechadura por 5 segundos.

Servidor: é um *software* que disponibiliza ou armazena recursos dos seus integrantes, responsável pelo armazenamento de todo os dados e o historial dos usuários.

Interface Homem – Máquina: São dispositivo electrónico e programa projectados para tornar mais fácil e eficiente a comunicação dos usuários com a máquina, consiste numa tela que permite que os usuários tenham acesso a todos os dados e históricos armazenados no servidor.

Fonte de Alimentação: é o dispositivo responsável por alimentar o sistema.

5.2. Especificações Gerais do Sistema

Na tabela 5 pode-se observar as especificações gerais do protótipo, onde o número máximo usuários e sectores foi limitado para permitir que todas as informações sejam armazenadas na memória RAM do ESP32, para permitir uma melhor capacidade de resposta do sistema.

Tabela 5: Especificações Gerais do Protótipo

Especificações técnicas	**Descrição**
N°. máximo de usuários cadastrados	498 Por Sector
Interface gráfica baseada	Baseada na web centralizada
Controlo de múltiplos sectores	Suportando até 45 sectores simultaneamente
N°. máximo de horários	Até 22.410 (498 por sector)
N°. máximo de registos	500.000 Com armazenamento estendido

Fonte: Autor

5.3. Componentes do sistema

Esta secção apresenta a descrição técnica dos componentes electrónicos que foram usados para a concepção do protótipo.

Microcontrolador

Para a concepção do protótipo foi escolhido o ESP32 ilustrado na figura 7, é microcontrolador CMOS de 32 bits. Projectado com a tecnologia TSMC de ultrabaixa potência e baixo custo, Com Bluetooth e Wi-fi já integrados. Vide a tabela 6 as especificações técnicas.

Tabela 6: Especificações técnicas do ESP32

Especificações técnicas	**Descrição**
Microprocessador	*Xtensa* ® Dual-Core 32-bits LX6 com um desempenho de 600 DMIPS
Memória ROM	448 Kbytes

Memória SRAM	Possui 520 KBy da memória *flash*
Clock máximo	240MHz
Memória Flash	4 MB
Wireless padrão	802.11 b/g/n
Conexão Wifi	2.4GHz
Alimentação	2,2 a 3,6 V
Temperatura	- 40°C a 125°C

Fonte: (Espressif, 2021)

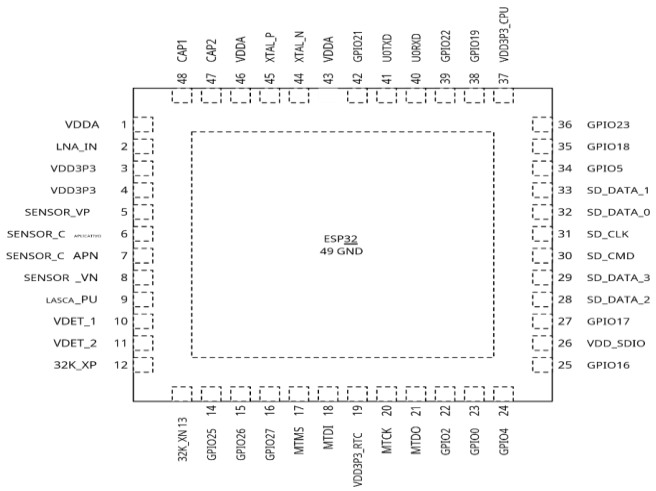


Figura 7: Microcontrolador ESP32

Fonte: (Espressif, 2021)

Modulo RFID

O MFRC522 é um leitor/gravador ilustrado na figura 8, altamente utilizado para comunicação sem contacto a 13,56MHz, de baixo consumo e pequeno tamanho, permite sem contacto ler e escrever em cartões que seguem o padrão *Mifare*. A tabela 6 apresenta especificações técnicas do MFRC522. A figura 9 mostra um exemplo de um Kit de Modulo RFID baseado no chip MFRC522

Tabela 7: Especificações técnicas do` MFRC522

Especificações técnicas	**Descrição**
Frequência de operação	13,56MHz

Alimentação DC	2.5 a 3.3 V
Temperatura de operação	- 20°C a 80°C
Taxa de transferência	10 Mbit/s
Dimensões	8,5 x 5,5 x 1,0cm
Umidade relativa	5% – 95%
Peso	21g
Tipos de cartões suportados	Mifare1 S50, S70 Mifare1, Mifare UltraLight, Mifare Pro, Mifare Desfire

Fonte: (NXP, 2016)

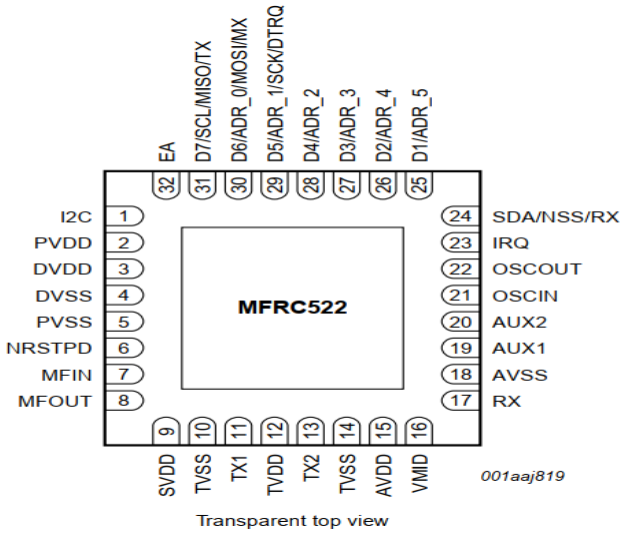


Figura 8: Modulo MFRC522

Fonte: (NXP, 2016)

Figura 9: *Kit* de Modulo RFID baseado no chip MFRC522

Fonte: (Filipeflop, 2021)

Tela

Para visualização de dados no protótipo foi escolhido o módulo LCD associado a um módulo I2C (vide a figura 10). Para o I2C suportar o LCD é necessário conectar os seus 16 pinos em ordem de expansão para em seguida conectar ao microcontrolador. A tabela 8 apresenta as especificações técnicas do módulo LCD associado com o módulo I2C.

Tabela 8: Especificações técnicas do módulo LCD com o módulo I2C

Especificações técnicas	**Descrição**
Interface de comunicação	I2C
Comunicação	4bits ou 8bits
Controlador do módulo I2C	PCF8574T
Cor do fundo	Azul
Tensão de Operação DC	4,5V a 5,5V
Número de caracteres (colunas x linhas)	16x2
Dimensões	36mm(L) x 17mm(A) x 83mm(C)
Tamanho da janela (alt. x larg.)	66x16 mm
Iluminação	LED
Cor da iluminação	Branca

Fonte: (ROBÓTICA, 2021)

Figura 10**:** *Display Lcd 16x2 com Adaptador I2C*

Fonte: (ROBÓTICA, 2021)

Fonte de Alimentação

A fonte de Alimentação do Protótipo é o Módulo Transformador (Fonte de Alimentação AC-DC 5V 700mA 3.5W Conversor AC 220V para DC 5V) ilustrado na figura 11 de alta qualidade possui um desempenho estável e rentável. A tabela 9 apresenta especificações técnicas

Tabela 9: Especificações técnicas da fonte de Alimentação

Especificações técnicas	**Descrição**
Tensão de entrada AC	85 a 265V, 50Hz;
Tensão e Corrente de saída DC	5V e 700mA;
Potência:	3,5W;
Temperatura de operação	20ºC a 60ºC;
Humidade relativa:	40-90%
Eficiência de saída:	80%;

Fonte: (ELECTROFUN, 2021)

Figura 11: Fonte de Alimentação AC-DC

Fonte: (ELECTROFUN, 2021)

Buzzer

Buzzer ilustrado na figura 12, é o elemento escolhido para criar um alarme sonoro em caso de um *tag* ou cartão seja a aproximado ao leitor. O buzzer contém um circuito oscilador embutido, assim basta energizar o componente para que o mesmo comece a emitir um *beep* contínuo. Na tabela 10 pode se observar as especificações técnicas.

Tabela 10 Especificações técnicas do Buzzer

Especificações técnicas	**Descrição**
Modelo	Buzzer tipo activo
Tensão de Operação	4 à 8VDC
Corrente de operação	30mA
Saída de som mínima	85dB
Frequência de ressonância	2300±300 Hz
Dimensões	11,8 x 9mm

Fonte: (Filipeflop, 2021)

Figura 12: Buzzer

Fonte: (Filipeflop, 2021)

Teclado

Teclado é um dispositivo de entrada pois permite, por meio de botões, inserir dados em um dispositivo.

Internamente são 16 teclas *push-buttons* tipo membrana. Conforme a tecla é pressionada, é feita a conexão entre a linha e a coluna correspondentes. Exemplo de

funcionamento, se pressionarmos a tecla A no teclado matricial, será feita a conexão entre os pinos 1 (linha 1) e 8 (coluna 4). (Filipeflop, 2021)

Os pinos das linhas deverão ser configurados como OUTPUT (Saída), e os pinos das colunas como INPUT (Entrada). Nos pinos referente às colunas, devera usar – se 4 resistores *pull-down,* mantendo-as em nível baixo quando não houver accionamento das teclas. (Filipeflop, 2021)

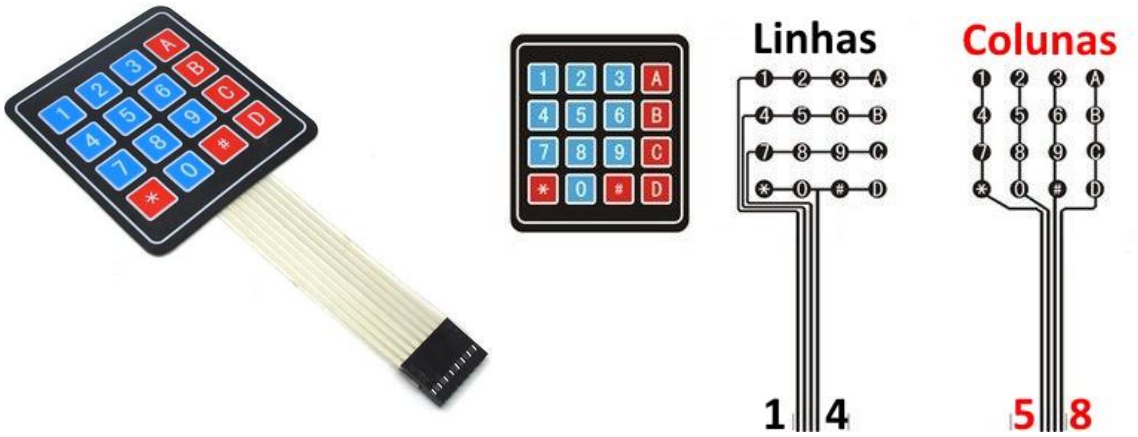


Figura 13: Teclado Matricial

Fonte: (Filipeflop, 2021)

Modulo Relé

O módulo relé é o dispositivo escolhido para accionar o micro servo, na figura 13 pode – se observar o módulo relé. Ele é equipado com transístores, conectores, leds, díodos e relés de alta qualidade. Cada canal possui um LED para indicar o estado da saída do relé. A tabela 11 apresenta especificações técnicas do módulo relé.

Tabela 11: especificações Técnicas do Modulo relé

Especificações técnicas	**Descrição**
Modelo	JQC-3FF-S-Z
Tensão de operação	5 VDC
Permite Controlar cargas	220V AC
Tensão máxima de saída	28 VDC a 10ª ou 250VAC a 10A
Dimensões	50 mm x 37 mm x 18 mm

Tempo de resposta:	5~10ms
Pinagem	Normal Aberto, Normal Fechado e Comum
Peso	30g

Fonte: (Filipeflop, 2021)

Figura 14: Modulo rele de 2 canais

Fonte: (Filipeflop, 2021)

Micro Servo

Na figura 15 pode – se observar o Micro Servo 9g SG90 de alta qualidade e excelente para teste de bloqueio no protótipo. A tabela 12 apresenta as especificações técnicas de micro servo.

Tabela 12: Especificações Técnicas de micro servo

Especificações técnicas	**Descrição**
Tensão de operação	4,8 a 7,2V
Ângulo de rotação:	180 Graus
Velocidade	0,12 seg/60graus
Temperatura de Operação	-30C a +60C
Dimensões	32 x 30 x 12mm

Fonte: (Filipeflop, 2021)

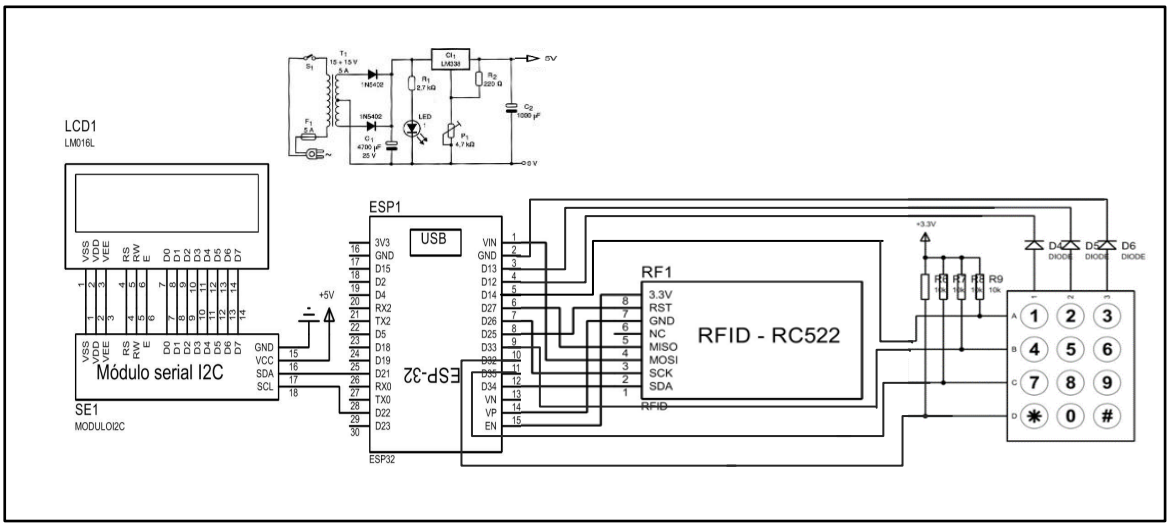
Figura 15: Micro Servo 9g SG90

Fonte: (Filipeflop, 2021)

5.4. Dimensionamento do projecto

5.4.1. Esquema Eléctrico

O elemento central do sistema é o ESP32, que faz o controlo de todos os outros dispositivos do sistema. Pode – se observar na figura 15, como estão ligados os



elementos do sistema (vide o anexo 5 – o esquema eléctrico).

Figura 16: Esquema Eléctrico do Protótipo

Fonte: Autor

Os pinos RST, MISO, MOSI, SCK e SDA do módulo MFRC522 são conectados ao microcontrolador, pela mesma correspondência. Estes enviam sinal de leitura dos bits

dos tags encontrados, através da comunicação SPI. Ligado aos pinos SDA e SCL encontra-se o LCD com módulo I2C. Este recebe os dados sobre o estado de cada operação através do mapeamento do mostrador. Ligados os pinos A, B, C, D, 1, 2 e 3 encontra-se o teclado matricial, que introduz dados no microcontrolador. A alimentação dos dispositivos é feita através de Fonte de Alimentação AC-DC 5VDC.

5.5. Programação

Fluxograma

Inicialmente, o sistema conecta – se ao servidor e faz todas as requisições necessárias e activa o módulo MFRC522, para autenticação cadastro, remoção de cartões e actualizar o horário. A figura 16 apresenta o fluxograma de operação de tag, o leitor RFID aguarda a leitura de cartões, caso seja encontrado é feita a comparação dos bits do cartão com os dados registados na base de dados (MySQL), caso afirmativo o sistema identifica o usuário e verifica se tem permissão para este tipo de operação ou não, caso o usuário tenha permissão para esta operação o sistema o sistema acciona o relé por 5 segundos para desbloquear a entrada e regista os dados de acesso.

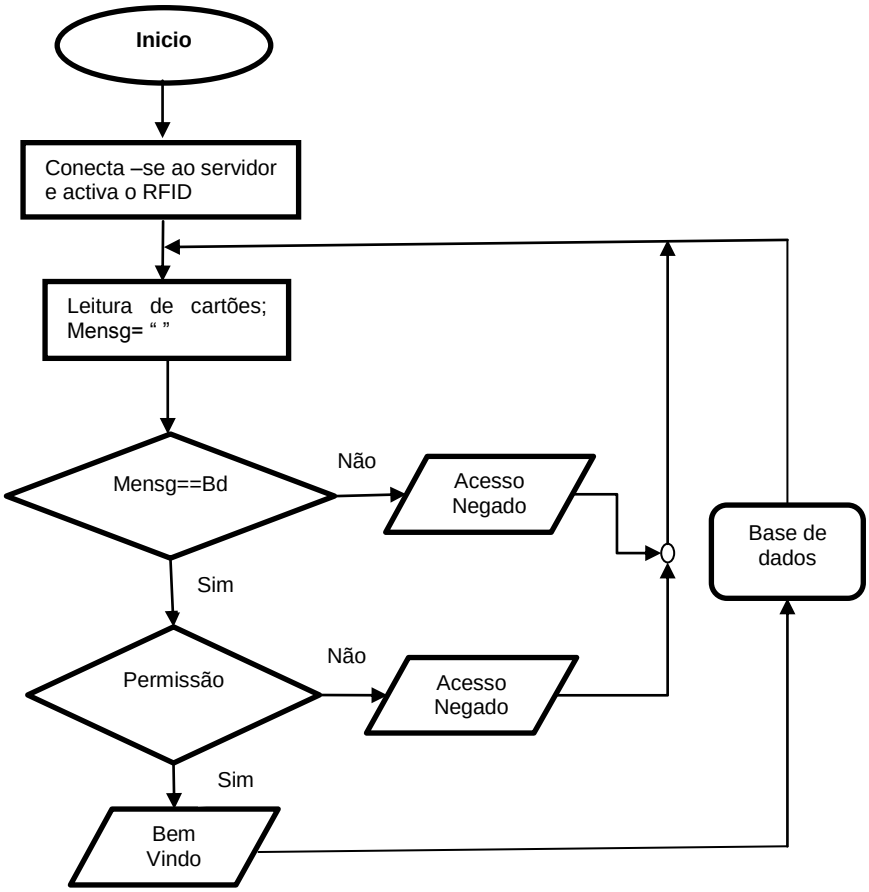


Figura 17: Fluxograma de operação de Cartão ou Tag

Fonte: Autor

Cadastro de Usuários

O registo de dados pode ser feito manualmente por usuários autorizados, foi criada uma matriz de armazenamento contínuo de UID de cartões e nome do usuário. Para tal o usuário pressiona a tecla #, de seguida passa o seu cartão para autenticação, caso o sistema reconhecer o usuário como autorizado para este processo deverá habilitar uma posição na matriz de cadastro, que será introduzido o nome do novo cartão e o UID do próprio cartão. O sistema deverá fazer a verificação/ varrimento destes dados e registar na MySQL, caso estes dados já tenham sido armazenados deverá responder com uma mensagem que afirma que o cartão já existe.

O administrador da base de dados também pode a partir dos comandos de MySQL adicionar ou remover um usuário.

Métodos

Existiu necessidade de importar bibliotecas *SoftwareSerial* para comunicação, *MFRC522* para leitor de cartões, SPI para comunicação serial do módulo RFID com

microcontrolador, *LiquidCrystal_I2C.h* para visualizar dados no mostrador digital, *Keypad.h* para inserir dados no sistema. *WiFi.h, HTTPClient.h* para conexão a rede de internet e armazenar dados num banco de dados locais (vide o Anexo 4)

5.6. Banco de Dados

Para a criação da base de dados foi utilizada a plataforma de gestão de base de dados *MySQL* de código aberto. Passos para criar o *MySQL* e definir a API:

- Instalar o servidor *MySQL*, servidor *web* e *PHP*;
- Criar conta de usuário *MySQL;*
- Criar banco de dados *MySQL*;
- Criar tabela *MySQL*;
- Escrever arquivos de script PHP;

Após a instalação, verificou – se a pasta **C:\xampp\htdocs.** Onde é colocado o código PHP. Abriu – se o painel de controlo do XAMPP, fez – se o *Start* do *MySQL* e *Apache* para habilitar o servidor *Web* e o *MySQL* (vide a figura 17).

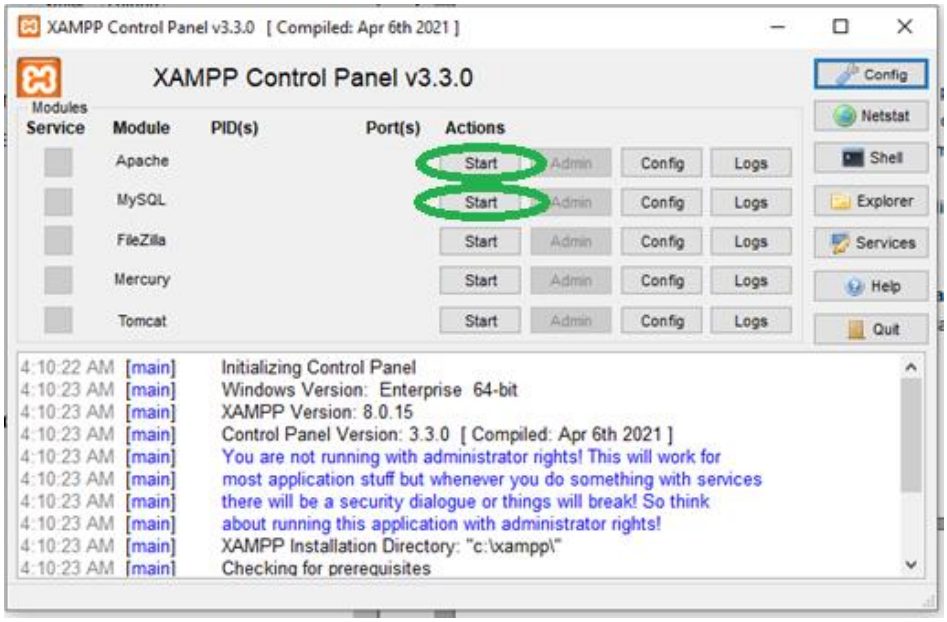
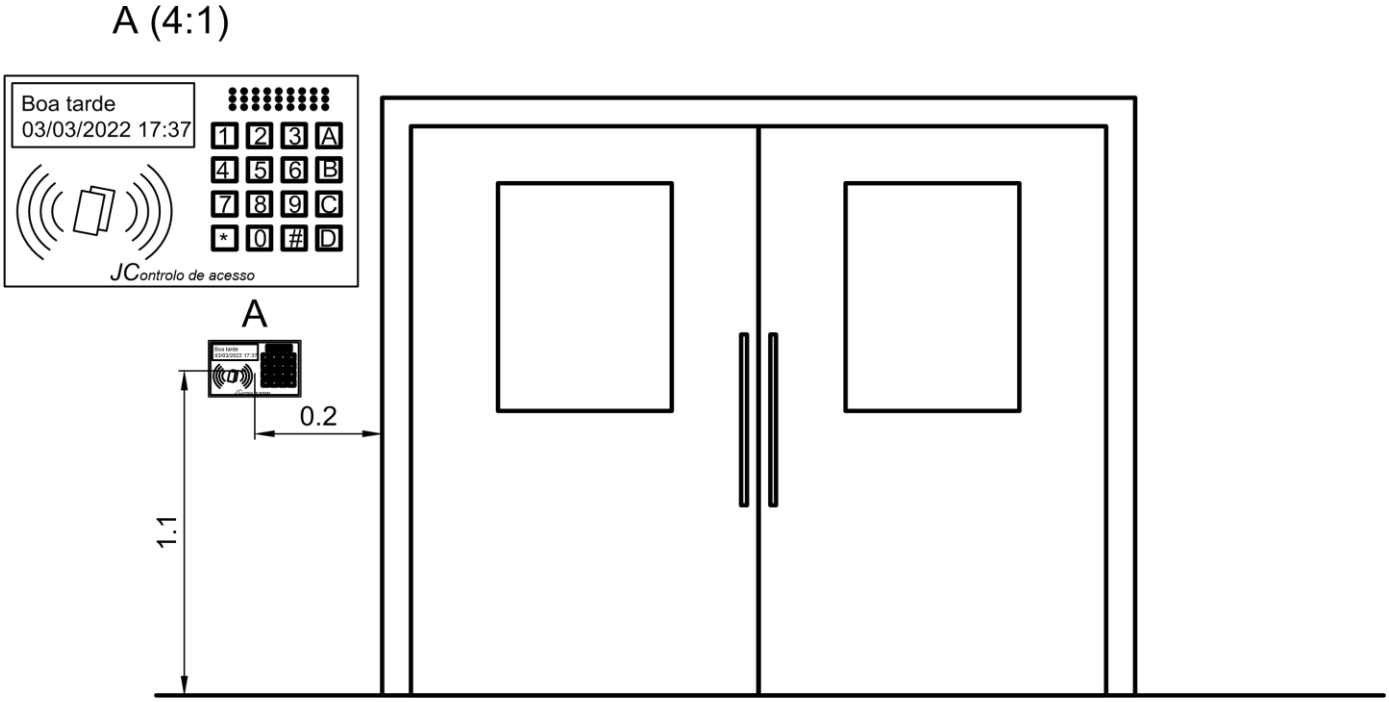


Figura 18: Painel de Controlo XAMPP

Foi Criada a conta *MySQL* com apenas permissões de acesso local, mesmo que os invasores saibam o nome de usuário/senha, eles não podem a cessar o banco de dados *MySQL*. O nome de usuário/senha é usado pelo PHP para se conectar ao banco de dados *MySQL.* Comandos usados para criar a conta:

- *cd C:\xampp\mysql\bin*
- *mysqladmin -u root password YOUR_ROOT_PASSWORD*
- *mysql.exe -u root –p*
- *CREATE USER 'Nome'@'localhost' IDENTIFIED BY 'Senha';*
- *GRANT ALL PRIVILEGES ON *.* TO 'Nome'@'localhost' WITH GRANT OPTION;*
- *FLUSH PRIVILEGES;*



Usou – se o comando o *CREATE DATABASE db_esp32 CHARACTER SET = 'utf8' COLLATE = 'utf8_general_ci';* para criar o banco de dados.

Para criar as tabelas foi usado o seguinte comando:

CREATE TABLE tbl_temp (

temp_id INT UNSIGNED NOT NULL AUTO_INCREMENT,

temp_value FLOAT DEFAULT 0.00,

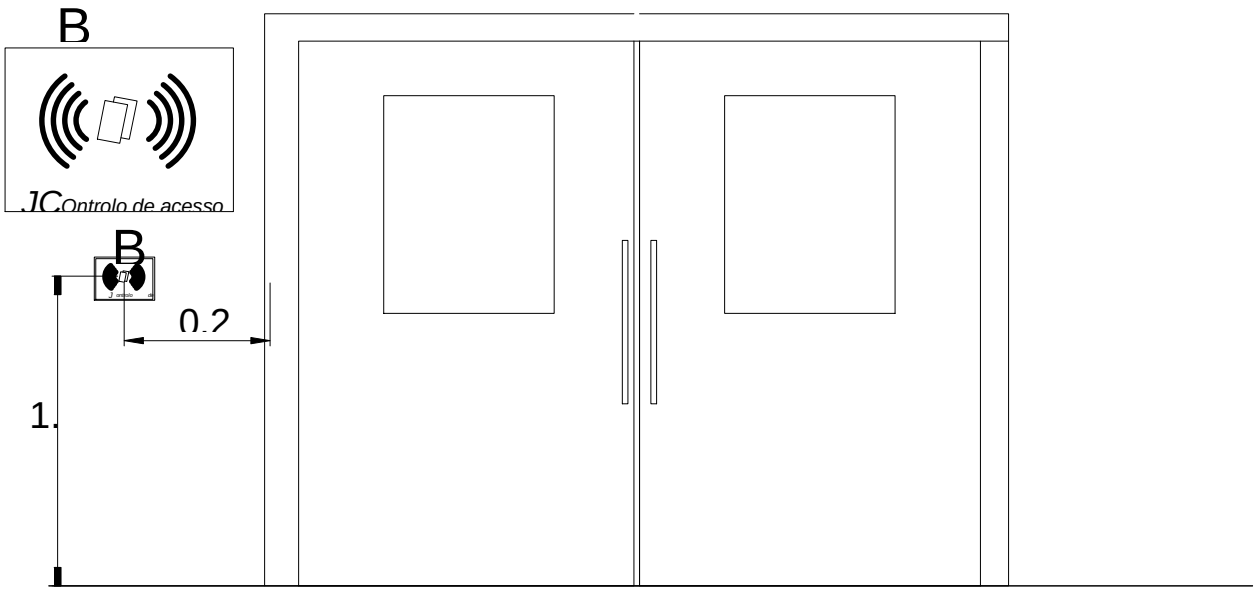
PRIMARY KEY (temp_id));

5.7. Instalação de Equipamento

O sistema tem dois dispositivos de leitura, um de entrada e um de saída. O dispositivo de leitura na entrada e saída serão instalados na parede perto da porta a uma altura de 1.1 metro e a um comprimento de 0.2 metro, como pode ser observado nas figuras 19

e 20. As fechaduras magnéticas serão instalados no canto superior entre as portas e o aro.

Figura 19: Exemplo de Instalação de equipamento leitura de entrada



Fonte: Autor

Figura 20: Exemplo de Instalação de equipamento leitura de saída

Fonte: Autor

5.8. Custo estimado do material

Os custos do projecto apresentados na tabela 13, se resumem em custo de *Hardware* já que os *softwares´s* usados são gratuitos.

Tabela 13: Orçamentação do protótipo

Descrição	**Preço Unitário (Mt)**	**Quantidade**	**Total (Mt)**
Microcontrolador ESP32	650	1	650
Kit De Modulo Rfid	220	1	220
Módulo Lcd - I2c	400	1	400
Díodo	6	4	24
Buzzer	65	1	65

Resistências	5	4	20
Fonte De Alimentação	200	1	200
Micro Servo 9g Sg90	180	1	180
Modulo Rele De 2 Canais	120	1	120
Total			1879

Fonte: Autor

Capítulo VI

6. Análise e discussão de resultados

Testes de velocidade

Para todos os testes de velocidade desta seção, o sistema está trabalhando em sua capacidade total para garantir que os resultados correspondam ao pior cenário em termos de tamanho de banco de dados. Isso significa que o sistema está utilizando bancos de dados com um total de 498 usuários e 49 sectores.

Tempo de inicialização

O tempo de inicialização do sistema inclui o tempo necessário para:

- Configurar os pinos e componentes do ESP (RFID, RTC e relé);
- Carregar os 4 arquivos de configuração (Rede, sectores, hora e senhas);
- Iniciar o servidor web;
- Carregar os bancos de dados (usuários, sectores, horários);
- Conectar-se à rede Wi-Fi;

Todas essas acções são feitas em 2,3 segundos (vide a figura 21). Isso significa que, em caso de reinicialização ou restauração de energia, os módulos estarão *online* e funcionando em menos de 3 segundos, um tempo impressionante que foi alcançado após muitas melhorias

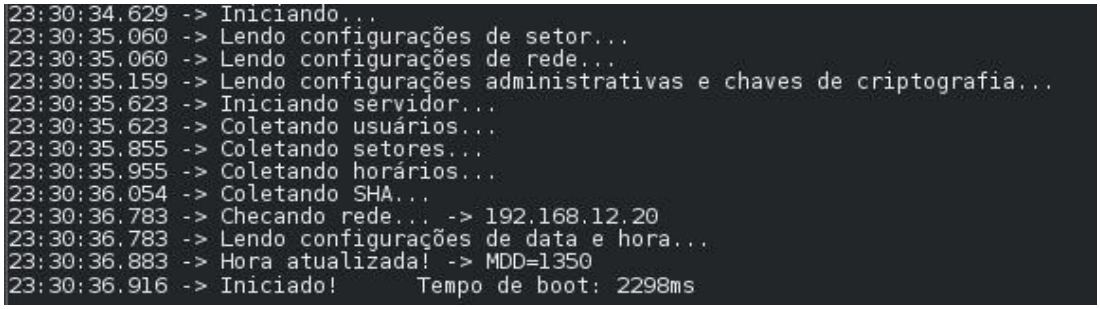


Figura 21: Tempo de inicialização

Modificação do arquivo

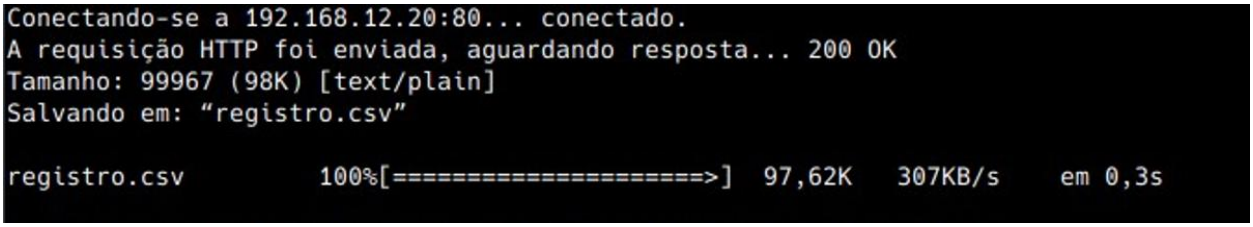
O tempo gasto para ler, escrever e gerar o *hash* dos arquivos também foi medido e representa o tempo utilizado pelo sistema quando o sistema precisa obter informações de um arquivo, ou alterá-lo. O tempo aproximado para processar os arquivos é mostrado na tabela 14

Tabela 14: Tempo necessário para processar os arquivos

	Velocidade de leitura	**Velocidade de escrita**
Banco de dados de usuários	~200 ms	~1,2s
Banco de dados de sectores	~100 ms	~800 ms
Banco de dados de agendamentos	~100 ms	~500 ms
Arquivos de configuração	~100 ms	~200 ms

Teste de Servidor Web

O servidor web também foi bastante aprimorado, pois é utilizado não apenas para a interface gráfica do usuário, mas também para a intercomunicação de módulos.



Essas melhorias podem ser vistas nos tempos de carregamento das páginas. Ao baixar arquivos grandes (como o arquivo de registos), a velocidade média de download é em torno de 300 KB/s (2,4 Mbps), conforme mostrado na figura 22.

Figura 22: Velocidade para baixar arquivos maiores

Fonte: Autor

Teste de Registo Dados

O sistema tem a capacidade máxima de até 45 sectores e por sector cadastrar até 498 usuários. Para o teste de registo de dados os leitores foram configurados para permitir o acesso ao usuário (Catine) nos "Sectores 1 e 2" e o usuário (Martins) no Sector 1. A figura 23 apresenta mais detalhes de teste de registo de dados.

Tipo	Nome	Sector	Data	Entrada	Saída	Duração
Permitido	Catine	Sector 2	22/03/2022	17:30	17:35	00:05
Permitido	Catine	Sector 1	22/03/2022	17:35	17:37	00:02
Permitido	Martins	Sector 1	22/03/2022	17:32	17:34	00:02
Negado	Catine	Sector 3	22/03/2022	-	-	-
Negado	Martins	Sector 2	22/03/2022	-	-	-
Negado	Martins	Sector 3	22/03/2022	-	-	-

Figura 23: Teste de Registo

Capítulo VII

7. Considerações Finais

7.1. Conclusão

O projecto desenvolvido teve como objectivo geral, desenvolver uma proposta de um Sistema de controlo de Acesso em Área restrita do Bloco Operatório do Hospital Central de Maputo usando autenticação por RFID e *Interface WEB*, baseado nos resultados dos testes realizados foi possível concluir que os objectivos foram alcançados, uma vez que que o protótipo cumpre com as exigências básicas para o qual foi planeado.

Pode-se concluir que é possível desenvolver um Sistema de Controlo de Acesso que contenha múltiplas funcionalidades avançadas (como controlo multissectorial e interface gráfica baseada) utilizando componentes padrão, sendo um boa alternativa aos produtos de mercado disponíveis hoje em dia.

O sistema também provou que é possível usar componentes convencionais e de baixo custo para criar um Sistema de Controlo de Acesso que inclui muitas funcionalidades que só estão disponíveis nos produtos de alto custo no mercado, como comunicação Wi-Fi, controlo multissectorial e horários para permissão de acesso.

7.2. Sugestão para trabalhos futuros

Para possíveis trabalhos futuros pode-se melhor os seguintes pontos no sistema desenvolvido:

- Colocar câmera para contar o número de pessoas que estão no sector;
- Desenvolver um *software* para assistente digital de pessoal (PDA) a fim de servir de codificador e descodificador para o usuário, eliminando a necessidade de consulta a uma tabela, e consequentemente reduzindo as chances de erro de interpretação.
- Utilização de um sistema *RFID* que opere na faixa de ultra frequência, para que o usuário não necessite de aproximar o cartão no leitor ao passar de um sector para outro;
- Confeccionar a Placa de Circuito Impresso (PCI), um vez que o circuito já está pronto;
- Colocar mais uma forma de autenticação utilizando sensor de leitura biométrica.

Bibliografia

APSEI. 2018. APSEI. *ASSOCIAÇÃO PORTUGUESA DE SEGURANÇA.* [Online] Junho de 2018. [Citação: 05 de Janeiro de 2022.] https://www.apsei.org.pt/sistemas-de-controlo-de-acessos-dispositivos-de-identificacao/..

Barros, Aryclenio, Dantas, Rummenigge e Silva, Gabriel da. 2018. Software de Registro de Presença em Sistema Embarcado com Integração Web. 05 de Dezembro de 2018, pp. 1-4.

Camargo, Mariana de Campos. 2021. Desenvolvimento de sistema de monitoramento com IoT de baixo custo para equipamentos médicos. 04 de Agosto de 2021, pp. 1-44.

Costa, Alexsander Muniz da. 2018. RFControl : sistema de gerência de estoque utilizando RFID. 2018, pp. 1-49.

Costa, Claudio Giulliano Alves da. 2001. Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenharia de Software. 2001, pp. 1-288.

ELECTROFUN. 2021. ELECTROFUN. [Online] 2021. [Citação: 10 de Janeiro de 2022.] https://www.electrofun.pt/fontes-de-alimentacao/modulo-transformador-fonte-alimentacao-ac-dc-5v-700ma-3-5w-conversor-ac-220v-dc-5v.

Espressif, Sistemas. 2021. Espressif. [Online] 3.8, 2021. [Citação: 04 de Janeiro de 2022.] https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf&ved=2ahUKEwit2p3lv6r1AhWkSvEDHVqQAUMQFnoECBAQAQ&usg=AOvVaw0aPqs26KTwgQAQ33yEvdPB.

Fernandes, Andrew Carvalho Barbosa. 2017. Free Pass - Sistema de controle de acesso utilizando cartões de proximidade RFID. 2017.

Filipeflop. 2021. Filipeflop. [Online] 2021. [Citação: 05 de Janeiro de 2022.] https://www.filipeflop.com/produto/kit-modulo-leitor-rfid-mfrc522-mifare/.

Francelino, Fábio Augusto e Tomazeti, Daiane Mastrangelo. AcessaIFSP: Sistema para Controle de Acesso. pp. 1-18.

Frankenfield, Jake. 2021. Investopedia. [Online] 26 de Outubro de 2021. [Citação: 16 de Dezembro de 2021.] https://www.investopedia.com/terms/a/activex.asp.

Gomes, António Augusto Araújo. 2010. Sistemas de Controlo de Acesso. Junho de 2010, pp. 1-14.

Gonçalves, Vinicius Rocha. 2019. Sistema de controle de acesso utilizando autenticação por RFID e gerenciamento por meio de software WEB. 2019, pp. 1-69.

Guimarães, André Rolim Almeida. 2013. Proposta de um sistema de controle de acesso utilizando tecnologia RFID. Setembro de 2013, pp. 1-80.

HCM. s.d.. Hospital Central de Maputo. [Online] s.d. [Citação: 05 de Dezembro de 2021.] https://www.hcm.gov.mz/sobre-nos/.

Intelbras. 2021. Intelbras. [Online] 2021. [Citação: 20 de Novembro de 2021.] https://www.topdata.com.br/controle-de-acesso-em-hospitais/.

Losi, Rafael Antonio. 2015. PROTÓTIPO DE INVENTÁRIO AUTOMATIZADO COM RFID. 2015, pp. 1-71.

Narciso, Marcelo Gonçalves. 2008. APLICAÇÃO DA TECNOLOGIA DE IDENTIFICAÇÃO POR RÁDIOFREQÜÊNCIA (RFID) PARA CONTROLE DE BENS PATRIMONIAIS PELA WEB. 2008, pp. 50-59.

Norman, Thomas L. 2017. How Electronic Access Control Systems Work. [ed.] Elsevier. *Electronic Access Control.* s.l. : 2nd, 2017, III, pp. 43-58.

NXP, Semiconductors. 2016. MFRC522 Standard performance MIFARE and NTAG frontend. NXP Semiconductors, 27 de Abril de 2016, Vol. Rev. 3.9, pp. 01-95.

Oliveira, Sérgio de. 2017. *Internet das Coisas com ESP8266, Arduino e Raspberry Pi.* [ed.] Carolina Kuwabata. São Paulo, SP – Brasil : Novatec Editora Ltda., 2017. pp. 1-257. Vol. i.

Penckowski, Vinicius. 2021. User access control system based on ESP32 technology. 2021, pp. 1-109.

Quaranta, Thiago Cinelli. 2019. Projeto e desenvolvimento de sistema de gestão de atendimento a pacientes em internação hospitalar. 2019, pp. 1-54.

ROBÓTICA, AUTOCORE. 2021. AUTOCORE ROBÓTICA. [Online] 2021. [Citação: 08 de Janeiro de 2022.] https://www.autocorerobotica.com.br/display-lcd-16x2-com-adaptador-i2c-backlight-azul.

Santiago, Valter Gabriel Paes. 2015. Registrador de eventos sobre uma plataforma com microcontrolador parallax propeller e interface web. 2015, pp. 1-95.

Souza, Ivan de. 2020. *Rockcontent.* [Online] 20 de Fevereiro de 2020. [Citação: 16 de Dezembro de 2021.] https://rockcontent.com/br/blog/banco-de-dados/.

Vilante, Leandro de Souza. 2007. Gereneiamento de Dados em Hospitais utilizando Sensores e RFID. 2007, pp. 1-25.

Weles, Enkindu Feitosa e Bruno, Daniel Otávio Tambasco. 2018. PROTÓTIPO PARA UM SISTEMA DE AUTOMAÇÃO DE CONTROLE PATRIMONIAL UTILIZANDO TECNOLOGIA RFID. 25 de Agosto de 2018, pp. 1-10.

EXMA SENHORA DIRECTORA CIENTÍFICA PEDAGÓGICA DO HOSPITAL CENTRAL DE MAPUTO

MAPUTO

José Catine Munguambe Júnior, de 22 anos, Solteiro, filho de José Catine Munguambe e Melta Vicente Munguambe, natural de Maputo, residente no Bairro Zona Verde, Q. 30, casa nº. 81, portador do Bilhete de Identidade nº. 110501558845P, emitido aos 09 de Marco de 2017, pelo Arquivo de Identificação da Cidade da Matola, estudante do 5º ano do curso de Engenharia Electrónica na faculdade de Engenharia, pela Universidade Eduardo Mondlane, Vem mui respeitosamente requer que V. Excia. Se digne **Autorizar a recolha de dados no Bloco Operatório** com objectivo de culminação de estudos, pelo que

Pede Deferimento

Maputo, 6 de Dezembro de 2021

José Catine Munguambe Júnior

Anexo 1 – Comprovativo de entrada

Anexo 2 – Documentos submetido e pareceres da direcção geral de HCM

Pº Solicitar a realização do estudo na instituição e remeter os resultados de dados após autorização ética e administrativa
16/12/2021

EXMA SENHORA DIRECTORA CIENTÍFICA PEDAGÓGICA DO HOSPITAL CENTRAL DE MAPUTO

MAPUTO

José Catine Munguambe Júnior, de 22 anos, Solteiro, filho de José Catine Munguambe e Melta Vicente Munguambe, natural de Maputo, residente no Bairro Zona Verde, Q. 30, casa nº. 81, portador do Bilhete de Identidade nº. 110501558845P, emitido aos 09 de Marco de 2017, pelo Arquivo de Identificação da Cidade da Matola, estudante do 5º ano do curso de Engenharia Electrónica na faculdade de Engenharia, pela Universidade Eduardo Mondlane, Vem mui respeitosamente requer que V. Excia. Se digne **Autorizar a recolha de dados no Bloco Operatório** com objectivo de culminação de estudos, pelo que

Pede Deferimento

Maputo, 6 de Dezembro de 2021

José Catine Munguambe Jr.

José Catine Munguambe Júnior

HOSPITAL CENTRAL DE MAPUTO
SECRETARIA GERAL
Entrada nº 1408
Data 09 / 12 / 2021
Horas

Contacto: 848564981

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA
CURSO DE ENGENHARIA ELECTRÓNICA

Autor: **José Catine Munguambe Júnior** Contacto: +258 848564981/821419462

Email: josecatinejunior@gmail.com

Tema: **PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E GERENCIAMENTO POR MEIO DE SOFTWARE WEB**

1. Introdução

1.1. Contextualização

Sempre foi problema da sociedade a necessidade de ter segurança no meio em que se vive, não somente em relação à segurança pessoal, mas também de manter um local seguro quando não se está nele ou próximo o suficiente para tê-lo em vista. Gonçalves 2019 diz que "Além da necessidade de manter um local seguro também é necessário ter o controle sobre determinados sectores, sendo possível o acesso somente por pessoas com autorização previamente declarada". Cardoso 2014 citado por Gonçalves 2019 afirma que "estas soluções já conhecidas como portas e fechaduras resolvem o problema de manter um local seguro elas não fornecem a solução do controle de acesso."

Nos dias actuais para identificação automática de objectos ou pessoas a tecnologia RFID é mais usado devido ao seu custo reduzido e melhorias em seu funcionamento, O Guimarães 2013 diz que "RFID é uma tecnologia que permite a transferência de informações sem fio através de campos electromagnéticos, com um propósito de identificar ou rastrear objectos que possuam algum dispositivo RFID presente."

Com o avanço da tecnologias as informações que levavam horas, dias, meses ou até anos para chegar, são entregues em questões de milissegundos, com isso, surge a possibilidade de criar

um sistema de controlo de acesso e monitoramento em tempo real, envolvendo grande fluxo de dados transferidos em milissegundos através da internet das coisas (Internet Of things).

O presente trabalho tem como objectivo desenvolver uma proposta de um sistema de controlo de acesso em áreas restritas do bloco operatório do hospital central de Maputo usando autenticação por RFID e gerenciamento por meio de software web. Será feita a integração de um sistema embarcado que será responsável por colectar a informação de um usuário e enviar essa informação para um software que realiza todo o gerenciamento do controlo de acesso de usuários, permitindo ou não o usuário ter o acesso ao local e salvando todo seu histórico em banco de dados para que um supervisor tenha controlo sobre seus colaboradores.

1.2. Definição do Problema

A pandemia do novo Coronavírus Covid 19 impactou o mundo inteiro. Enquanto alguns locais fecham, outros vêem sua demanda aumentar significativamente, o que é o caso do Hospital Central de Maputo. Nos últimos dias o Hospital tem visto o fluxo de pessoas aumentar, o que consequentemente requer um aumento da segurança.

O bloco operatório é um sector com acesso limitado e devido em três áreas nomeadamente área irrestrita (secretaria, vestiários, área de transferência, corredor de entrada), área semi - restrita (salas de estar, descanso e de preparo do material) e áreas restritas (salas cirúrgicas, de recuperação pós-anestésica e corredor interno), por conta disso necessita de um sistema de controlo de acesso físico que atenda as normas da Agencia Nacional de Vigilância sanitária (Anvisa).

O monitoramento em tempo real de entradas e saídas nessas instituições é complexo, há áreas que a entrada é permitido a um determinado grupo (Funcionários e emergências). Isso faz com que cada área esteja protegida da forma mais adequada, resguardando equipamentos e dados críticos.

A falta de um controle de acesso bem estruturado em hospitais os torna sujeitos a uma série riscos. Alguns exemplos são o roubo de medicamentos, saídas de pacientes sem autorização médica, entrada de pessoas não autorizadas.

1.3. Relevância da pesquisa

Nos últimos anos, tem sido uma tendência a utilização da tecnologia no dia-a-dia do ser humano, em diversos sectores e áreas da sua vida. No que diz respeito à tecnologia de Controlo

de Acesso, a segurança Electrónica tem muito a somar neste segmento, pois disponibiliza soluções modernas e eficientes para uma rotina mais tranquila tanto para profissionais da saúde, quanto para pacientes e visitantes

O controlo de acesso no Bloco Operatório da HCM é indispensável, para evitar que certo grupo de pessoa tenha acesso a áreas restritas, este sistema ira facilitar entradas e saídas e auxiliar o sector de Recursos Humanos por trazer informações sobre a jornada de trabalho de cada colaborador.

1.4. Objectivos

1.4.1. Objectivo Geral

Desenvolver uma proposta de um Sistema de controlo de Acesso em Área restrita do Bloco Operatório do Hospital Central de Maputo usando autenticação por RFID e gerenciamento por meio de software WEB

1.4.2. Objectivos Específicos

- Desenvolver um protótipo de um sistema embarcado de fechaduras electrónicas integrado leitores de Rfid e Led;
- Desenvolver um Sistema Web para o monitoramento;
- Usar o Servidor Microsoft SQL para Base de dados;
- Ter um Histórico;
- Explicar o principio de funcionamento do Sistema de controlo de Acesso.

1.5. Justificativa

O âmbito da escolha do tema surgiu numa experiência pratica no HCM que UTL presta serviços na automatização das portas do Banco de Socorro, que esta em reabilitação e requalificação total, fiquei encantado pelo alto preço dos Sistemas de Controlo de Acesso comerciais, e a falta de recursos avançados em alguns deles, como permissões de agendamento, capacidade de controlar vários sectores por Wi-Fi, facilitar actualização de dados de usuários no banco de dados, possuir um hardware externo (como servidores), interface baseada em página da web e muitos outros. Desta forma, pretendo desenvolver um Sistema de Controle de Acesso que contenha todas as funcionalidades mencionadas, mantendo um preço abaixo, com o uso da tecnologia IoT para permitir a integração com outros sistemas e baseado em Wi-Fi.

A tecnologia RFID se tornou uma maneira fácil e barata de identificar usuários. Além disso, a área de Sistemas de Controlo de Acesso tem grande importancia na actualidade, quando questões envolvendo privacidade e segurança estão em alta. Para resolver esse problema de privacidade e segurança a maior parte das empresas tem adoptado esses tipos de sistemas de segurança..

1.6. Metodologia

Este projecto baseia - se numa pesquisa aplicada que visa a aplicar conhecimentos na área de Segurança Electrónica. Pretendo fazer uma abordagem quantitativa de dados já existentes, pesquisa explicativa de como se beneficiar com uso do Sistema de controlo de Acesso. A técnica aplicada obedeceu o esquema abaixo.

- Pesquisa bibliográfica;
- Pesquisa documental;
- Observação;
- Estudo de Caso;
- Estudo de campo;
- Escolha de Materiais e Tecnologias Envolvida

2. Referências Biográficas

Barros, A., Dantas, R., & Silva, G. d. (05 de Dezembro de 2018). Software de Registro de Presença em Sistema Embarcado com Integração Web. doi:https://doi.org/10.5753/epoca.2018.13453

Camargo, M. d. (04 de Agosto de 2021). Desenvolvimento de sistema de monitoramento com IoT de baixo custo para equipamentos médicos. Obtido em 26 de Novembro de 2021, de https://repositorio.unifesp.br/handle/11600/61522

Costa, A. M. (2018). RFControl : sistema de gerência de estoque utilizando RFID. Obtido em 2021 de Novembro de 26 , de http://www.monografias.ufop.br/handle/35400000/821

Fernandes, A. C. (2017). Free Pass - Sistema de controle de acesso utilizando cartões de proximidade RFID. Obtido em 26 de Novembro de 2021, de http://hdl.handle.net/1884/48216

Francelino, F. A., & Tomazeti, D. M. (s.d.). AcessaIFSP: Sistema para Controle de Acesso. Obtido em 26 de Novembro de 2021, de https://suap.ifsp.edu.br/media/edu/projeto_final/TCC_Fabio_Francelino.pdf

Gonçalves, V. R. (2019). Sistema de controle de acesso utilizando autenticação por RFID e gerenciamento por meio de software WEB. Obtido em 2021 de Novembro de 26, de https://monografias.ufop.br/bitstream/35400000/2222/3/MONOGRAFIA_SistemaControleAcesso.pdf

GUIMARÃES, A. R. (Setembro de 2014). Proposta de um sistema de controle de acesso utilizando tecnologia RFID. Obtido em 26 de Novembro de 2021, de http://dspace.sti.ufcp.edu.br:8080/jspui/handle/riufcp/18256

LOSI, R. A. (2015). PROTÓTIPO DE INVENTÁRIO AUTOMATIZADO COM RFID. Obtido em 26 de Novembro de 2021, de http://dsc.inf.furb.br/arquivos/tccs/monografias/2016_2_rafael-antonio-losi_monografia.pdf

Narciso, M. G. (2008). APLICAÇÃO DA TECNOLOGIA DE IDENTIFICAÇÃO POR RÁDIOFREQÜÊNCIA (RFID) PARA CONTROLE DE BENS PATRIMONIAIS PELA WEB. Obtido em 26 de Novembro de 2021, de https://www.alice.cnptia.embrapa.br/bitstream/doc/17793/1/rfid.PDF

Oliveira, S. d. (2017). *Internet das Coisas com ESP8266, Arduino e Raspberry Pi* (Vol. i). (C. Kuwabata, Ed.) São Paulo, SP Brasil: Novatec Editora Ltda. Obtido em 26 de Novembro de 2021, de https://dokumen.pub/download/internet-das-coisas-com-esp8266-arduino-e-raspberry-pi-1nbsped-8575225812-9788575225813.html

Penckowski, V. (2021). User access control system based on ESP32 technology. Obtido em 26 de Novembro de 2021, de http://hdl.handle.net/10198/23662

QUARANTA, T. C. (2019). Projeto e desenvolvimento de sistema de gestão de atendimento a pacientes em internação hospitalar. Obtido em 26 de Novembro de 2021, de https://repositorio.utfpr.edu.br/jspui/bitstream/1/24380/1/atendimentopacientesinternacaohospitalar.pdf

Santiago, V. G. (2015). Registrador de eventos sobre uma plataforma com microcontrolador parallax propeller e interface web. Obtido em 26 de Novembro de 2021, de http://www.tce.sc.usp.br/tce/disponiveis/97/970010/tce-05012016-174557/publico/Santiago_Valter_Gabriel_Paes_tce.pdf

Vilante, L. d. (2007). Gereneiamento de Dados em Hospitais utilizando Sensores e RFID. Obtido em 26 de Novembro de 2021, de http://dspace.sti.ufcg.edu.br:8080/jspui/bitstream/riufcg/17348/1/LEANDRO%20DE%20SOUZA%20VILANTE%20-%20TCC%20ENG.%20EL%C3%89TRICA%202007.pdf

Weles, E. F., & Bruno, D. O. (25 de Agosto de 2018). PROTÓTIPO PARA UM SISTEMA DE AUTOMAÇÃO DE CONTROLE PATRIMONIAL UTILIZANDO TECNOLOGIA RFID. Obtido em 26 de Novembro de 2021, de http://revistabrmecatronica.com.br/ojs/index.php/revistabrmecatronica/article/view/47/46

UNIVERSIDADE EDUARDO MONDLANE

Faculdade de Engenharia

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

CREDENCIAL

Para os efeitos julgados conveniente, e credenciado o estudante, **José Catine Munguambe Júnior** do 5º ano do curso de Engenharia Eletrónica do regime laboral para recolha de dados no Hospital Central de Maputo, para ajudar na realização do Estágio Profissional.

Maputo, 19 de Outubro de 2021

O Chefe do Departamento,

FACULDADE DE ENGENHARIA

Mestre José Nelsen Cuamba, engº.

(Assistente Universitário)

Av. de Moçambique, Km 1,5, C. Postal 257, Tel.: (+258) 21 475315, Fax.: (+258) 21 475311,
Maputo – Moçambique

REPÚBLICA DE MOÇAMBIQUE
BILHETE DE IDENTIDADE
Nº :110501558845P
Nome/Name :
JOSÉ CATINE MUNGUAMBE JÚNIOR
Data de Nascimento/ Birthdate :
17/07/1999
Naturalidade/ Place of Birth :
CIDADE DE MAPUTO
Nome do Pai / Father's Name :
JOSE CATINE MUNGUAMBE
Nome da Mãe / Mother's Name :
MELTA VICENTE MUNGUAMBE
Estado Civil / Marital Status : SOLTEIRO
Local de Residência / Address :
-
Sexo / Sex : M
Altura / Height : 1,70m
Assinatura do Portador / Signature :
22

Emitido em / Issued in :
CIDADE DA MATOLA
Data de emissão / Issuance date :
09/03/2017
Validade / Expiration date :
09/03/2022
Director Nacional / The National Director :
BIMOZ01558845<803638991<<<<<<<
9907179M2203090MOZ11051001P<<3
MUNGUAMBE<JUNIOR<<JOSE<CATINE<

ANEXO 3: Pesquisa de campo no HCM

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA ELECTRÓNICA

PROPOSTA DE UM SISTEMA DE CONTROLO DE ACESSO EM ÁREAS RESTRITAS DO BLOCO OPERATÓRIO DO HOSPITAL CENTRAL DE MAPUTO USANDO AUTENTICAÇÃO POR RFID E INTERFACE WEB

1. Marque com X, o papel que exerces no HCM?

☐ Funcionário ☐ Colaborador ☐ Paciente ☐ Acompanhante

2. Quantos sectores tem o Bloco Operatório?

2.1. Quais são os Sectores de acesso restrito?

3. Existe um sistema de Controlo de Acesso?

3.1. Se sim, qual?

4. Existe um sistema de Monitoramento de entrada e saídas?

4.1. Se sim, qual?

5. Conheces sistema de controlo de acesso electrónico?

5.1. Se sim, qual é a sua opinião desses sistemas nos hospitais?

Anexo 4: Algoritmo de funcionamento do protótipo na linguagem C++

```
//*******************************libraries********************************

//RFID----------------------------

#include <SPI.h>

#include <MFRC522.h>

//NodeMCU-------------------------

#include <NTPClient.h>

#include <WiFiUdp.h>

#include <ESP8266WiFi.h>

#include <ESP8266HTTPClient.h>

#include <WiFiClient.h>

#include <LiquidCrystal_I2C.h>

//#include <Servo.h>

//#define SERVO_PIN  D0

//*************************************************************************

#define SS_PIN D4  //--> SDA / SS is connected to pinout D2

#define RST_PIN D3  //--> RST is connected to pinout D1

//*************************************************************************

MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.

LiquidCrystal_I2C lcd(0x27, 16, 2);

//*************************************************************************

/* Set these to your desired credentials. */
```

```
const char* ssid = "Martins";

const char* password = "844218018";

const char* device_token  = "e055e7bf2db22fb3";

//************************************************************************

WiFiUDP ntpUDP;

NTPClient timeClient(ntpUDP, "pool.ntp.org");

String URL = "http://192.168.43.120/controlo_acesso_hcm/getdata.php"; //computer IP or the server domain

String getData, Link;

String OldCardID = "";

unsigned long previousMillis = 0;

String weekDays[7]={"Domingo", "Segunda", "Terca", "Quarta", "Quinta", "Sexta", "Sabado"};

//Month names

String months[12]={"Jan.", "Fever.", "Marc", "Abril", "Maio", "Junho", "Jullho", "Agosto", "Setem", "Outubro", "Novem", "Dizem"};

//************************************************************************

void setup() {

  delay(1000);

  Serial.begin(115200);

  //servo.attach(SERVO_PIN);    // attaches the servo on pin 9 to the servo object

  //servo.write(angle);

  SPI.begin();  // Init SPI bus
```

```
  mfrc522.PCD_Init(); // Init MFRC522 card
  delay(500);
  lcd.begin();                // Initialize 16x2 LCD Display
  lcd.clear();
  pinMode(D0, OUTPUT);
   digitalWrite(D0, HIGH);
  timeClient.begin();
  timeClient.setTimeOffset(0);
}
//************************************************************************
void loop() {
   //check if there's a connection to Wi-Fi or not
  if(!WiFi.isConnected()){
    connectToWiFi();    //Retry to connect to Wi-Fi
  }
  //-----------------------------------------
  if (millis() - previousMillis >= 15000) {
    previousMillis = millis();
    OldCardID="";
    relogio();
   delay(20);
  }
```

```
  delay(50);
 //--------------------------------------------
//look for new card
if ( ! mfrc522.PICC_IsNewCardPresent()) {
  return;//got to start of loop if there is no card present
}
// Select one of the cards
if ( ! mfrc522.PICC_ReadCardSerial()) {
  return;//if read card serial(0) returns 1, the uid struct contians the ID of the read card.
}
String CardID ="";
for (byte i = 0; i < mfrc522.uid.size; i++) {
  CardID += mfrc522.uid.uidByte[i];
}
//--------------------------------------------
if( CardID == OldCardID ){
  return;
}
else{
  OldCardID = CardID;
}
 //--------------------------------------------
```

```
//  Serial.println(CardID);
  SendCardID(CardID);
  delay(1000);
  }
//************send the Card UID to the website*************
void SendCardID( String Card_uid ){
   lcd.clear();
  Serial.println("Sending the Card ID");
  lcd.setCursor(0, 0);
    lcd.print("Enviando o Card ID");
    if(WiFi.isConnected()){
    WiFiClient client;
    HTTPClient http;    //Declare object of class HTTPClient
    //GET Data
    getData = "?card_uid=" + String(Card_uid) + "&device_token=" + String(device_token); // Add the Card ID to the GET array in order to send it
    //GET methode
    Link = URL + getData;
    http.begin(client, Link); //initiate HTTP request   //Specify content-type header

    int httpCode = http.GET();   //Send the request
    String payload = http.getString();    //Get the response payload
```

```
//    Serial.println(Link);   //Print HTTP return code
    Serial.println(httpCode);   //Print HTTP return code
    Serial.println(Card_uid);     //Print Card ID
    Serial.println(payload);//Print request response payload
        if (httpCode == 200) {
      if (payload.substring(0, 5) == "login") {
        String user_name = payload.substring(5);
      Serial.println(user_name);
       lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Bem Vindo");
     lcd.setCursor(0, 1);
    lcd.print(user_name);
  digitalWrite(D0,LOW );   // turn the LED on (HIGH is the voltage level)
     delay(3000);                       // wait for a second
     digitalWrite(D0, HIGH);    // turn the LED off by making the voltage LOW


      }
      else if (payload.substring(0, 6) == "logout") {
        String user_name = payload.substring(6);
     Serial.println(user_name);
```

```
 lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Obrigado");
lcd.setCursor(0, 1);
lcd.print(user_name);
 digitalWrite(D0,LOW );   // turn the LED on (HIGH is the voltage level)
 delay(3000);                       // wait for a second
 digitalWrite(D0, HIGH);
      }
  else if (payload == "succesful") {
  }
  else if (payload == "available") {

  }
   else if (payload == "Not Allowed!") {
     lcd.clear();
     lcd.setCursor(0, 0);
     lcd.print("Nao tem");
     lcd.setCursor(0, 1);
     lcd.print("Permissao");
  }
  else if (payload == "Not found!") {
```

```
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Cartao nao");
        lcd.setCursor(0, 1);
        lcd.print("Registado");
      }
      delay(100);
      http.end();  //Close connection
    }
    else if(httpCode == -1) {
       lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Problemas com");
        lcd.setCursor(0, 1);
        lcd.print("a conexao!");
          }
  }
  }
//********************connect to the WiFi******************
void connectToWiFi(){
   WiFi.mode(WIFI_OFF);          //Prevents reconnection issue (taking too long to connect)
```

```
delay(1000);
WiFi.mode(WIFI_STA);
Serial.print("Connecting to ");
Serial.println(ssid);
WiFi.begin(ssid, password);
 lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Connecting to ");
lcd.setCursor(0, 1);
lcd.print(ssid);

while (WiFi.status() != WL_CONNECTED) {
  delay(500);
  Serial.print(".");
}
Serial.println("");
Serial.println("Connected");

Serial.print("IP address: ");
Serial.println(WiFi.localIP());  //IP address assigned to your ESP
 lcd.clear();
lcd.setCursor(0, 0);
```

```
    lcd.print("Conectado IP:");
    lcd.setCursor(0, 1);
    lcd.print(WiFi.localIP());

    delay(700);

}
void relogio() {
  timeClient.update();

  time_t epochTime = timeClient.getEpochTime();
  Serial.print("Epoch Time: ");
  Serial.println(epochTime);

  String formattedTime = timeClient.getFormattedTime();
  Serial.print("Formatted Time: ");
  Serial.println(formattedTime);

  int currentHour = timeClient.getHours();
  Serial.print("Hour: ");
  Serial.println(currentHour+2);
```

```
int currentMinute = timeClient.getMinutes();
Serial.print("Minutes: ");
Serial.println(currentMinute);

int currentSecond = timeClient.getSeconds();
Serial.print("Seconds: ");
Serial.println(currentSecond);

String weekDay = weekDays[timeClient.getDay()];
Serial.print("Week Day: ");
Serial.println(weekDay);

//Get a time structure
struct tm *ptm = gmtime ((time_t *)&epochTime);

int monthDay = ptm->tm_mday;
Serial.print("Month day: ");
Serial.println(monthDay);

int currentMonth = ptm->tm_mon+1;
Serial.print("Month: ");
Serial.println(currentMonth);
```

```
  String currentMonthName = months[currentMonth-1];
  Serial.print("Month name: ");
  Serial.println(currentMonthName);


  int currentYear = ptm->tm_year+1900;
  Serial.print("Year: ");
  Serial.println(currentYear);


  //Print complete date:
  String currentDate = String(monthDay) + " " + String(currentMonthName) + " " + String(currentYear);
  String Hora = String(weekDay)+ " " + String(currentHour+2) + ":" + String(currentMinute);
  Serial.print("Current date: ");
  Serial.println(currentDate);
  lcd.clear();
  lcd.setCursor(0, 0);
    lcd.print(Hora);
    lcd.setCursor(0, 1);
    lcd.print(currentDate);
  Serial.println("");
```

```
}

//=============================================================================
======
```

Anexo 5 – Esquema Eléctrico