TÉCNICO LISBOA

Monitorização Electrónica baseada em Dispositivos Móveis para o Controlo de Doenças Contagiosas

Diogo Agostinho Borda de Água Reis

Dissertação para obtenção do Grau de Mestre em

Engenharia Electrotécnica e de Computadores

Orientador: Professor José Eduardo Charters Ribeiro da Cunha Sanguino

Júri

Presidente: Professor Paulo Luís Serras Lobato Correia
Orientador: Professor José Eduardo Charters Ribeiro da Cunha Sanguino
Vogais: Professor Pedro Joaquim Amaro Sebastião

Novembro 2021

Declaração

Declaro que o presente documento é um trabalho original da minha autoria e que cumpre todos os requisitos do Código de Conduta e Boas Práticas da Universidade de Lisboa.

Agradecimentos

Uma dissertação de mestrado é um trabalho longo, que inclui um trajeto repleto de inúmeros desafios e conquistas, altos e baixos, tristezas e alegrias. Contudo, apesar de por vezes um pouco solitário, reúne o contributo de várias pessoas, indispensáveis para a conclusão deste trabalho, às quais faz sentido agradecer e dedicar esta dissertação.

O primeiro agradecimento é dedicado ao meu orientador, Professor José Sanguino, do Instituto Superior Técnico. Agradeço a orientação exemplar pautada por um elevado e rigoroso nível científico, por uma visão crítica e oportuna e pelo seu empenho, os quais contribuíram para enriquecer o trabalho realizado.

Ao Instituto de Telecomunicações pelos recursos disponibilizados que foram uma mais valia para a conclusão desta dissertação.

Quero agradecer também a todos os familiares que sempre me apoiaram nesta etapa curricular Mãe, pai, mana, mano, avó, João e Maria Inês, obrigado pelo vosso apoio incondicional que, sempre estando presentes, me ajudaram com que concluísse esta etapa com sucesso.

Aos meus colegas de Engenharia Electrotécnica e de Computadores e de outros cursos do Instituto Superior Técnico. Todos os trabalhos desenvolvidos com vocês e todas as conversas dentro e fora de aulas, permitiram que desenvolvesse o espírito crítico sobre as matérias em estudo e permitiram a troca mútua de ideias e melhorias para a dissertação.

E, por fim, mas não menos importante, a todos os meus amigos de sempre e para sempre, que sempre me apoiaram em todos os momentos. Estiveram nos dias bons, em que o desenvolvimento da dissertação corria como planeado, e estiveram também nos dias menos bons, onde os falhanços assumiam o controlo do dia e o mau humor predominava.

A todos, os meus sinceros agradecimentos.

Abstract

Infectious-contagious diseases are becoming increasingly common in society, at the present time we live in. They have a great propagation capacity and it turns out to be difficult to control them in space and time. With this problem, it was born a need to create a system capable of monitoring the evolution of the infection of diseases, in real time.

In order to be able to monitor the infection, a system capable of collecting navigation data from its users was designed. This collection is done through an application with the ability to collect GPS coordinates and the names of available Wi-Fi networks. This data is transmitted to a server capable of storing and processing it. Beyond the application, there is also a website, in which, not only, a map where the different concentration of infected people can be seen, but also, a list containing the names of the networks, where there are more infected people. On the website, it is also possible for healthcare professionals to add an infected user.

After the development of the entire system, it was necessary to test it. During the testing of the system, several scenarios were studied, namely the consequences of inserting positive users to the disease. These consequences created the expected results which are the marking of users who have been with infected ones and who are at risk of contracting the disease. It was also during the testing phase of the system that some susceptible aspects bound to improve for a next phase of development were verified.

Keywords

GPS, Wi-Fi, Tracking, App, Pandemic, Disease

Resumo

As doenças infectocontagiosas são cada vez mais comuns na sociedade, nos tempos que decorrem. Elas têm grande capacidade de propagação e torna-se difícil controlá-las no espaço e no tempo. Deste problema, nasceu a necessidade de criar um sistema capaz de monitorizar a evolução, em tempo real, do contágio das doenças.

A fim de ser possível haver a monitorização do contágio, desenhou-se um sistema capaz de recolher dados de navegação dos seus utilizadores. Essa recolha é possível através de uma aplicação com a capacidade de recolher coordenadas GPS e os nomes das redes Wi-Fi disponíveis. Esses dados são transmitidos para um servidor capaz de os armazenar e processar. A par da aplicação, existe também um website, no qual é possível ver um mapa onde há maior concentração de pessoas infetadas e onde existe uma lista contendo os nomes das redes onde existem mais pessoas infetadas. No website, é também possível os profissionais de saúde inserirem um utilizador infetado.

Após desenvolvido todo o sistema, foi necessário proceder à sua testagem. Durante a testagem do sistema, foram estudados vários cenários, nomeadamente as consequências de inserir utilizadores positivos à doença. Essas consequências criaram os resultados espectáveis que são a marcação de utilizadores que estiveram com utilizadores infetados e que correm o risco de virem a contrair a doença. Foi também durante a fase de testagem do sistema que se verificou alguns aspetos suscetíveis a melhorias numa próxima fase de desenvolvimento.

Palavras Chave

GPS, Wi-Fi, Monitorização, Aplicação, Pandemia, Doença

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos

AES	Norma de Criptografia Avançada
API	Application Programming Interface
BLE	Bluetooth Low Energy
CA	Certificado de Acesso
CL	Código de Legitimação
DP-3T	Decentralized Privacy-Preserving Proximity Tracing
GAEN	Google-Apple Exposure Notification
GPS	Global Positioning System
HMAC	Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
JSON	Javascript Object Notation
MAC	Media Access Control
REST	Representational State Transfer
RGPD	Regulamento Geral sobre a Proteção de Dados
RPI	Rolling Proximity Identifier
SDK	Kit de Desenvolvimento de Software
SLD	Servidor de Legitimação de Diagnósticos
SOAP	Simple Object Access Protocol
SPD	Servidor de Publicação de Diagnósticos
SQL	Structured Query Language
SSID	Service Set Identifier
TCP	Transmission Control Protocol

TEK Temporary Exposure Key

UDP User Datagram Protocol

Wi-Fi Wireless Fidelity

1

Introdução

As doenças infecto-contagiosas são cada vez mais comuns na sociedade, nos tempos que decorrem. Cada vez há mais doenças e, cada vez mais, elas são propagadas com grande rapidez. É, portanto, cada vez mais difícil de as controlar no espaço e no tempo.

Com o aparecimento de uma nova doença infecto-contagiosa, as autoridades de saúde procedem com o desenvolvimento de medicação para o tratamento da doença e com o desenvolvimento de uma vacina.

No final do ano de 2019, um novo vírus foi descoberto, o SARS-CoV-2. Este vírus, quando contraído pelos humanos, pode provocar o desenvolvimento da sua doença, a COVID-19. Este vírus, tem a especial característica de ser altamente propagado através do contacto humano, de poder ou não dar sintomas e, esses sintomas apenas se revelarem uns dias após a contração do vírus. Todos estes fatores, ajudam a propagação do vírus.

Visto que este vírus era totalmente desconhecido, não havia qualquer tipo de medicação para curar a COVID-19 nem nenhuma vacina para prevenir a contração do vírus. Tendo isto em conta, o mundo entrou todo em estado de alerta. Os cidadãos ficaram em quarentena e todos os serviços não essenciais à vida humana foram cancelados. O mundo ficou em serviços mínimos.

Conclui-se que as doenças infecto-contagiosas têm um grande efeito na vida social da população, podendo condicionar os seus movimentos.

Tendo em conta todas estas condicionantes que uma doença infecto-contagiosa pode originar, decidiu-se desenvolver uma aplicação que monitorize uma população de indivíduos potencialmente contagiados por doenças infecto-contagiosas a nível global.

O trabalho desta dissertação inicia com a pesquisa do trabalho já existente nesta área. Começa-se por verificar as aplicações já desenvolvidas e que tecnologias usam. Estuda-se também quais são as tecnologias de interesse a aplicar na aplicação a desenvolver, nomeadamente o GPS e o Wi-Fi.

De seguida, propõe-se o desenvolvimento da aplicação para dispositivos móveis. Paralelamente à aplicação, será também desenvolvido um servidor e um website.

Com recurso às tecnologias supra-mencionadas, será possível mapear zonas de risco, tendo em conta o número de utilizadores infetados por região. Através do registo de infeções, tenciona-se também criar uma lista de utilizadores em risco de infeção, isto é, utilizadores que não estão confirmados positivos à doença mas que, devido a terem estado próximos a utilizadores infetados, estão em risco de contraírem a doença. Todas estas informações serão guardadas no servidor e acessíveis através do website.

2

Estado de Arte

Conteúdo

Este capítulo debruçar-se-á acerca do processo de pesquisa que foi feito para a elaboração da dissertação. Começa-se pela explicação de todos os processos de comunicação e do modo de funcionamento de aplicações já existentes no mercado. Verifica-se, também, quais são as aplicações que existem no mercado, fazendo um breve estudo sobre cada uma dessas aplicações. Por fim, descreve-se que tecnologias são usadas para a elaboração de todo o *software* da aplicação.

2.1 Modo de Funcionamento

Após um breve estudo sobre as aplicações existentes no mercado, que será detalhado na seção 2.2, verificou-se que todas têm um modo de funcionamento [1] semelhantes.

Inicialmente, é importante referir que há três entidades importantes deste sistema. As entidades são os utilizadores finais da aplicação, o Servidor de Legitimação de Diagnósticos (SLD) e o Servidor de Publicação de Diagnósticos (SPD). Com as constantes evoluções e atualizações das aplicações, a segurança e a confidencialidade dos utilizadores também foi melhorando, devido à possibilidade de eventuais ataques informáticos. O modo como as aplicações previnem esses ataques informáticos será também explicado.

2.1.1 Funcionamento da Aplicação de Utilizador

A aplicação de utilizador comum é a aplicação que está disponível a todos os cidadãos, através das lojas online de aplicações móveis. Esta aplicação permite uma localização relativa entre utilizadores, que posteriormente comunica com os servidores para o armazenamento de dados.

Para o correto funcionamento da aplicação, é necessário que o Bluetooth e as Google-Apple Exposure Notification (GAEN) estejam ligadas. Estas tecnologias serão explicadas em detalhe na seção 2.3.1 e na seção 2.3.2, respetivamente.

Quando ativa em segundo plano, a aplicação está em constante escuta e envio de dados, através de bluetooth.

Diariamente, é gerada uma chave aleatória de 360 bit, que é denominada de Temporary Exposure Key (TEK). Cada chave diária TEK é usada numa função pseudo-aleatória do tipo HMAC-SHA256 (seção 2.3.3) que, por sua vez, é usada noutra função pseudo-aleatória do tipo da Norma de Criptografia Avançada (AES) (seção 2.3.4). Esta última função retorna uma chave de tamanho 144 x 16 bytes, que correspondem a 144 pequenas chaves, onde cada uma dessas chaves é denominada de Rolling Proximity Identifier (RPI).

A cada 10 minutos, 1 RPI é difundido via bluetooth. Portanto são difundidos 6 RPI por hora, equivalendo a 144 RPI diários. Essa difusão é feita para todos os dispositivos que estejam a poucos metros

do telemóvel. Cada dispositivo guarda durante 14 dias todas as TEK geradas. Após os 14 dias, todas as TEK guardadas são eliminadas automaticamente.

Um dispositivo móvel, enquanto está a difundir um RPI, pode também estar a receber vários RPI. Cada RPI é armazenado também durante os 14 dias. Juntamente com RPI recebidos, são também guardados alguns parâmetros de interesse, tais como a potência do sinal recebido e a duração do estabelecimento da ligação.

O facto de existir uma troca de RPI em curtos intervalos de tempo, dificulta o seguimento de cada dispositivo móvel, havendo apenas uma informação acerca da posição relativa entre dois dispositivos.

Como será explicado mais adiante neste capítulo, a aplicação está em constante comunicação com o Servidor de Legitimação de Diagnósticos e com o Servidor de Publicação de Diagnósticos. Quando um utilizador fica positivo à doença, é para o SPD que a aplicação transmite as TEK.

Em funcionamento normal, a aplicação também comunica com o SPD duas vezes por dia. Essas comunicações, que não têm hora definida, têm como objetivo obter as novas chaves TEK que tenham sido publicadas recentemente. Após descarregadas as novas chaves TEK, a aplicação procede com a comparação dessas chaves com as que tinham sido recebidas por bluetooth. Caso coincidam, avalia-se se o contacto foi de risco ou não.

2.1.2 Servidor de Legitimação de Diagnósticos

O Servidor de Legitimação de Diagnósticos (SLD) implementa um sistema em que apenas utilizadores com diagnóstico positivo à doença partilhem as suas TEK. Para que tal mecanismo seja assegurado, é necessário que um profissional de saúde insira um novo registo de infeção para o utilizador infetado. Nesta etapa, é bastante importante que o médico questione a data em que os primeiros sintomas apareceram.

Para aceder ao SLD, o médico tem que se autenticar com o seu cartão de cidadão ou com a sua cédula profissional. Após a autenticação, este servidor fornece dois códigos: um Código de Legitimação (CL) e um Certificado de Acesso (CA).

O Código de Legitimação é um código composto por 12 algarismos e é fornecido ao médico, sendo o médico responsável por transmiti-lo ao doente. Não há qualquer meio de transmissão predefinido para o médico transmitir o código ao doente, podendo ser verbal ou eletronicamente. É nesta fase que o médico insere a data dos primeiros sintomas, questionado previamente ao doente.

Após recebido o CL, o doente tem que o inserir na aplicação. Por sua vez, a aplicação comunica com o SLD e é obtido o Certificado de Acesso. O CA será importante para a interação da aplicação do doente com o Servidor de Publicação de Diagnósticos. No CA está também contido a data dos primeiros sintomas (inserido previamente pelo médico) subtraído de 3 dias, que corresponde ao início do período em que há um maior risco de contágio. Por fim, e com recurso ao CA, a aplicação acede ao

SPD e partilha as TEK dos dias a partir da data que está no CA.

Devido à grande importância que todo este sistema tem, a aplicação e as devidas comunicações com os servidores são suscetíveis a ataques informáticos. A fim de garantir que a aplicação entrega o Código de Legitimação apenas ao verdadeiro SLD, e que não é suscetível a ataques do tipo *man-in-the-middle*, o certificado SLD é conhecido previamente e usado para validar todas as interações do SLD (*certificate pinning*). As aplicações também simulam a troca de Código de Legitimação por Certificado de Acesso no SLD, de forma a dificultar eventuais tentativas de obtenção de informações dos utilizadores, através da análise do tráfico de rede.

Tendo em conta que o acesso ao SLD por parte dos utilizadores não é autenticado, este servidor é sensível a acessos abusivos para obtenção de um Certificado de Acesso existente. Esses acessos são feitos por força-bruta ou por saturação e consequente quebra de serviço. A mitigação a estes ataques é efetuada recorrendo a técnicas devidamente comprovadas.

2.1.3 Servidor de Publicação de Diagnósticos

O Servidor de Publicação de Diagnósticos (SPD) destina-se apenas ao armazenamento de dados. Estes dados são as TEK de cada utilizador.

Quando um utilizador acusa positivo, e após todo o processo de obtenção de um Certificado de Acesso (CA) no SLD, a aplicação faz um carregamento das TEK do doente para o SPD, correspondentes aos dias em que houve probabilidade de estar infetado.

Todas as chaves TEK guardadas neste servidor, são guardadas por um período máximo de 14 dias. É também validado o certificado do SPD (*certificate pinning*) de forma a garantir que as chaves TEK não são intercetadas por qualquer intermediário. Para que haja uma segurança ainda maior, as aplicações simulam a entrega das chaves TEK ao SPD, dificultando eventuais tentativas de identificação dos utilizadores, através da análise do tráfego da rede.

O acesso a estas chaves é proporcional ao número de utilizadores ativos. Portanto, para que a resposta seja eficaz, os acessos ao SPD por parte das aplicações são distribuídas de forma aleatória no tempo, estando o SPD equipado com mecanismos de replicação e caching.

2.2 Aplicações Semelhantes Existentes

No início da pandemia, muitos foram os projetos de empresas e de universidades que tinham como objetivo encontrar uma maneira de poder controlar a pandemia. É importante fazer um rastreamento da evolução da pandemia, assim como dos eventuais contactos de risco mas, mais importante ainda, é assegurar a privacidade das pessoas e o cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD).

É sobre estes projetos que este capítulo incide. Enquanto uns projetos não tiveram qualquer desenvolvimento, outros foram desenvolvidos até à sua fase final, a aplicação. Estas aplicações são também as aplicações de referência nalguns países.

2.2.1 StayAway COVID

Esta aplicação é a aplicação oficial usada em Portugal no rastreio da COVID-19 [2, 3].

Figura 2.1: Logótipo da aplicação StayAway Covid

Esta aplicação, recomendada pela Direção Geral da Saúde Portuguesa, tem como princípios orientadores a utilidade, liberdade e transparência. É útil no rastreio da COVID-19. É livre na sua utilização, que é voluntária e não discriminatória. E é também transparente, na medida e que todo o seu código de desenvolvimento do software está disponível. A aplicação garante ainda o anonimato e o respeito pela legislação europeia e nacional, aplicável à proteção de dados pessoais.

A StayAway Covid faz uma extensa recolha de informações de possíveis exposições ao vírus usando, para tal, uma lista de contactos recentes. Permite, então, que uma pessoa seja alertada quando exposta a fatores de risco de contacto.

Este projeto resultou de uma iniciativa, no âmbito do programa INCoDe.2030, com o objetivo de desenvolver uma solução de rastreio digital de contactos para prevenir e mitigar a propagação da COVID-19. Esta solução apresentada, decorreu do trabalho de investigação desenvolvido no projeto Decentralized Privacy-Preserving Proximity Tracing (DP-3T) [4]. O projeto DP-3T é um sistema digital de rastreio de proximidade que pretende preservar a privacidade e a segurança dos utilizadores. Todos estes projetos foram desenvolvidos na Universidade do Porto. Do projeto DP-3T resultou um Kit de Desenvolvimento de Software (SDK) que implementa todo o protocolo de geração de chaves aleatórias, difusão e receção de identificadores aleatórios.

O modo de funcionamento desta aplicação foi descrito na seção 2.1. Muitas das funcionalidades desenvolvidas inicialmente neste projeto foram incorporadas pelos sistemas operativos da Google-Apple Exposure Notification. Com o uso da GAEN, a aplicação passou a usar o SDK DP-3T para acesso da GAEN e para garantir a interoperabilidade com outras aplicações europeias.

Esta aplicação teve como base vários projetos, nomeadamente FollowMyHealth e a monitorCovid19.pt.

2.2.2 FollowMyHealth

O projeto FollowMyHealth [5] também nasceu na Universidade do Porto no âmbito da linha de financiamento ”Research4Covid19”. Este projeto tem como principal objetivo o desenvolvimento de uma aplicação capaz de fazer uma análise espacial.

A aplicação também visa melhorar o conhecimento sobre a sua transmissão. Com esse conhecimento, é possível parametrizar os modelos de transmissão do vírus, o que é possível fornecer ao utilizador uma espécie de indicador de auto-vigilância, através da avaliação e análise de cada local. Essa análise refere-se ao tipo de atividade exercida em cada local, a sua dimensão e o tempo que as pessoas permanecem nesse local. Através desta recolha de dados, é possível alertar os utilizadores da aplicação caso tenham estado ou se aproximem de locais com elevado potencial de contágio.

Outro objetivo desta aplicação é fazer o acompanhamento de pessoas que, devido a estarem infetadas ou tenham suspeita de infeção, estejam em isolamento profilático. Através deste acompanhamento, é possível também estudar o estado emocional das pessoas nos diferentes estados da pandemia.

2.2.3 monitorCovid19.pt

Este projeto [6] foi desenvolvido pelo Instituto de Engenharia de Sistemas e Computadores - Tecnologia e Ciência da Faculdade de Engenharia da Universidade do Porto.

O monitorCovid19.pt consistia no desenvolvimento de uma aplicação capaz de monitorizar e rastrear a circulação da população. Com esta monitorização, seria possível alertar as pessoas que tenham tido contacto direto com alguém infetado pelo SARS-COV-2.

2.2.4 TraceTogether

A aplicação oficial de rastreio da COVID-19 na Singapura é a TraceTogether [7].

Figura 2.2: Logótipo da aplicação TraceTogether

O modo de funcionamento da aplicação é semelhante ao descrito anteriormente.

A aplicação tem como lema: ”Protege-te, protege quem amas e protege a nossa comunidade”. Com o uso desta aplicação, é possível sermos rapidamente notificados acerca de contactos de risco que possam ter ocorrido. Ao ser rápido, é possível reduzir o contágio da COVID-19 pela comunidade.

A TraceTogether prima pela privacidade. A troca de informações que existem entre utilizadores que estejam próximos é feita com o consentimento de cada utilizador. As informações são trocadas através de bluetooth e os dados armazenados são automaticamente eliminados após 25 dias. É também garantido que não é guardado qualquer tipo de informações provindas de localização Global Positioning System (GPS), Wi-Fi ou da rede móvel.

Esta aplicação guarda ainda informações de cada utilizador, nomeadamente o número de telemóvel, os detalhes de identificação e um ID de utilizador completamente aleatório e anónimo. Estas informações estão guardadas num servidor e nunca são reveladas ao público.

A TraceTogether foi um exemplo a seguir para o desenvolvimento de outras aplicações.

2.2.5 PEPP-PT

O Pan-European Privacy-Preserving Proximity Tracing [8] é um sistema europeu de controlo da COVID-19, inspirado na aplicação TraceTogether.

Figura 2.3: Logótipo da PEPP-PT

Este sistema visa recolher as questões legais ao nível da privacidade dos utilizadores. É um sistema de *contact-tracing* com informação centralizada, cujo principal objetivo é rastrear os contactos de proximidade, informando as pessoas potencialmente expostas. Relativamente à privacidade dos utilizadores, este sistema tem duas abordagens: centralizada e descentralizada.

As críticas a este sistema revelam falta de transparência nas operações de software.

2.2.6 COVIDSafe

Esta é a aplicação oficial da Austrália para o controlo da pandemia de COVID-19 [9, 10].

Esta aplicação também foi inspirada na TraceTogether. Distingue-se das restantes na medida em que os dados de contacto de proximidade são guardados durante 21 dias, ao contrário dos 25 dias na TraceTogether. Os 21 dias são calculados através dos 14 dias de tempo de incubação do vírus, adicionando 7 dias referentes ao tempo que é necessário para confirmar um teste positivo.

Figura 2.4: Logótipo da aplicação COVIDSafe

Os dados armazenados não contemplam a localização GPS. Contemplam sim, os códigos trocados, o dia, a hora e a potência do sinal bluetooth recebido. Todos estes dados são encriptados.

Uma das críticas apontadas à aplicação é a invasão de privacidade.

2.2.7 SwissCovid

A aplicação SwissCovid [11, 12] é a aplicação oficial da Suíça para o rastreio da COVID-19.

Figura 2.5: Logótipo da aplicação SwissCovid

Esta aplicação resultou de uma projeto conjunto entre a École Polytechnique Fédérale de Lausanne e o Swiss Federam Institute of Tecnology em Zurique. O seu modo de funcionamento é semelhante às restantes aplicações.

2.2.8 Radar COVID

Esta é a aplicação oficial em Espanha.

Esta aplicação [13, 14] foi desenvolvida pela Secretaria de Estado de Digitalização e Inteligência Artificial de Espanha. O modo de funcionamento é semelhante ao explicado, sendo que os dados ficam também armazenados durante os 14 dias.

Em Portugal, esta aplicação também está disponível mas apenas para iOS.

Figura 2.6: Logótipo da aplicação Radar COVID

2.2.9 Stop COVID19 CAT

Esta aplicação [15, 16] é usada pelos habitantes da Catalunha.

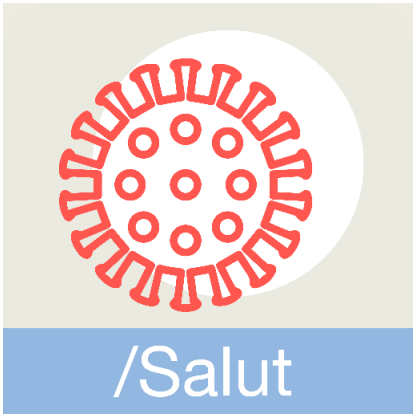


Figura 2.7: Logótipo da aplicação Stop COVID19 Cat

Esta aplicação fornece aos utilizadores um diagnóstico precoce, informando o Sistema de Emergências Médicas da situação de cada pessoa. A autenticação é feita através de um Código Pessoal de Intervenção do cartão de saúde, ligando os dados desse cartão com os dados aplicação, de uma maneira totalmente segura. Esta aplicação recomenda também o isolamento profilático a utilizadores com contactos de risco.

2.3 Tecnologias com Potencial a Serem Usadas

2.3.1 Bluetooth Low Energy

Bluetooth Low Energy (BLE) [17–19] é a tecnologia usada em todas as aplicações acima mencionadas. Esta tecnologia, que é também conhecida como Bluetooth Smart, é uma rede sem fios muito usada em aplicações para a saúde, para o bem-estar e para a segurança. O BLE está disponível para os sistemas operativos macOS, Linux, Windows 8 e Windows 10 e para os sistemas operativos móveis iOS, Android, Windows Phone e BlackBerry.

Figura 2.8: Bluetooth Low Energy

O BLE tem quatro modos de funcionamento.

O primeiro modo é o modo **difusor**. Este modo é usado como um servidor e tem como principal objetivo a transmissão regular de dados para outros dispositivos, não recebendo qualquer tipo de dados.

Contrariamente ao modo difusor, existe o modo **observador**. Neste modo, o dispositivo apenas recebe dados enviados pelo difusor, não estando por isso habilitado para enviar qualquer tipo de informação.

O terceiro modo é o modo **central**. Um dispositivo neste modo providencia dois tipos de conexão: modo conectado e modo de propaganda.

Diretamente relacionado com o modo central, temos o modo **periférico**. Este modo permite conexões e constantes trocas de informação com dispositivos em modo central.

Na fig. 2.9 encontra-se uma ilustração dos modos de funcionamento que existem no Bluetooth Low Energy.

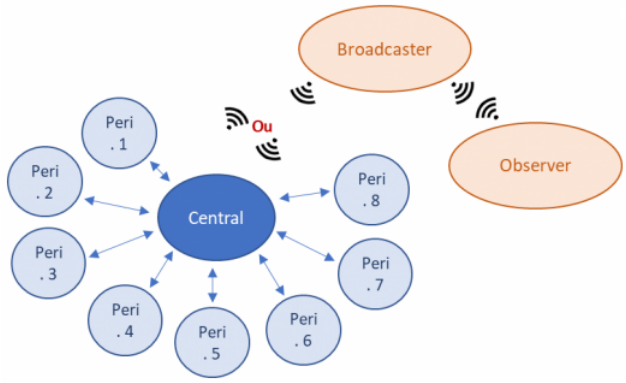


Figura 2.9: Modos de Funcionamento do Bluetooth Low Energy

De seguida, compara-se o BLE com o clássico Bluetooth (Bluetooth denomina-se de Bluetooth Basic Rate/Enhanced Data Race). O Bluetooth é usado para a transferência e troca de grandes quantidades de dados. Visto que são trocadas grandes quantidades de informação, irá consumir mais energia.

Por outro lado, o BLE é ideal para aplicações que não requerem a transferência de grandes quantidades de dados e que, por isso, recolhem pouca informação para um mesmo alcance de comunicação.

Com o uso de BLE, a bateria de um dispositivo pode durar vários dias.

A nível de hardware, o BLE usa as mesmas frequências de rádio (2.4 GHz) que o clássico Bluetooth, permitindo aos dispositivos terem apenas uma antena de rádio. Quando se usa BLE, o processo de modulação torna-se mais simples.

O BLE não é compatível com o clássico Bluetooth.

Quando um dispositivo se apresenta como tendo Bluetooth 4.0, significa que esse dispositivo pode comunicar usando os sistemas de Bluetooth Basico Rate/Enhanced Data Rate ou Bluetooth Low Energy.

2.3.2 Google-Apple Exposure Notifications

A Google-Apple Exposure Notification (GAEN) [20, 21] nasceu no contexto da pandemia de COVID-19. Com o aumento de aplicações para tentar travar o avanço da pandemia, várias questões foram levantadas a essas aplicações, nomeadamente a questão da privacidade e da segurança. Para tentar contornar essas questões, a Google e a Apple uniram-se de modo a desenvolver um sistema que respeitasse a privacidade do utilizador.

A solução encontrada foi um sistema descentralizado, tendo por base Bluetooth Low Energy. Este sistema implementa também um protocolo criptográfico que preserva a privacidade. Este sistema criado é similar ao protocolo Decentralized Privacy-Preserving Proximity Tracing (DP-3T) mas é implementado ao nível do sistema operativo, permitindo uma eficiência maior nas operações.

Geralmente, os protocolos de rastrear têm dois objetivos principais: registo de encontro e relatório de infeção. As notificações de exposição apenas definem um registo de encontro com uma arquitetura descentralizada. Para esse registo de encontro, o sistema usa BLE para enviar mensagens para dispositivos que se encontrem por perto. Também para garantir a privacidade dos utilizadores, o endereço Media Access Control (MAC) do bluetooth muda a cada 10 minutos.

A nível do utilizador, há alguns pontos a saber

É o utilizador que escolhe se recebe as Notificações de Exposição, sendo possível a qualquer momento ativar ou desativar essas notificações.

Este sistema de notificações de exposição não monitoriza a localização GPS. Visto que este sistema apenas utiliza BLE, apenas é monitorizada a posição relativa entre dois dispositivos, isto é, se estão próximos ou não.

Nem a Google nem a Apple conseguem ver a identidade do utilizador. Tendo em conta que as notificações de exposição ocorrem em cada dispositivo, é impossível a Apple e a Google saberem a identificação do utilizador. No entanto, é possível que as autoridades de saúde solicitem o número de telemóvel para poderem comunicar com o utilizador, sendo essa informação fornecida apenas com a devida autorização.

Este sistema (GAEN) apenas é utilizado pelas autoridades de saúde pública.

2.3.3 HMAC-SHA256

Um Hash Message Authentication Code (HMAC) [22] é um código de autenticação com base numa hash. Este código envolve uma função hash criptográfica e uma chave secreta e é usado para verificar a integridade e a autenticidade de uma mensagem. Este código é usado na aplicação na parte da geração de RPI.

Qualquer função hash criptográfica pode ser usada no cálculo do HMAC. Neste caso, a função hash utilizada é a SHA-256.

Esta tecnologia é utilizada na aplicação, quando há necessidade de gerar chaves TEK.

2.3.4 Norma de Criptografia Avançada

A Norma de Criptografia Avançada (AES) [23] é uma metodologia para a encriptação de dados. Foi desenvolvida no Instituto Nacional de Padrões e Tecnologia dos Estados Unidos e é usado por todo o mundo. Este algoritmo é também o único algoritmo acessível à população que é aprovado pela Agência de Segurança Nacional dos Estados Unidos.

Este algoritmo é de chave simétrica, ou seja, a mesma chave é usada para encriptar e desencriptar dados.

Na aplicação, este processo de encriptação é usado na parte da geração de RPI.

2.3.5 Global Positioning System (GPS)

O Global Positioning System [24–27] é um sistema de navegação que usa satélites para fornecer ao utilizador a sua posição, bem como a informação temporal. É possível usar o GPS sob quaisquer condições atmosféricas, a qualquer momento e em qualquer lugar do planeta Terra.

Para que o recetor possa fornecer todos os dados acima mencionados, é necessário estar ao alcance de quatro satélites.

Hoje em dia, qualquer dispositivo móvel possui um recetor GPS. Eles estão integrados, por exemplo, nos telemóveis e nos automóveis. O sistema GPS dá também informação sobre a velocidade e a direção do deslocamento do recetor.

Esta tecnologia será bastante importante na realização deste projeto. Com o sistema GPS, pretende-se complementar o uso do BLE, na medida em que se tende prever zonas no mapa em que o risco de contágio seja mais alto que o normal, devido à aglomeração da população.

A fig. 2.10 retrata o modo de funcionamento do GPS, nomeadamente na parte da trilateração dos quatro satélites.

Para o bom funcionamento do sistema GPS, são necessários quatro satélites. Cada satélite possui um relógio interno. Os relógios dos satélites não estão síncronos entre si nem estão síncronos com o

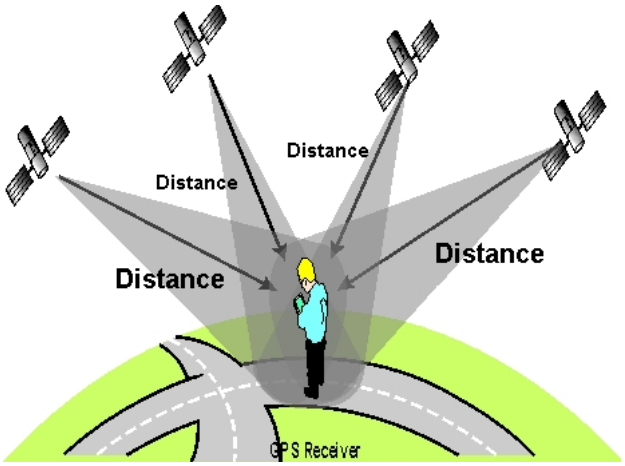


Figura 2.10: Modo de Funcionamento do GPS

relógio do recetor GPS.

O recetor GPS comunica com cada um desses satélites. O sinal que o satélite envia ao recetor inclui a hora a que o sinal foi enviado. Ao receber o sinal, o recetor compara as horas de envio e receção do sinal e, sabendo a velocidade a que um sinal rádio viaja, é calculado a distância a que o recetor se encontra do satélite. Contudo, os relógios do satélite e do recetor não estão síncronos. O cálculo feito para a distância apresenta um erro. Portanto, para cada sinal enviado por um satélite temos quatro incógnitas: a latitude, a longitude, a altitude e o erro de sincronismo. Ao utilizar quatro satélites, é possível determinar o erro e, assim, calcular a posição real do recetor.

Para além do sistema GPS, existem também outros sistemas de localização.

O GLONASS [28] é o sistema russo de localização. Foi desenvolvido durante os anos 70 apenas para uso militar. Mais tarde, durante os anos 80, é que se começou a usar esta tecnologia em aplicações comerciais, usando como recurso os 24 satélites que foram distribuídos em três orbitais terrestres.

Na China também foi desenvolvido um sistema de localização, o BeiDou [29].

A União Europeia está a desenvolver o sistema Galileo [30]. Este sistema opera com 14 satélites e tenciona melhorar a sua precisão em regiões com maiores latitudes. Para 2020, o principal objetivo era ter um total de 24 satélites distribuídos em 6 orbitas terrestres.

2.3.6 Wireless Fidelity (Wi-Fi)

O Wi-Fi é uma rede sem fios à qual cada dispositivo pode aceder. Esta rede permite uma comunicação entre cada computador e permite também o acesso à internet.

Para se ter acesso à internet, o dispositivo tem que estar no raio de abrangência de um ponto de acesso. O ponto de acesso transmite um sinal sem fios que abrange um raio de 100 a 300 metros.

O ponto de acesso tem vários parâmetros, nomeadamente o nome da rede e a palavra-passe de

Figura 2.11: Wi-Fi

acesso. O nome da rede denomina-se Service Set Identifier (SSID).

O SSID tem dois modos de utilização: visível e oculto.

No primeiro caso, significa que a rede está acessível a todos os aparelhos eletrónicos sem que o utilizador tenha que fazer a procura da rede manualmente. Isto é, quando um dispositivo procura uma rede disponível para se ligar, esta aparecerá automaticamente. Este modo é o modo padrão de todos os pontos de acesso.

No modo oculto, os pontos de acesso trabalham de maneira diferente. Neste caso, quando um dispositivo se tenta conectar à rede, esta não aparece na lista de redes disponíveis. Está, portanto, oculta. Para o dispositivo se conectar, o utilizador terá que saber o nome exato do ponto de acesso. Este modo apresentar algumas vantagens e desvantagens comparativamente ao modo visível. Uma das vantagens é a segurança. Este modo aumenta significativamente a segurança da rede visto que qualquer invasor terá que conhecer previamente o SSID da rede para a poder atacar. A principal desvantagem é o facto de a conexão à rede ser menos intuitiva. O utilizador tem que conhecer o nome exato que o administrador da rede deu ao SSID para se poder conectar.

O SSID de uma rede pode ser mudado. Normalmente, os pontos de acesso vêm com um nome padrão escolhido pela operadora de rede móvel que fornece o acesso à internet. Contudo, o administrador da rede pode facilmente alterar o SSID bastando, para isso, aceder ao endereço IP do ponto de acesso num browser.

Este parâmetro será bastante importante no contexto deste projeto. Com o SSID, pretende-se fazer um estudo acerca das pessoas que estão no alcance de determinados pontos de acesso. Se um utilizador ficar infetado, é possível, com esta informação, verificar que outros utilizadores estiveram conectados a essa mesma rede e identificá-las como utilizadores com risco de estarem infetados.

2.3.7 Protocolos de Comunicação

Hoje em dia, para haver transferência de dados entre duas ou mais entidades, é necessário que haja comunicação entre essas entidades. Os protocolos de comunicação existem para que haja um entendimento entre todas as entidades, isto é, que funcionem com um conjunto de regras-padrão pré-

definidas. Portanto, para que haja comunicação, é necessário existir um emissor, um recetor, um canal, uma mensagem e um protocolo de comunicação. Neste sub-capítulo abordam-se dois protocolos de comunicação bastante comuns: Transmission Control Protocol (TCP) e User Datagram Protocol (UDP) [31, 32].

O diagrama da fig. 2.12 retrata como é feita a transferência de dados usando os dois protocolos de comunicação.

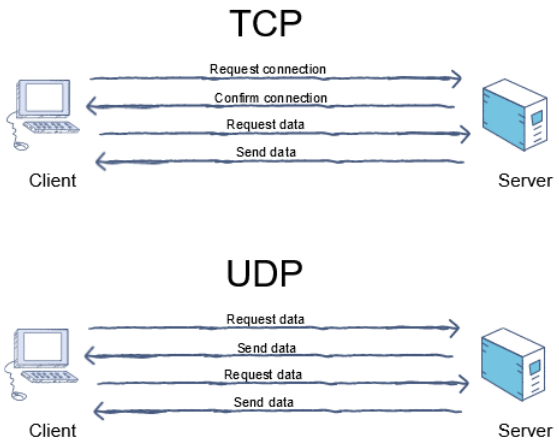


Figura 2.12: Transferência de Dados em TCP e UDP

O protocolo de comunicação TCP é um protocolo orientado à conexão, isto é, é necessário estabelecer primeiro uma conexão entre o emissor e o recetor para que os dados possam ser transferidos. Uma vez estabelecida a conexão, é possível trocar dados nas duas direções.

Este protocolo tem a particularidade de ter mecanismos com a capacidade de retransmitir as mensagens que não forem confirmadas pelo receptor e para garantir que os dados são entregues na ordem em que foram enviados. No diagrama da fig. 2.12 é possível observar que um pacote só é enviado se o pacote anterior chegar ao recetor. Sendo este um protocolo que garante a entrega de dados ao recetor, é perfeito para transferências de informações, tais como, imagens e ficheiros de dados.

Apesar de ser um protocolo bastante confiável para a transferência de dados, os seus mecanismos de correção de erros resultam numa sobrecarga maior, que se traduz num maior uso de largura de banda da rede.

O protocolo de comunicação UDP é um protocolo que, contrariamente ao TCP, não necessita de estabelecer uma conexão para poder transferir dados. Não sendo necessário estabelecer nenhuma conexão, não cria nenhuma sobrecarga para abrir, manter ou terminar a conexão.

Tendo em conta que não há qualquer conexão estabelecida, não é possível haver mecanismos especiais de correção de erros, pelo que, se algum pacote se perder ou ficar corrompido, não será

retransmitido pelo emissor. Na parte do emissor existe uma emissão contínua dos pacotes, visto que o emissor não espera por nenhuma confirmação acerca da chegada do pacote ao recetor. No diagrama da fig. 2.12 é possível verificar que a mensagem 3 é enviada e perdida. Contudo, como o emissor não tem qualquer feedback acerca da receção da mensagem, enviando a mensagem seguinte.

Outra grande diferença entre estes dois protocolos de comunicação é a velocidade.

No TCP existe um mecanismo que é o arranque-lento. Este mecanismo é um algoritmo que regulando a quantidade de dados que são enviados através da ligação. Começa por haver uma negociação entre o remetente e o destinatário da conexão, definindo a quantidade de dados que podem ser transmitidos em cada pacote. Essa quantidade de dados é aumentada gradualmente até se atingir a capacidade máxima da conexão. O arranque-lento permite a transmissão do máximo de dados possível sem haver qualquer congestionamento na rede.

A tabela 2.1 resume todas as diferenças entre os protocolos de comunicação TCP e UDP.

Tabela 2.1: Diferenças entre TCP e UDP

	TCP	**UDP**
Conexão	Necessita de conexão prévia	Não necessita de conexão
Sequência de Dados	Garante entrega de dados em sequência	Não garante entrega de dados sequência
Entrega de Dados	Garante a entrega ao recetor	Não garante a entrega ao recetor
Retransmissão de Dados	Retransmite quando há perdas de dados	Não retransmite
Broadcast	Não permite o broadcast de dados	Permite o broadcast

Os protocolos de comunicação serão usados no sistemas a desenvolver quando surgir a necessidade de haver comunicação entre servidor e aplicação.

2.3.8 REST-API

A Representational State Transfer-Application Programming Interface trata-se de uma unificação de duas tecnologias que visa a simplificar a troca de informações entre servidores e clientes. A fig. 2.13

demonstra a integração desta tecnologia numa relação cliente-servidor.

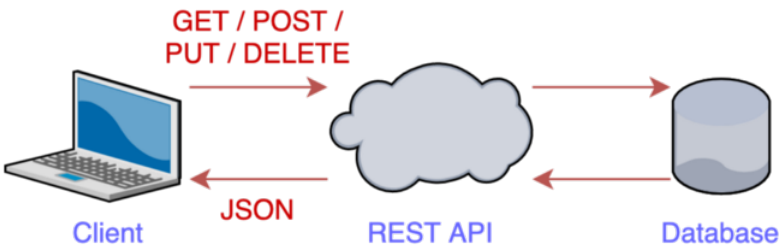


Figura 2.13: Diagrama de Funcionamento da REST-API

Uma Application Programming Interface (API) é um conjunto de definições e protocolos usados no desenvolvimento e na integração de aplicações. As API são um mediador entre um provedor de informações e um cliente que deseja obter alguma informação. Servem também para que as organizações partilhem os seus recursos, mantendo a segurança, o controlo e a obrigatoriedade de autenticação de quem acede.

O Representational State Transfer (REST) é um conjunto de restrições de arquitetura. É uma arquitetura implementada paralelamente a uma API. Esta tecnologia foi criada pelo cientista de computação Roy Fielding.

Unindo estas duas tecnologias, resulta uma REST-API, que não é mais do que uma interface de programação de aplicações (API) que está em conformidade com as restrições do estilo de arquitetura REST. Quando um cliente faz uma solicitação usando uma REST-API, a API envia uma representação do estado do recurso ao endpoint. A informação enviada, que é entregue via Hypertext Transfer Protocol (HTTP), pode ter vários formatos: Hypertext Markup Language (HTML), Python ou Javascript Object Notation (JSON). O formato JSON é o formato mais usado devido à facilidade de ser lido tanto por máquinas como por humanos.

Existem ainda alguns critérios que devem ser respeitados para que uma API seja considerada do tipo REST. É necessário existir uma arquitetura cliente/servidor, formada por clientes, servidores e recursos, com solicitações intermediadas por HTTP. A comunicação entre o cliente e servidor tem que ser stateless, significando que nenhuma informação do cliente é armazenada nas solicitações GET e que todas as solicitações são separadas e desconectadas. Nesta arquitetura é necessário também haver armazenamento de dados em cache para otimizar as interações entre cliente e servidor. É importante também existir uma interface uniforme entre componentes para que as informações sejam transferidas num formato padronizado.

Paralelamente à Representational State Transfer, existem outras arquiteturas de estilo semelhante. A Simple Object Access Protocol (SOAP) é uma dessas arquiteturas sendo mais complexa de usar do que a REST. A SOAP tem requisitos mais específicos, tais como o uso de XML, e tem de cumprir com exigências de segurança incorporada e transações, tornando esta tecnologia mais lenta e pesada.

Uma das vantagens da arquitetura REST é o facto de ser composta por um conjunto de diretrizes que apenas são implementadas conforme necessário. Esta particularidade torna a arquitetura REST mais rápidas, leves e escaláveis, sendo uma arquitetura ideal a implementar no desenvolvimento de aplicações móveis.

Esta arquitetura de REST-API é usado no sistema, nomeadamente na interligação existente entre o servidor e o cliente web.

3

Arquitetura do Sistema

Conteúdo

Findo o processo de pesquisa de informação e de tecnologias relevantes para o desenvolvimento deste sistema (detalhado no capítulo 2), segue-se o processo de desenvolvimento desse mesmo sistema. É sobre o desenvolvimento do sistema que este capítulo se debruçará.

Como foi explicado anteriormente, o objetivo desta dissertação é o desenvolvimento de uma aplicação que monitorize uma população de indivíduos potencialmente contagiados por doenças infecto-contagiosas. Para tal, é necessário desenvolver uma aplicação que seja facilmente descarregada para dispositivos móveis, que seja de fácil utilização para os utilizadores e que não interfira com o uso normal dos dispositivos móveis. Contudo, apenas com o desenvolvimento da aplicação para dispositivos móveis, não seria possível fazer o processamento de todos os dados, bem como o registo de novas infeções. Para isso, foi necessário criar um servidor que reúna todas essas funcionalidades. No servidor são guardados todos os registos de utilizadores, assim como registos de GPS e Wi-Fi obtidos através das aplicações. Para uma melhor visualização dos dados, criou-se um site onde é possível ver, em tempo real, todos os registos guardados no servidor.

A fig. 3.1 retrata a arquitetura deste sistema. Como é possível observar, todos os dispositivos móveis apenas comunicam com o servidor, quer para enviar dados como para solicitar. No outro lado, existe o website que, tal como os dispositivos móveis, apenas comunica com o servidor. O servidor funciona como um bypass de informação entre os diversos componentes do sistema.

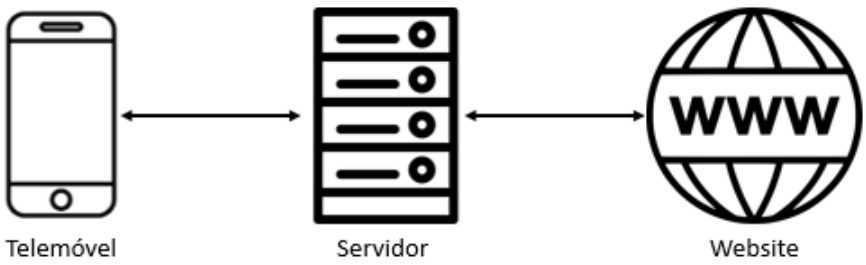


Figura 3.1: Arquitetura do Sistema

No restante capítulo, começa-se por explicar o modo de funcionamento da aplicação para dispositivos móveis. De seguida, estuda-se o servidor e o modo de como os dados recolhidos pela aplicação são recebidos e tratados. Por fim, é demonstrado de que forma os dados são mostrados no site, bem como o método usado para a transmissão de dados do servidor para o site.

3.1 Aplicação Móvel

A aplicação para os dispositivos móveis foi desenvolvida com recurso ao Android Studio e à linguagem de programação Java.

Esta aplicação tem como objetivo principal fazer uma recolha de informação através do uso de GPS e de Wi-Fi. Periodicamente, é feita uma análise às informações fornecidas pelo GPS, nomeadamente a latitude, a longitude e a altitude. Relativamente às informações fornecidas pelo Wi-Fi, são extraídas todos os SSID das redes disponíveis às quais os dispositivos se conseguem ligar.

3.1.1 Página de Login

Quando se inicia a aplicação, é pedido ao utilizador que faça o login na aplicação. O login é composto por um nome de utilizador e por uma palavra-passe.

O login nesta aplicação existe para criar uma noção de confidencialidade nas informações dos utilizadores. Cada utilizador apenas pode entrar na sua sessão.

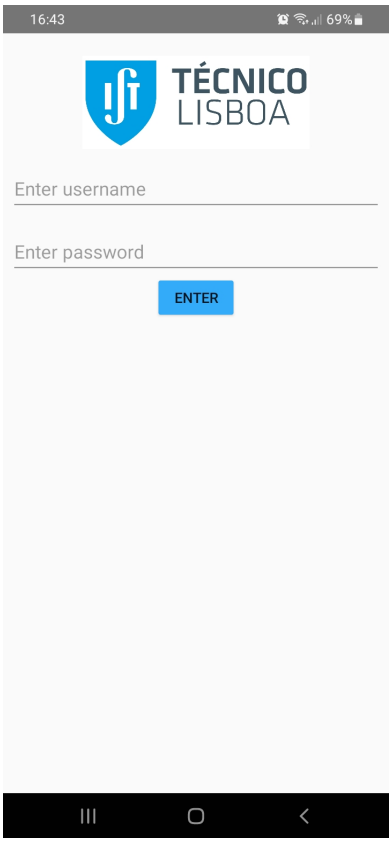


Figura 3.2: Página de Login da Aplicação

Na fig. 3.2 encontra-se uma captura de ecrã da aplicação em funcionamento na Página de Login.

Para fazer o login, o utilizador tem que preencher os espaços com o seu nome de utilizador e com a palavra-passe. Posteriormente, ao pressionar o botão Enter, a aplicação gera uma mensagem onde está contido o nome de utilizador e a palavra-passe. Com essa mensagem, é criado um pacote de dados UDP que é transmitido para o servidor. Após a transmissão da mensagem, espera-se uma outra mensagem vinda do servidor. Essa mensagem será fundamental para que o login seja concluído com sucesso. Dependendo da mensagem recebida pode ocorrer uma de duas situações. Se o nome de utilizador inserido coincidir com um nome de utilizador já existente na base de dados do servidor e a palavra-passe não corresponder, a aplicação continua na mesma página. Quando a palavra-passe corresponde com o nome de utilizador inserido, a aplicação automaticamente passa para a página seguinte, a página de recolha de dados.

Existe ainda a possibilidade de o nome de utilizador inserido não coincidir com nenhum dos nomes de utilizadores armazenados na base de dados do servidor. Nessa situação, é criado um novo utilizador cuja palavra-passe é a que está inserida na caixa de texto e a aplicação prossegue para a página seguinte.

Por uma questão de bom funcionamento de aplicação, o botão Enter apenas funciona se ambas as caixas de texto, a do nome de utilizador e a da palavra-passe, não estiverem vazias.

3.1.2 Página de Recolha de Dados

Após o login ser bem sucedido, isto é, após iniciar sessão ou após criação de novo utilizador, a aplicação automaticamente mostra uma nova página, a Página de Recolha de Dados. Na mudança de página são enviados o nome de utilizador e a palavra-passe do utilizador.

Esta página tem uma extrema importância para este projeto pois, é aqui que se faz toda a recolha de dados de GPS e de Wi-Fi.

A fig. 3.3 retrata uma captura de ecrã da Página de Recolha de Dados.

Como é possível observar pela fig. 3.3, esta página tem dois botões, em que cada um deles tem uma função diferente.

O primeiro botão é o botão usado para obter informação acerca do GPS. Quando o utilizador carrega nesse botão, a aplicação começa o processo de obtenção de coordenadas GPS. Em cada conjunto de coordenadas, extrai-se a latitude, a longitude e a altitude. Quando esta ação é bem conseguida, é colocado numa caixa de texto no ecrã todas as informações recolhidas, como se observa no exemplo da fig. 3.3. Se ocorrer algum erro na obtenção das coordenadas, coloca-se uma mensagem de erro nessa caixa de texto.

No outro botão trabalha-se com o Wi-Fi. Ao pressionar o botão, a aplicação inicia uma análise das redes disponíveis para o qual o dispositivo móvel se pode conectar. Após feito esse scan das redes disponíveis, é colocado na caixa de texto abaixo do botão o SSID de cada uma dessas redes.

Figura 3.3: Página de Recolha de Dados

Após desenvolvidas as funções de obtenção de coordenadas e de obtenção de redes Wi-Fi disponíveis através de toques em botões, segue-se o desenvolvimento para que estas funções se realizem automaticamente e periodicamente sem necessidade de carregar nos botões.

Para que a execução das duas funções ocorram periodicamente, desenvolveu-se um temporizador de funções. O temporizador de funções é caracterizado por ter uma função que tem que executar e um tempo de intervalo entre cada execução. A função do temporizador começa por extrair a data e a hora real de cada execução, que são necessárias mais tarde, e, de seguida, executa as funções de obtenção de coordenadas e de redes Wi-Fi disponíveis. Este temporizador inicia logo após a Página de Recolha de Dados iniciar e é executado a cada 15 segundos. Com a introdução do funcionamento do temporizador, os botões continuam em pleno funcionamento.

3.1.3 Interligação com o Servidor

Com todos os dados recolhidos na aplicação, é necessário enviar esses dados para o servidor. Durante o funcionamento normal da aplicação, existem dois momentos onde a aplicação comunica com o servidor: quando é necessário validar o login do utilizador e quando é necessário transmitir dados de

GPS e Wi-Fi.

Em todas as comunicações, é usado o protocolo de comunicação User Datagram Protocol (UDP). Quando o utilizador tenta iniciar sessão na Página de Login, é criado um pacote de transmissão de dados de UDP. Esse pacote apenas contém o nome de utilizador e a palavra-passe que foram inseridos nas caixas de texto. Esse pacote é enviado para o servidor. Após enviado o pacote, a aplicação fica a aguardar outro pacote. Esse novo pacote é um pacote de resposta do servidor ao primeiro pacote enviado. O pacote de resposta é um pacote UDP simples contendo apenas uma palavra. A palavra de resposta informa a aplicação se o login foi feito com sucesso ou se o utilizador o tem que repetir.

Para a transmissão dos dados relativos às coordenadas GPS e dos SSID das redes Wi-Fi disponíveis, também é usado o protocolo UDP. Quando a Página de Recolha de Dados é iniciada, é criada uma socket que funciona paralelamente à aplicação. Essa socket é uma socket que funciona como um cliente UDP. Cada vez que são obtidas coordenada GPS com sucesso, é criada uma mensagem de texto que contém o nome de utilizador, a data e hora de obtenção das coordenadas, a latitude, a longitude e a altitude. O mesmo acontece quando é feito um scan das redes Wi-Fi disponíveis. Por cada rede disponível, uma mensagem é criada contendo o nome de utilizador, a data e hora e o SSID da rede correspondente. Assim que uma dessas mensagens de texto é criada, são enviadas para a socket UDP. Na socket, a mensagem de texto é transformada num pacote de dados UDP e enviado para o servidor. Contrariamente ao que acontece no processo de validação do login, após a transmissão destes pacotes, a aplicação não fica a aguardar resposta do servidor.

Decide-se transmitir os dados referentes ao GPS e Wi-Fi por UDP devido à sua rapidez de transmissão de dados. O facto de não haver qualquer correção de erro nem retransmissão de pacotes perdidos poderia revelar-se uma desvantagem ao uso de UDP. Mas, visto que a cada 15 segundos são recolhidos dados GPS e Wi-Fi, no caso de haver alguma perda de dados, essa perda será insignificante comparativamente aos restantes dados transmitidos.

3.1.4 Autorizações Necessárias

Para que a aplicação funcione corretamente, é necessário que o utilizador permita que a aplicação use algumas tecnologias do dispositivo móvel.

A primeira permissão necessária é o uso de internet. A aplicação necessita logo no início de internet para que se consiga fazer o início de sessão. Para tal, verifica-se primeiro o estado da internet, isto é, se está ligada ou não e, em caso de não estar, é necessário ligá-la. Neste ponto a internet pode provir de dados móveis ou de Wi-Fi.

De seguida, é necessário obter coordenadas GPS. Para ser possível obtê-las, verifica-se o estado da ligação do geolocalizador e, caso necessário, ativa-se. O utilizador tem que autorizar a utilização do geolocalizador para que a aplicação funcione.

Para a recolha de redes Wi-Fi disponíveis, é necessário que o utilizador autorize o uso do Wi-Fi. Caso autorize, a aplicação verifica o estado do Wi-Fi e, caso se encontre desativado, ativa-o.

3.2 Servidor

O servidor é a peça essencial deste sistema. O servidor tem que ser capaz de receber grandes quantidades de dados provindos das aplicações dos dispositivos móveis. Após recebidos esses dados, tem que armazená-los de forma que sejam facilmente acedidos. Para além da receção e armazenamento de dados, o servidor necessita também de fazer processamento dos dados guardados. Esse processamento será necessário para responder a pedidos provindos do site.

Devido a esta complexidade do servidor, decidiu-se dividi-lo em vários componentes, conforme consta no diagrama da fig. 3.4. Inicialmente, criaram-se servidores UDP para receber informações provindas das aplicações. A fim de armazenar, de forma eficiente, todos os dados recolhidos provindos das aplicações, foram criadas três bases de dados. Por fim, criou-se uma proxy para responder a todos os pedidos provindos do site. A proxy é responsável pelo acesso às bases de dados, tendo em conta os dados solicitados pelo site. Todo o servidor foi desenvolvido usando a linguagem de programação Python.

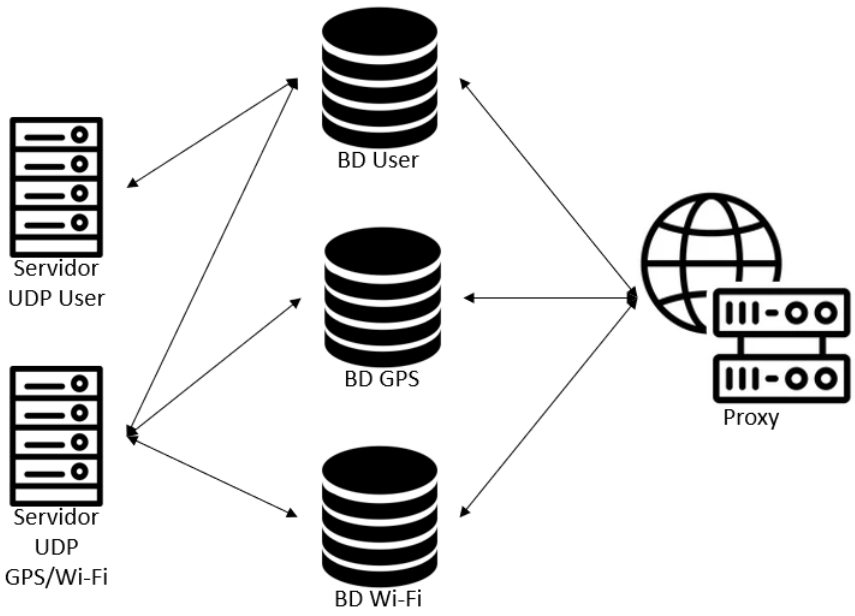


Figura 3.4: Organização Interna do Servidor

3.2.1 Bases de Dados

Como referido anteriormente, as bases de dados são essenciais neste sistema. Todas as bases de dados foram criadas usando como recurso a linguagem de programação Structured Query Language (SQL).

Base de Dados de Utilizadores

Inicialmente começa-se por organizar todas as informações relativas aos utilizadores numa base de dados. Para tal, existem três tabelas para dividir os diferentes tipos de dados.

A primeira tabela de dados criada é a tabela *User*. Esta tabela é responsável por armazenar todas as informações dos utilizadores. Neste momento de desenvolvimento deste sistema, apenas são armazenados dois atributos de cada utilizador, que são os parâmetros de início de sessão: nome de utilizador e palavra-passe. Tem ainda outro parâmetro que é o seu identificador. Esse identificador é um número que, a cada inserção na tabela, vai incrementando, sendo único para cada utilizador. Associados a esta tabela, existem algumas funções com a capacidade de aceder e modificar dados:

newUser: Esta função é a responsável por cada inserção na tabela de *User*. Recebe como parâmetros um conjunto de nome de utilizador e palavra-passe e, em caso de sucesso de inserção, retorna o identificador.

checkUserExist: Quando um utilizador faz login na aplicação, é necessário verificar se esse nome de utilizador já existe na base de dados. Esta função é invocada nessa situação, que recebe o nome de utilizador e retorna o número de entradas existentes na tabela com esse nome de utilizador.

checkUserPassword: Na mesma situação de login, quando é verificado que existe o nome de utilizador, é necessário verificar se a palavra-passe coincide com a guardada. Para essa verificação, esta função recebe o conjunto de nome de utilizador e palavra-passe inseridas na aplicação e verifica se esse conjunto existe na base de dados.

getIdUser: Quando existem dados a serem transmitidos da aplicação para os servidor, os dados vêm acompanhados do nome de utilizador. Contudo, o parâmetro do utilizador que é guardado junto dos outros dados é o identificador sequencial. Esta função retorna esse identificador.

allUsersDICT: Esta função retorna todas as entradas tabela *User*. Para cada entrada da tabela, as informações são transformadas num dicionário, para serem facilmente acedidas. É retornado uma lista contendo todos os dicionários de cada entrada da tabela.

De seguida, criou-se uma nova tabela para armazenar todos os utilizadores que testaram positivo. Decidiu-se colocar numa tabela separada da anterior pois cada utilizador pode testar positivo à doença mais do que uma vez, em períodos de tempo distintos. Cada linha da tabela *UserInfected* corresponde a um período de infeção de um utilizador. Portanto, nesta tabela armazena-se o identificador do utilizador, a data de início e a data de término da infeção e o identificador sequencial. Afetos a esta tabela, existem

algumas funções:

newUserInfected: Sempre que se registe uma nova infeção, esta é a função responsável por adicionar mais um registo à tabela *UserInfected*. Quando inserido com sucesso, a função retorna o identificador sequencial.

allUsersInfectedDICT: Esta função acede a todas as entradas da tabela *UserInfected*, transformando cada uma delas num dicionário e retornando todos os dicionários numa lista.

A última tabela desta base de dados é a tabela *UserPossibleInfected*. Sabe-se que um utilizador, mesmo não estando positivo à doença, pode possivelmente estar infetado devido a possível contactos de risco com utilizadores infetados. Esta tabela guarda um registo de utilizadores que podem ter contraído a doença sem ainda estarem diagnosticados. Cada linha da tabela armazena, para além do identificador sequencial, o identificador do utilizador, a data em que houve contacto de risco e o número de vezes que o utilizador se cruzou com alguém infetado nesse dia. O número de contactos de risco é dividido tento em conta se o contacto de risco foi através de GPS ou Wi-Fi. As funções inerentes a esta tabela são:

newUserPossibleInfected: Esta função, através da data e do identificador do utilizador fornecido, cria uma entrada na tabela *newUserPossibleInfected*, retornando o identificador sequencial.

allUsersPossibleInfectedDICT: Esta função reúne todas as entradas da tabela, devolvendo-as numa lista.

updateOc: Quando é necessário atualizar o número de contactos de risco para um determinado utilizador, é chamada esta função. Esta função recebe o identificador do utilizador, a data do contacto de risco e um identificador que indica se é necessário atualizar a informação correspondente ao Wi-Fi ou ao GPS.

Base de Dados de Registos de GPS

Através da aplicação, são recolhidas grandes quantidades de dados relativos a coordenadas GPS. É necessário organizá-los e armazená-los de modo a que sejam facilmente acedidos. Dessa necessidade, existe a base de dados *GPSLog*, que armazena todos os registos GPS de todos os utilizadores. Esta tabela armazena, para além do identificador único sequencial, o identificador do utilizador, a data e hora de recolha do registo, a latitude, a longitude, a altitude e um marcador de perigo, que será explicado mais adiante. Associada a esta tabela, existem várias funções:

newGPSLog: Esta função é responsável por adicionar um novo registo à tabela devolvendo o identificador sequencial.

allGPSLogsDICT: Quando é necessário obter todos os registos armazenados na tabela, esta é a função utilizada.

allGPSLogsMarkedDICT: O marcador de perigo é utilizado após confirmação da infeção. Quando um utilizador confirma positivo à doença em determinado período de tempo, todos os seus registos GPS ficam sinalizados como sendo de um utilizador doente. Este marcador assume dois valores: *zero* em caso normal e *um* em caso positivo. Quando é necessário saber todos os registos marcados a perigo, invoca-se esta função.

changeMarked: Quando o utilizador confirma positivo à doença é necessário mudar os seus registos, conforme referido anteriormente. Esta função trata dessa mudança para determinado utilizador em determinado intervalo de tempo.

userPossibleInfected: Após inserção de um novo utilizador positivo à doença, são pesquisados todos os utilizador que possivelmente estiveram em contacto com esse utilizador. Qualquer utilizador que tenha estado a menos de 50 metros de um local onde o utilizador infetado tenha estado, é marcado como um possível contacto de risco. Esta função calcula, através dos registos de coordenadas GPS, as distâncias a que os utilizadores estiveram, devolvendo uma lista de utilizadores com possíveis contactos de risco.

Base de Dados de Registos de Wi-Fi

Paralelamente à base de dados de registos GPS, existe outra base de dados para guardar os registos recolhidos através de Wi-Fi, a tabela *WiFiLog*. Os parâmetros armazenados são semelhantes: identificador único sequencial, identificador do utilizador, data e hora do registo, o SSID da rede e o marcador de perigo. As funções relativas a esta base de dados são:

newWiFiLog: Cria um novo registo na tabela *WiFiLog*, devolvendo o identificador sequencial.

allWifiLogsDICT: Devolve, na forma de lista de dicionários, todos os registos da tabela *WiFiLog*.

wifiLogsMarked: O marcador de perigo nesta base de dados funciona de forma semelhante do que na base de dados de registos GPS. Esta função devolve todos os registos da tabela *WifiLog* que tenham o marcador de perigo ativo.

wifiLogsNonMarked: Semelhante à função anterior, esta função devolve apenas todos os registos da base dados que tenham o marcador de perigo inativo.

changeMarked: Esta funcão é semelhante à que existe na base de dados de registos GPS. Sempre que alguém confirma positivo à doença em determinado intervalo de tempo, esta função é invocada para alterar o marcador de perigo.

usersPossibleInfectedWiFi: Quando um utilizador testa positivo à doença, todos os outros utilizadores que estiveram em contacto próximo com ele, estão em risco. Esta função analisa todos os SSID em que estiveram utilizadores positivos e devolve todos os outros utilizadores que estiveram conectados a esses SSID.

3.2.2 Servidores UDP

Na seção 3.2.1, estudou-se o modo de armazenamento de todos os dados necessários para o bom funcionamento deste sistema. A maioria dos dados armazenados provém das aplicações para dispositivos móveis. Na seção 3.1.3 explicou-se como eram transmitidos esses dados do ponto de vista da aplicação. No lado do servidor principal existem dois servidores UDP para receção dos dados.

Servidor UDP de Utilizadores

O servidor de utilizadores é um servidor UDP que aguarda sempre a chegada de uma mensagem. Essa mensagem, que provém da Página de Login da aplicação, contém um nome de utilizador e uma palavra-passe. Após verificar o formato da mensagem recebida, o servidor conecta-se à base de dados de utilizadores para verificar a existência do nome de utilizador, invocando a função *checkUserExists*. Caso o nome de utilizador não exista na base de dados, o servidor cria um novo utilizador, cuja palavra-passe é a que foi enviada na mensagem. Quando o nome de utilizador corresponde com um presente na base de dados, é verificada se a palavra-passe guardada corresponde com a inserida na aplicação. A função *checkUserPassword* devolve o resultado dessa pesquisa.

Por fim, o servidor envia para a aplicação uma mensagem de texto, cujo conteúdo pode variar tendo em conta o resultado das verificações de nome de utilizador e de palavra-passe.

Servidor UDP de Registos GPS e Wi-Fi

Tal como o servidor de utilizadores, este servidor está em permanente espera por uma mensagem de texto. Após receber a mensagem de texto, verifica-se o estado da mensagem e a primeira palavra dessa mensagem de texto. A primeira palavra indica se a mensagem de texto se encontra com informações GPS ou informações Wi-Fi. De seguida, acede-se à base de dados do utilizador e interroga-se o identificador sequencial do utilizador, usando como recurso a função *getIdUser*. Por fim, insere-se um novo registo na base de dados de GPS ou Wi-Fi.

Contrariamente ao servidor de utilizadores, este servidor não envia qualquer tipo de mensagens, apenas recebe.

3.2.3 Servidor HTTP

No sistema, está implementada uma proxy para que seja possível aceder, através da web, a todos os dados presentes nas bases de dados do sistema [33]. Uma proxy é uma ponte usada entre uma origem e um destino de uma requisição. É normalmente usado como uma interligação de uma rede de computadores com um servidor. A proxy serve para um controlo de acesso dos usuários da rede, isto é, os administradores da rede podem permitir ou proibir que os usuários da rede acedam ou não à internet. Para além do controlo de acesso, é também possível fazer um filtro de conteúdo, impedindo que os usuários acedam a sites específicos.

A proxy usada no sistema, é diferente da proxy comum. É denominada de proxy reversa. Neste caso, a origem das requisições dos pedidos estão na internet, que procuram informações que se encontram dentro do servidor. Este tipo de proxy tem vários benefícios, nomeadamente o balanceamento da carga e a cache. Relativamente ao balanceamento da carga, a proxy reversa permite que haja conexão com vários servidores de destino, podendo direcionar as requisições para que não haja sobrecarga de nenhum servidor. A nível da segurança, as requisições da internet apenas conhecem o endereço IP da proxy. A cache é também usada nas proxies. Os servidores de proxies reversas armazenam elementos da página armazenada nos servidores internos, havendo uma atualização periódica do conteúdo. Com a cache, os servidores da página recebem menos requisições, havendo uma menor sobrecarga.

O servidor HTTP representa a proxy, que responde aos pedidos vindos dos browsers usando REST. Esses pedidos e a forma como respondem são explicados na seção 3.3.

3.3 Site

O site foi criado com a necessidade de visualizar, em tempo real, os dados armazenados nas bases de dados. É constituído por um total de 8 páginas. As páginas enviam pedidos REST para a proxy a fim de popular as páginas com os dados requeridos.

3.3.1 Página Inicial do Site

Quando se entra no site, a página inicial que o site tem é a que se encontra na fig. 3.5.

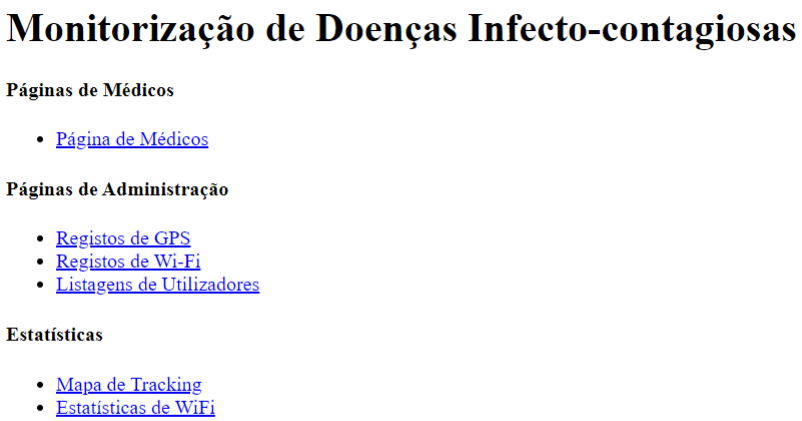


Figura 3.5: Página Inicial do Site

A partir desta página, é possível navegar por todo o restante site. Inicialmente, existe uma página

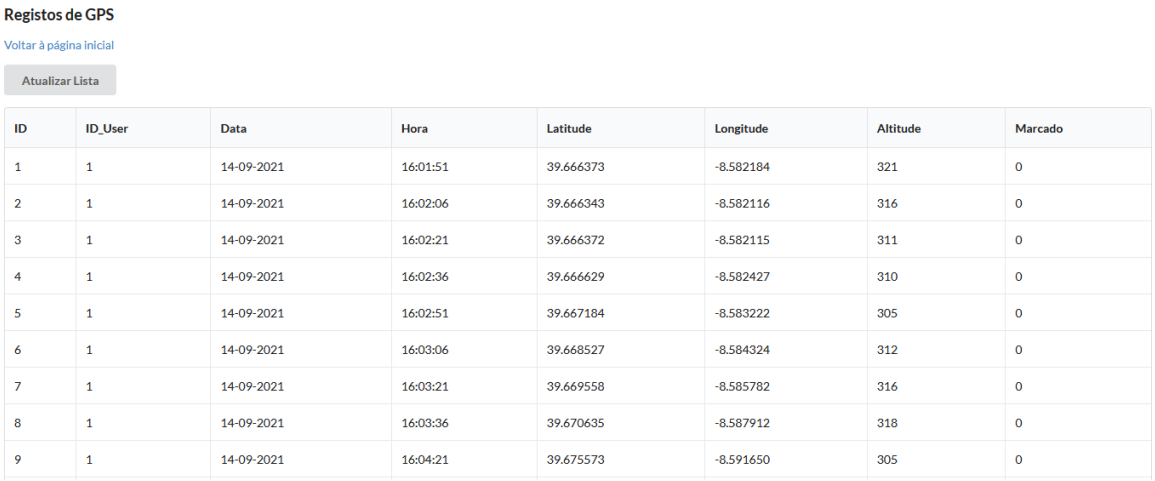
destinada aos médicos, onde os profissionais de saúde podem inserir utilizadores infetados. De seguida, as páginas de administração são uma representação, em tempo real, das bases de dados do servidor. Por último, é possível ver um mapa de onde estiveram todos os utilizadores infetados e ver algumas estatísticas de redes Wi-Fi.

3.3.2 Páginas de Administração

As Páginas de Administração servem para ver os dados das bases de dados em tempo real. Visto haver três bases de dados, existem três Páginas de Administração, cada uma contendo dados de apenas uma base de dados.

Página de Registos GPS

Na fig. 3.6 é possível ver a data e hora de cada registo, o identificador do utilizador, a latitude, a longitude, a altitude e o marcador de perigo, relativos à base de dados de registos GPS.


Registos de GPS

Voltar à página inicial

Atualizar Lista

ID	ID_User	Data	Hora	Latitude	Longitude	Altitude	Marcado
1	1	14-09-2021	16:01:51	39.666373	-8.582184	321	0
2	1	14-09-2021	16:02:06	39.666343	-8.582116	316	0
3	1	14-09-2021	16:02:21	39.666372	-8.582115	311	0
4	1	14-09-2021	16:02:36	39.666629	-8.582427	310	0
5	1	14-09-2021	16:02:51	39.667184	-8.583222	305	0
6	1	14-09-2021	16:03:06	39.668527	-8.584324	312	0
7	1	14-09-2021	16:03:21	39.669558	-8.585782	316	0
8	1	14-09-2021	16:03:36	39.670635	-8.587912	318	0
9	1	14-09-2021	16:04:21	39.675573	-8.591650	305	0

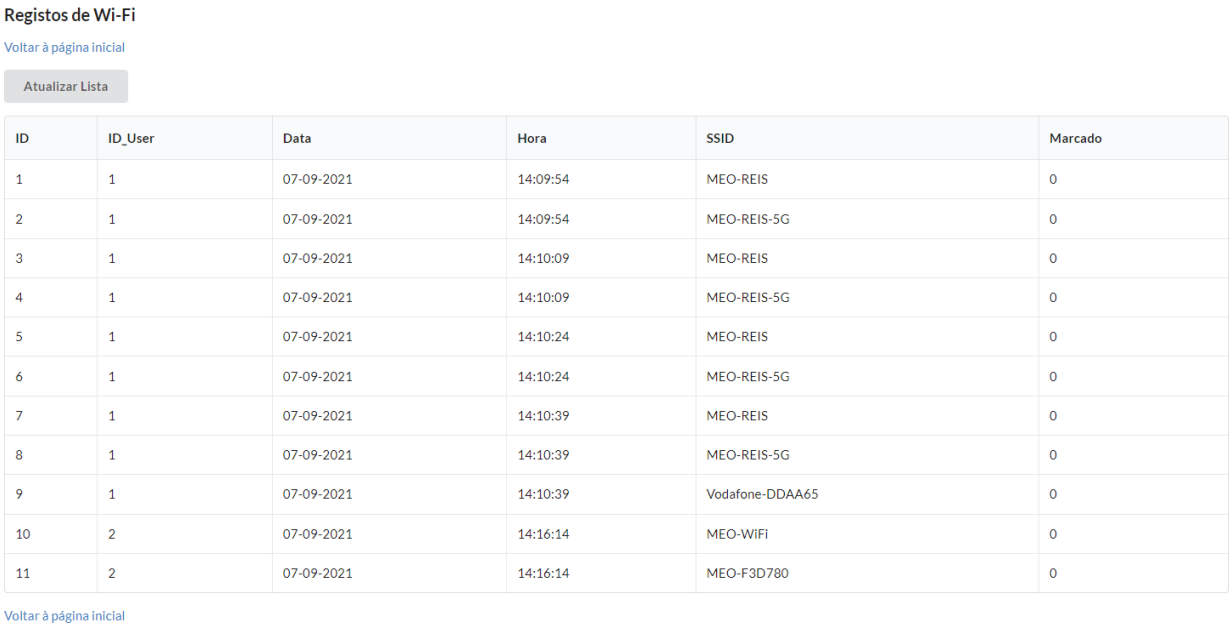
Figura 3.6: Página de Registos de GPS

Esta página, para que consiga popular a tabela, faz um pedido REST do tipo GET ao servidor. Quando a proxy recebe o pedido, contacta com a base de dados de registos de GPS para que a base de dados devolva todos os registos GPS. Os registos são devolvidos ao site no formato de uma lista de dicionários. Ao receber os dados, o site coloca-os na tabela pela ordem que está na base de dados.

A atualização da tabela é feita de forma automática quando se abre a página. No entanto, é possível atualizá-la manualmente carregando no botão *Atualizar Lista*. É também possível voltar à pagina inicial no *link* debaixo da tabela.

Página de Registos Wi-Fi

A Página de Registos Wi-Fi funciona de maneira semelhante à Página de Registos GPS. Quando a página é carregada, o site faz um pedido à proxy. Esse pedido está relacionado com os dados Wi-Fi. Após recebido o pedido REST, a proxy conecta-se à base de dados Wi-Fi para que esta devolva todos os registos da tabela *WifiLog*. Ao devolver os dados, o site trata de popular a tabela da fig. 3.7. Nessa tabela, é apresentado o identificador do utilizador, a data e hora, o SSID da rede e o marcador de perigo.



Registos de Wi-Fi

Voltar à página inicial

Atualizar Lista

ID	ID_User	Data	Hora	SSID	Marcado
1	1	07-09-2021	14:09:54	MEO-REIS	0
2	1	07-09-2021	14:09:54	MEO-REIS-5G	0
3	1	07-09-2021	14:10:09	MEO-REIS	0
4	1	07-09-2021	14:10:09	MEO-REIS-5G	0
5	1	07-09-2021	14:10:24	MEO-REIS	0
6	1	07-09-2021	14:10:24	MEO-REIS-5G	0
7	1	07-09-2021	14:10:39	MEO-REIS	0
8	1	07-09-2021	14:10:39	MEO-REIS-5G	0
9	1	07-09-2021	14:10:39	Vodafone-DDAA65	0
10	2	07-09-2021	14:16:14	MEO-WiFi	0
11	2	07-09-2021	14:16:14	MEO-F3D780	0

Voltar à página inicial

Figura 3.7: Página de Registos de Wi-Fi

A atualização da lista é feita automaticamente quando a página é carregada. Também é possível atualizá-la carregando no botão *Atualizar Lista*.

Página de Registos de Utilizadores

A fig. 3.8 representa a Página de Registos de Utilizadores. Nesta página são representadas três tabelas, correspondendo cada uma a cada tabela existente na base de dados de utilizadores.

A primeira tabela representa todos os utilizadores registados no sistema. Para cada utilizador, apenas é guardado o seu nome de utilizador e a palavra-passe. Na base de dados de utilizadores, é também guardado a lista de utilizadores infetados. Na segunda tabela, são demonstrados esses registos de infeções, revelando o identificador do utilizador, bem como o período em que esteve infetado. De notar que, nesta tabela, o mesmo utilizador pode ter mais do que um registo, desde que o período de infeção seja diferente. A última tabela diz respeito a utilizadores que não estão infetados mas que, devido a alguns contactos de risco, têm possibilidade de estarem infetados. Os contactos de risco são feitos em determinado momento e, portanto, por cada contacto de risco é guardado a data em que

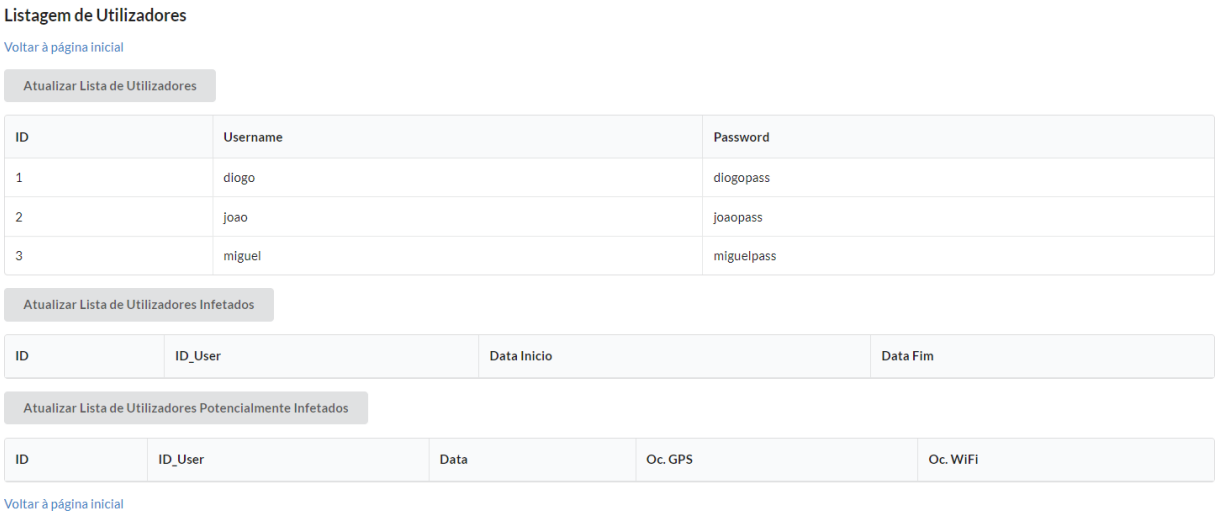


Figura 3.8: Página de Registos de Utilizadores

houve esse contacto e não um período de risco. Cada utilizador pode aparecer mais do que uma vez nesta tabela, mas só uma vez por cada dia. Na tabela é também visível o número de ocorrências de contactos de risco que o utilizador teve nesse mesmo dia, quer através de GPS, quer através de Wi-Fi.

Quando a página carrega, apenas a primeira tabela é populada automaticamente. As restantes tabelas são populadas quando se carrega no botão adequado para atualizar a lista. Os botões, quando pressionados, enviam para a proxy pedidos REST do tipo GET. A proxy, contacta com a base de dados de utilizadores a fim de obter as informações pretendidas. Dependendo do botão acionado, a proxy solicita pedidos diferentes à base de dados. Por fim, a proxy devolve os dados para o site, populando a devida tabela.

3.3.3 Página de Médicos

A Página de Médicos é a página onde os profissionais de saúde inserem no sistema a infeção de um utilizador. A fig. 3.9 mostra uma captura de ecrã da página.

Para que um médico insira um utilizador infetado, é necessário que o utilizador tenha já recuperado da infeção, ou seja, o período de infeção tem de estar terminado. É necessário saber o identificador único do utilizador para a inserção na base de dados. Para que médico saiba o identificador, está inserida uma tabela na página contendo apenas o identificador único e o nome de utilizador. Ao pressionar o botão *Mostrar Utilizadores*, que se encontra na fig. 3.9, aparece a tabela que se encontra na fig. 3.10.

De seguida, insere-se o identificador na caixa de texto, assim como a data de início e de término da infeção. Quando se submete os dados, a página apenas é responsável por verificar que o identificador inserido é um número inteiro positivo. Se não for, a página não submete qualquer pedido para a proxy.

Quando o identificador se encontra válido, o site faz um pedido REST do tipo UPDATE para a proxy,

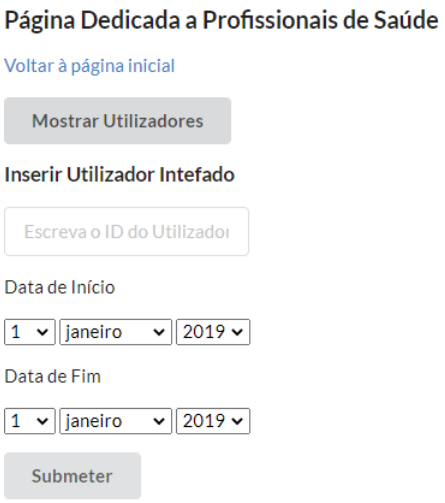


Figura 3.9: Página de Médicos

enviando como dados o identificador inserido, assim como as datas inseridas.

Ao receber o pedido, a proxy começa por contactar com as três bases de dados. Inicialmente, faz-se uma procura nas bases de dados de GPS e de Wi-Fi pelos registos do utilizador no período de infeção. Em todos esses registos, é atualizado o marcador de perigo. Após essa marcação, é criado na tabela *UserInfected* um novo registo de infeção. De seguida, é feita uma procura de utilizadores que estiveram em contacto próximo com o utilizador infetado. Em cada dia de infeção, são procurados os registos GPS do utilizador infetado e os registos dos outros utilizadores. Cada registo do utilizador infetado é comparado com os restantes registos, atráves das coordenadas GPS guardadas. É calculada, através das coordenadas, a distância entre os registos. Se a distância for menor do que 50 metros, é guardado o registo como potencialmente em risco. Cada registo marcado como potencialmente em risco, é depois processado pela base de dados de utilizadores. Por cada registo, é verificado se existe na tabela *UserPossibleInfected* uma entrada contendo a data e o utilizador. Se este par de dados, não se encontrarem na tabela, é criado um novo registo. Por fim, é atualizado o contador que contabiliza o número de vezes que o utilizador se cruzou com alguém positivo. Após comparados os registos GPS, são verificados os registos Wi-Fi. Os dados são também comparados a cada dia. Se um utilizador esteve perto de uma rede Wi-Fi com o mesmo SSID pertencente a um registo de um utilizador infetado, esse utilizador será marcado como potencialmente infetado e o processo de marcação é semelhante ao descrito para coordenadas GPS.

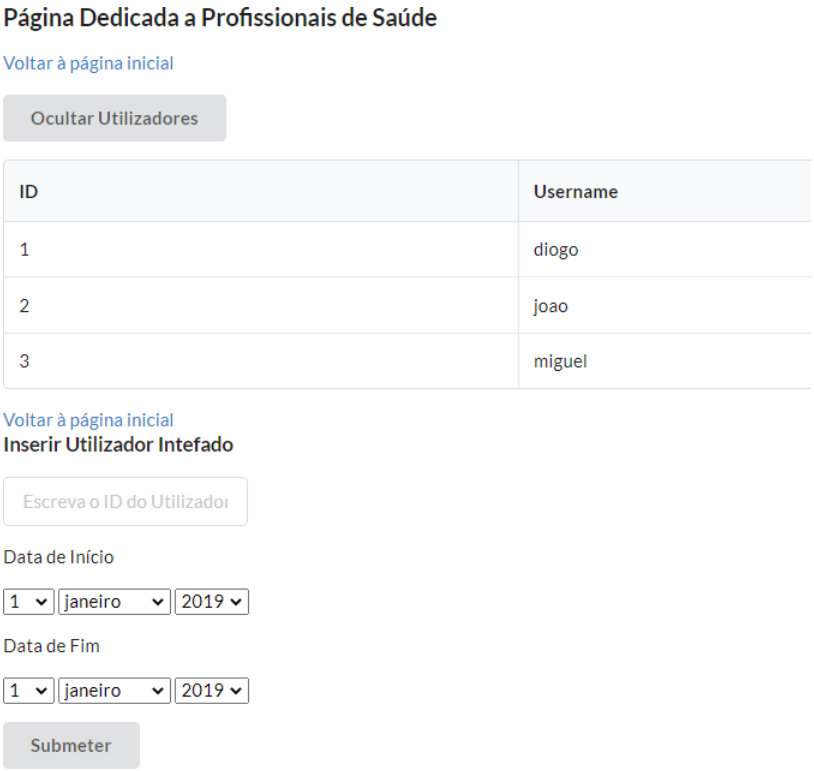


Figura 3.10: Página de Médicos com Utilizadores

3.3.4 Mapa de Tracking

O Mapa de Tracking nasceu da necessidade de poder ver, em tempo real, os locais no mapa onde houve mais registo de infetados. Este mapa está acessível a todos os utilizadores do sistema.

No mapa da fig. 3.11 é possível ver alguns marcadores vermelhos. Cada marcador vermelho existente no mapa, representa um conjunto de coordenadas GPS pertencentes a um utilizador que testou positivo. Quando se diminui o zoom da imagem, podem-se verificar uma série de marcadores vermelhos bastante próximos, indicando que, naquela área, existe uma grande densidade de tráfego de pessoas que testaram positivo, representando um local onde o contágio é bastante elevado. Se, pelo contrário, houver uma grande dispersão de marcadores vermelhos, indica que há uma baixa densidade de pessoas positivas.

Esta informação é importante estar disponível para todos os utilizadores para que, se possível, evitarem locais com grande densidade de pessoas infetadas.

O mapa visível nesta página é fornecido pela Google. Para tal, foi necessário importar esse recurso oferecido pela Google para o site. Após carregado o mapa, esta página contacta com a proxy a fim de receber informações acerca dos pontos a marcar. Por sua vez, a proxy contacta com a base de dados de registos GPS pedindo apenas os registos nos quais o marcador de perigo está ativo. O site, ao

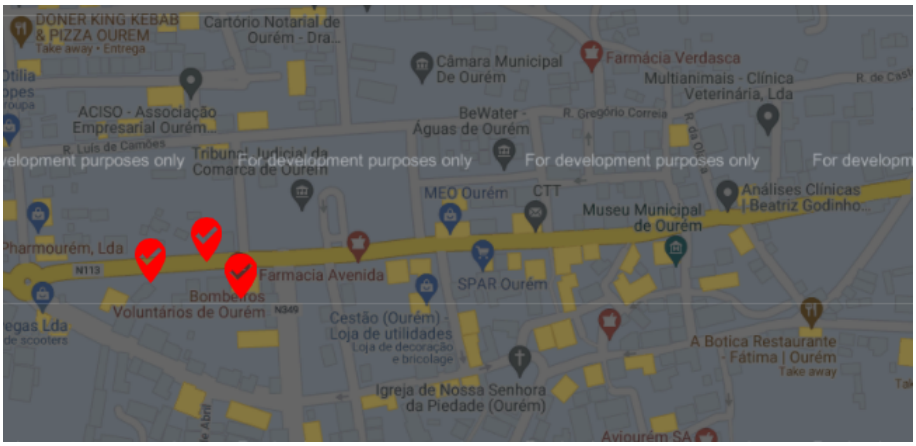


Figura 3.11: Mapa de Tracking

receber esses dados, faz uma marcação no mapa de cada um desses registos.

3.3.5 Página de Estatísticas

Paralelamente à página do site que contém o mapa, onde se faz um levantamento acerca dos dados fornecidos pela base de dados de registos de GPS, criou-se uma página que contém estatísticas acerca dos dados fornecidos pelas redes Wi-Fi.

Estatísticas de Wi-Fi

Voltar à página inicial

Atualizar Lista

SSID	Sinalizado	Não-sinalizado	[%]
Vodafone-CF2471	2	0	100
MEO-476430	1	0	100
MEO-WiFi	96	70	57.83
NOS-6B1C_EXT	1	0	100
NOS-6B1C	1	0	100
MEO-7F7363	1	0	100
AMOUREENSE	5	0	100
Pires	10	0	100
NOS-15C0	5	0	100
DIRECT-90-HP OfficeJet 3830	5	0	100

Figura 3.12: Estatísticas de Wi-Fi

A fig. 3.12 representa a página onde se faz a estatística das redes Wi-Fi. Cada linha da tabela representa apenas uma rede Wi-Fi. Como se sabe, cada entrada na tabela *WifiLog* da base de dados de registos Wi-Fi está presente um marcador de perigo, que pode estar ativo ou não, conforme o utilizador esteja positivo ou não. Assim, a tabela abaixo resume a quantidade de vezes que cada rede

está marcada com o marcador de perigo ou não. A última coluna representa a percentagem de pessoas que estiveram perto da rede e que testaram positivo.

A tabela é atualizada quando a página carrega ou quando é pressionado o botão *Atualizar Lista*. Ao atualizar, o site contacta a proxy a fim de obter os dados a mostrar. A proxy faz vários pedidos à base de dados de registos Wi-Fi, obtendo todos os dados necessários. Com todos os dados na proxy, são contabilizados, para cada SSID, o número de entradas que existem com o marcador de perigo ativo e inativo. Após essa contabilização, é calculada a percentagem de entradas com marcador de perigo ativos. Por fim, todos estes valores são transmitidos para o site.

4

Testagem do Sistema

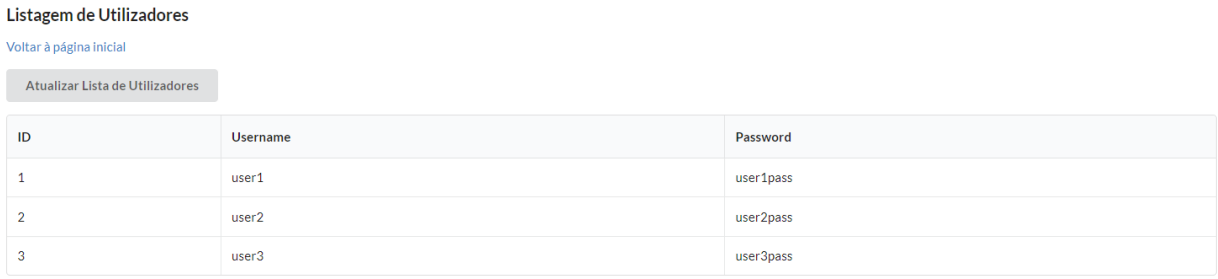
Conteúdo

Após desenvolvido todo o sistema, é necessário haver uma testagem de todo o sistema. Para tal, começou-se por recolher dados de navegação de vários utilizadores. De seguida, inseriram-se utilizadores positivos à doença e verificou-se se houve contactos de risco ou não.

4.1 Recolha de Dados

Para que haja uma testagem do sistema é necessário começar pela limpeza das bases de dados, a fim de eliminar todas as informações antigas.

De seguida, criou-se 3 novos utilizadores do sistema, conforme pode ser visto na fig. 4.1.


Listagem de Utilizadores

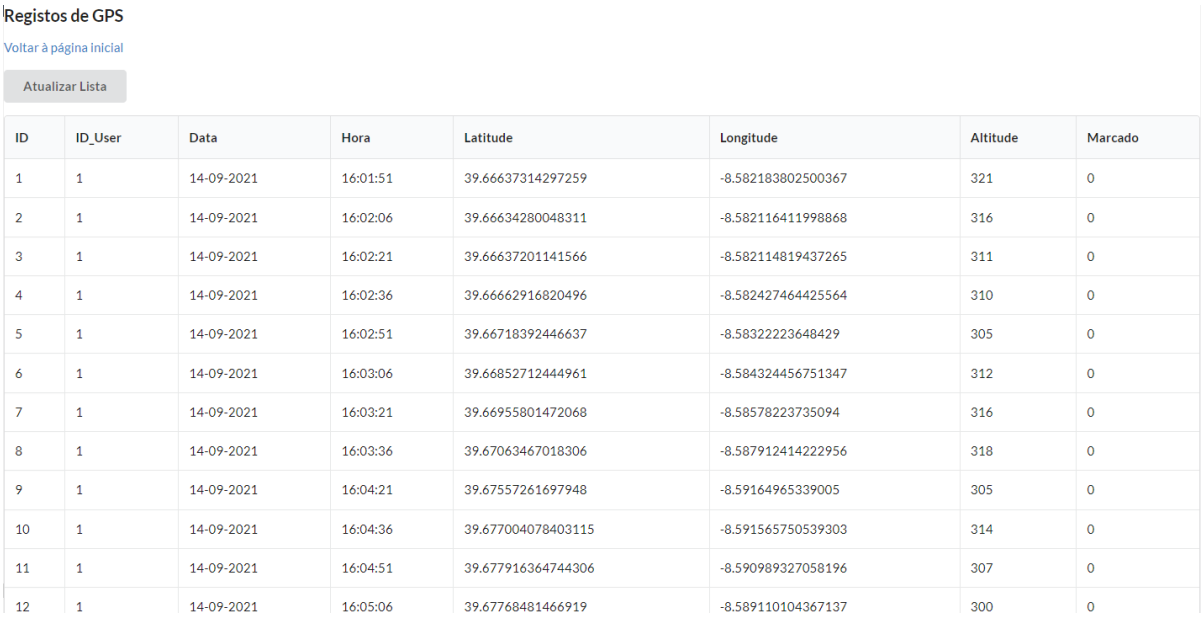
Voltar à página inicial

Atualizar Lista de Utilizadores

ID	Username	Password
1	user1	user1pass
2	user2	user2pass
3	user3	user3pass

Figura 4.1: Utilizadores Registados no Sistema

Visto que ainda se trata do início do teste do sistema, as listas de utilizadores infetados e de utilizadores potencialmente infetados ainda se encontram vazias. A fim de popular as restantes bases de dados, desenhou-se um percurso para que os três utilizadores recolham dados.


Registos de GPS

Voltar à página inicial

Atualizar Lista

ID	ID_User	Data	Hora	Latitude	Longitude	Altitude	Marcado
1	1	14-09-2021	16:01:51	39.66637314297259	-8.582183802500367	321	0
2	1	14-09-2021	16:02:06	39.66634280048311	-8.582116411998868	316	0
3	1	14-09-2021	16:02:21	39.66637201141566	-8.582114819437265	311	0
4	1	14-09-2021	16:02:36	39.66662916820496	-8.582427464425564	310	0
5	1	14-09-2021	16:02:51	39.66718392446637	-8.58322223648429	305	0
6	1	14-09-2021	16:03:06	39.66852712444961	-8.584324456751347	312	0
7	1	14-09-2021	16:03:21	39.66955801472068	-8.58578223735094	316	0
8	1	14-09-2021	16:03:36	39.67063467018306	-8.587912414222956	318	0
9	1	14-09-2021	16:04:21	39.67557261697948	-8.59164965339005	305	0
10	1	14-09-2021	16:04:36	39.677004078403115	-8.591565750539303	314	0
11	1	14-09-2021	16:04:51	39.677916364744306	-8.590989327058196	307	0
12	1	14-09-2021	16:05:06	39.67768481466919	-8.589110104367137	300	0

Figura 4.2: Dados GPS Recolhidos

Registos de Wi-Fi

Voltar à página inicial

Atualizar Lista

ID	ID_User	Data	Hora	SSID	Marcado
1	1	14-09-2021	16:01:36	MEO-REIS	0
2	1	14-09-2021	16:01:36	Vodafone-DDAA65	0
3	1	14-09-2021	16:01:51	MEO-REIS	0
4	1	14-09-2021	16:01:51	Vodafone-DDAA65	0
5	1	14-09-2021	16:01:51	Vodafone-DDAA65	0
6	1	14-09-2021	16:02:06	MEO-REIS	0
7	1	14-09-2021	16:02:06	Vodafone-DDAA65	0
8	1	14-09-2021	16:02:06	Vodafone-DDAA65	0
9	1	14-09-2021	16:02:21	MEO-REIS	0
10	1	14-09-2021	16:02:21	Vodafone-DDAA65	0
11	1	14-09-2021	16:02:36	MEO-REIS	0
12	1	14-09-2021	16:02:36	Vodafone-DDAA65	0

Figura 4.3: Dados Wi-Fi Recolhidos

As fig. 4.2 e fig. 4.3 mostram uma parte dos dados recolhidos. No total, foram recolhidos 92 registos GPS e 908 registos Wi-Fi. Para haver uma testagem eficaz do sistema, é necessário que a recolha de dados seja feita de forma a que seja possível prever os resultados. A recolha de dados foi feita de modo a que, geograficamente, o utilizador 1 apenas se cruzasse com o utilizador 2, e que o utilizador 3 também apenas se cruzasse com o utilizador 2.

Neste momento de testagem, o mapa de tracking encontra-se sem qualquer marcação e as estatísticas de Wi-Fi não têm qualquer registo de um SSID marcado.

4.2 Registo de Utilizadores Infetados

Após toda a recolha de dados, segue-se o teste do restante sistema, nomeadamente, a sua capacidade de inserir utilizadores positivos e de calcular possíveis contactos de risco.

Visto existirem 3 utilizadores no sistema, verifica-se o que acontece quando um dos três acusam positivo. Estudar-se-á os três casos isolados, isto é, a inserção de cada um dos utilizadores positivos quando os restantes continuam negativos.

Em cada caso, verifica-se a lista de contactos de risco, o mapa de tracking e as estatísticas de Wi-Fi.

4.2.1 Registo de Infeção do Utilizador 1

Começou-se por colocar o utilizador 1 na lista de infetados, conforme regista a fig. 4.4. O período de infeção escolhido corresponde apenas ao período em que foram recolhidos os dados.

Figura 4.4: Inserção de Utilizador 1 Positivo

Após a inserção, o sistema coloca o utilizador na base de dados. O passo seguinte é a verificação dos contactos de risco existentes. A fig. 4.5 regista os contactos de risco do utilizador 1.

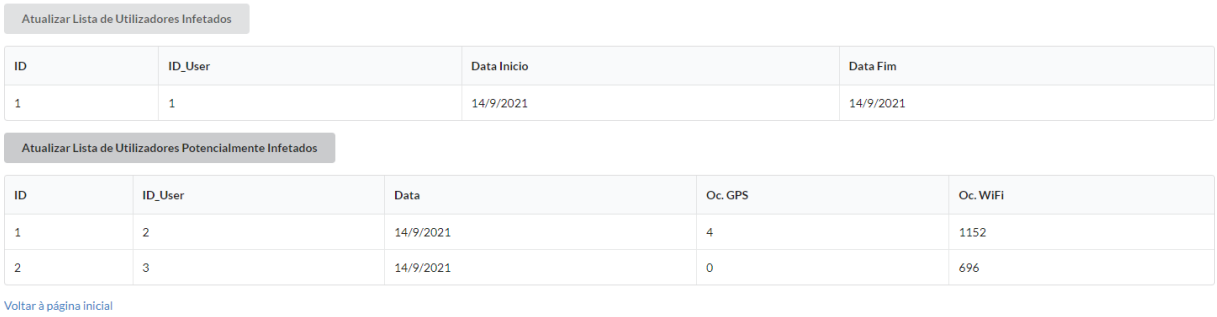


Figura 4.5: Contactos de Risco do Utilizador 1

Através da fig. 4.5, é possível verificar que o utilizador 1 esteve geograficamente próximo do utilizador 2 mas nunca esteve próximo do utilizador 3.

4.2.2 Registo de Infeção do Utilizador 2

De seguida, fez-se uma limpeza nas bases de dados a nível de registos de infeções e simulou-se o registo de infeção do utilizador 2.

Figura 4.6: Inserção de Utilizador 2 Positivo

Após o registo de infeção, o sistema calculou os seus contactos de risco, tendo em conta que nenhum dos outros dois utilizadores se encontram infetados. A fig. 4.7 regista os contactos de risco.

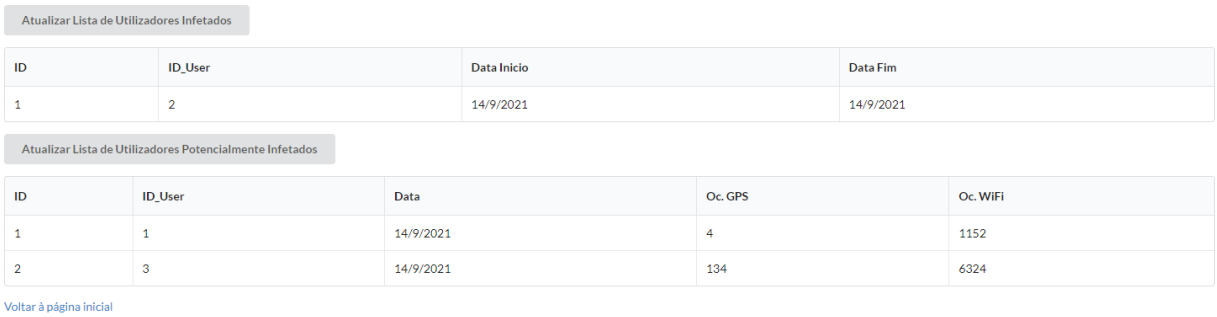


Figura 4.7: Contactos de Risco do Utilizador 2

Como foi referido anteriormente, o utilizador 2 é o único utilizador que tem contacto geográfico com os restantes utilizadores. Portanto, é normal haver o contactos de risco através de GPS com todos os utilizadores.

4.2.3 Registo de Infeção do Utilizador 3

Para o utilizador 3 repetiu-se o processo. Após limpeza das bases de dados, inseriu-se o utilizador 3 na lista de infetados.

Figura 4.8: Inserção de Utilizador 3 Positivo

Feita a inserção na base de dados, o sistema calculou os contactos de risco, presentes na fig. 4.9. Visto que o utilizador 3 apenas tem contacto geográfico com o utilizador 2, é normal não haver registo de contactos de risco atráves de GPS com o utilizador 1.

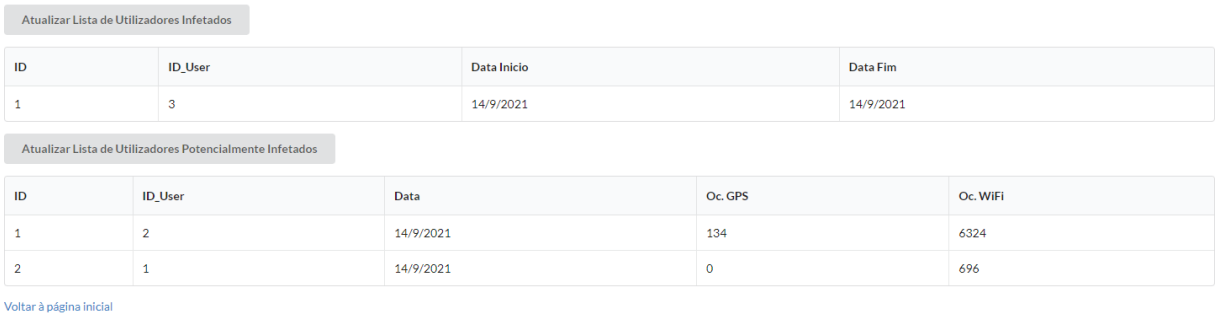


Figura 4.9: Contactos de Risco do Utilizador 3

4.2.4 Análise de Resultados

Através dos resultados demonstrados anteriormente, é possível retirar várias conclusões relativamente ao uso de coordenadas GPS e de SSID de redes Wi-Fi para a monitorização da doença.

O uso de GPS demonstra ser eficaz. As coordenadas obtidas através dos dispositivos móveis apresentam erro, que está diretamente ligado com a localização do utilizador. Se o utilizador estiver em ambientes abertos, a precisão ronda entre os 1 e os 10 metros. Contudo num ambiente urbano, existe reflexão dos sinais rádio, afetando o erro obtido. Tendo em conta os valores das coordenadas GPS obtidos, considerando os dados nas tabelas de contactos de risco, é possível concluir que o cálculo da distância entre coordenadas é feito de maneira correta, visto que, entre utilizadores, existem o mesmo número de contactos de risco por GPS. Considera-se, também, que um utilizador é um contacto de outro utilizador infetado se estiveram no local, no mesmo dia. Esta consideração é justificada com o facto de o vírus permanecer nas superfícies durante algum tempo.

Relativamente aos dados obtidos através de Wi-Fi, os resultados também são positivos. O cálculo do contacto de risco através de Wi-Fi é feito comparando os SSID que cada utilizador esteve próximo. Quando o SSID é igual, é incrementado o número de contactos de risco. Contudo, verifica-se algo inesperado entre os resultados entre os utilizadores 1 e 3. Estes utilizadores não estiveram geograficamente próximos, comprovado pelo número inexistente de contactos de risco por GPS. Mas, apresentam contactos de risco devido aos SSID das redes Wi-Fi. Este fenómeno ocorre devido a haver redes Wi-Fi, distantes entre si, mas com o mesmo nome de SSID.

5

Análise do Sistema

Conteúdo

Findo o desenvolvimento do sistema, é necessário analisá-lo de forma crítica, identificando as suas limitações e procurando eventuais melhorias a implementar numa próxima fase de desenvolvimento.

Neste capítulo, começa-se por analisar qualitativamente a capacidade de resposta dos servidores UDP e da proxy. Visto haver apenas um servidor UDP para a receção dos dados recolhidos nos dispositivos móveis, pode haver informação perdida. A proxy pode também sofrer de uma sobrecarga de pedidos vindos da web que provoque lentidão nas respostas aos pedidos. Por fim, são sugeridas algumas melhorias para posteriormente implementar no sistema.

5.1 Análise dos Servidores UDP

Ambos os servidores UDP, o dedicado aos utilizadores e o dedicado à receção de dados de navegação, são servidores que correm apenas numa thread, isto é, não executam mais do que uma função em simultâneo.

O servidor dedicado à receção de dados de navegação, após a abertura da socket e a ligação às bases de dados, inicia um ciclo repetitivo. Nesse ciclo, a primeira instrução é a receção de um pacote UDP vindo da socket previamente aberta. Após a receção no pacote, o servidor processa a informação recebida e, só após processada essa informação, é que volta a estar disponível para a receção de um novo pacote UDP. O processamento envolve a descodificação da mensagem recebida e a conexão à base de dados correspondente para a inserção de um novo registo. Um dispositivo móvel recolhe dados a cada 15 segundos. Os dados recolhidos são relativos às coordenadas GPS e aos SSID da redes Wi-Fi disponíveis. A cada 15 segundos, são enviadas pelo dispositivo móvel um mínimo de dois pacotes UDP, tendo em conta que é possível obter coordenadas e que existem redes disponíveis. Por minuto, são enviados, no mínimo, 8 pacotes. Se existirem poucos utilizadores, o ciclo repetitivo é rápido o suficiente para receber um pacote, processá-lo e voltar à escuta de mais pacotes. Contudo, este sistema foi desenhado para ser usado pelo máximo de utilizadores possíveis, para que exista mais informação acerca dos utilizadores e, consequentemente, uma melhor previsão de utilizadores potencialmente infetados. Quantos mais utilizadores existem, mais informação é enviada para o servidor UDP, aumentando o número de ligações às bases de dados. Este aumento de ligações às bases de dados pode implicar uma sobrecarga das mesmas, podendo progredir para um aumento significativo do tempo de ligação do servidor às bases de dados. Esse aumento do tempo de ligação implica que o ciclo repetitivo também aumente o seu tempo de execução. Assim, o servidor fica menos disponível para receber pacotes através da sua socket visto que o ciclo repetitivo demora mais tempo. Num sistema com bastantes utilizadores, existe muito mais informação para ser transmitida e a informação demora mais a ser processada. Esta situação pode traduzir-se na perda de pacotes UDP, que nunca chegam ao servidor.

No servidor dedicado aos utilizadores, a situação descrita anteriormente não acontece tão frequentemente. Apesar da estrutura do servidor ser semelhante, isto é, um ciclo repetitivo cuja primeira instrução é a receção de um pacote UDP, este servidor apenas é contactado uma vez por cada utilizador, havendo menos possibilidade do servidor não receber todos os pacotes.

Para que não haja perdas de informação no servidor UDP, uma solução seria a descentralização do servidor. Com a criação de vários servidores, os pacotes seriam distribuídos de forma uniforme por cada servidor sem haver uma sobrecarga de apenas um servidor. A existência de vários servidores permite redundância, implicando que, cada vez que algum servidor sofra um ataque ou falhe a conexão à rede, os pacotes sejam reencaminhados para outro servidor, evitando perdas de informação.

5.2 Análise das Bases de Dados

Uma limitação deste sistema é a memória e o armazenamento dos dados guardados. Este sistema quer-se usado pelo máximo de utilizadores pelo que, quantos mais utilizadores, maior a quantidade de dados a armazenar.

Cada base de dados tem a limitação da memória correspondente à máquina em que está a correr. Portanto, com o número de utilizadores a aumentar, aumenta também os dados recolhidos pela aplicação.

Para que não haja perdas de informação armazenadas, a solução seria criar uma base de dados implementada em várias máquinas. Assim, o sistema teria uma memória facilmente escalável com o número de utilizadores.

5.3 Análise do Servidor HTTP

A proxy é o componente do sistema responsável pelo envio de dados para o website. O envio de dados corresponde ao envio de páginas HTML, mas também corresponde ao envio de dados presentes nas bases de dados. Para tal, é necessário haver conexão com as bases de dados, para que seja possível ler e escrever informação.

Como acontece nos servidores UDP, conforme aumentam os utilizadores na web, mais são os pedidos para a proxy. Caso haja uma grande quantidade de pedidos, a proxy pode sofrer uma sobrecarga. A sobrecarga pode levar à lentidão das respostas da proxy para o website. Para cada pedido de informação à proxy é necessário recolher informação contida nas bases de dados. Portanto, uma sobrecarga à proxy, pode resultar numa sobrecarga de pedidos às bases de dados, afetando a sua eficácia de resposta.

A fim de reduzir as sobrecargas da proxy, uma solução seria a replicação da proxy. Com essa

replicação, os pedidos vindos da web seriam distribuídos pelas várias proxies existentes. A redução no número de vezes em que há conexão às bases de dados implicaria numa diminuição de tempo de resposta dos pedidos web. Uma solução para conseguir reduzir o número de conexões com as bases de dados seria implementar uma memória temporária na proxy, com os dados contidos nas bases de dados. Seria necessária uma atualização periódica desses dados, contudo iria reduzir o número de procuras nas bases de dados.

6

Considerações Finais

Conteúdo

6.1 Aspetos Futuros

O sistema que foi desenhado, encontra-se implementado e está a funcionar. Contudo, foram encontradas algumas limitações que se impõe resolver numa próxima fase de desenvolvimento. Para além das limitações, encontraram-se também uns aspetos a melhorar.

A lista seguinte reúne todos os tópicos que apresentem limitações ou possíveis melhoramentos da aplicação, do servidor e do site:

Melhoramento do estado de atividade da aplicação. No normal funcionamento da aplicação para dispositivos móveis, a aplicação desliga-se automaticamente quando o utilizador deixa de pressionar o ecrã durante algum tempo. Sendo esta uma aplicação em que não tem a necessidade de interação do utilizador, este aspeto apresenta uma limitação devido a parar de recolher informações de navegação.

Funcionamento da aplicação em segundo plano. Como referido no ponto anterior, esta é uma aplicação que não necessita da interação do utilizador. Um melhoramento para a aplicação seria o seu normal funcionamento em segundo plano. Assim, a recolha de informações de navegação não fica comprometida.

Otimização de obtenção de coordenadas GPS. Quando é iniciada a aplicação, o processo de obtenção de coordenadas GPS começa automaticamente. Por vezes, acontece que as primeiras coordenadas obtidas não correspondem com o local onde foram obtidas. Isto acontece porque a aplicação possivelmente guarda numa memória local as coordenadas previamente obtidas antes do término da aplicação. Uma proposta de melhoria seria a obtenção com precisão das primeiras coordenadas GPS.

Melhoramento da página de login dos utilizadores. Atualmente a página de login da aplicação apenas apresenta dois campos: um para a introdução do nome de utilizador e outro para a introdução da palavra-passe. Quando se pressiona o botão, é iniciada a sessão, caso o utilizador já se tenha registado no sistema ou, caso contrário, é criado um novo utilizador. Uma proposta de melhoria seria a separação de início de sessão da criação de um novo utilizador. Para tal, seria necessário criar uma nova página na aplicação onde seja possível recolher todos os dados necessários. Com esta implementação, seria possível obter mais dados relativos aos utilizador como, por exemplo, o número de telemóvel e o e-mail.

Uso de criptografia para o nome de utilizador e palavra-passe. Ao fazer o login, o utilizador coloca o seu nome de utilizador e a palavra-passe. Para verificar que esse par correspondem mutuamente, é enviado, através de uma mensagem de texto, o conteúdo preenchido pelo utilizador. A palavra-passe está incluída na mensagem de texto que viaja desde a aplicação móvel para o servidor UDP responsável pela gestão de utilizadores. Sendo uma mensagem de texto, facilmente pode

ser pirateada. Uma solução para este problema seria a utilização de encriptação da palavra-passe, onde a encriptação e desencriptação fosse apenas possível na aplicação para dispositivos móveis e no servidor UDP.

Correção da aplicação quando há comunicação do utilizador. Quando se comunica o nome de utilizador e a palavra-passe para o servidor, a aplicação fica a aguardar a resposta do servidor. Contudo, pode haver um erro do servidor em que este não esteja online. Caso isto aconteça, o servidor não envia a resposta à aplicação. No entanto, a aplicação só avança no seu normal funcionamento quando receber a resposta. Esta situação origina um erro na aplicação que só é ultrapassado encerrando forçadamente a aplicação.

Transferência de dados de navegação para o servidor. Como está desenvolvida a aplicação, os dados de navegação são recolhidos a cada 15 segundos e são logo enviados para o servidor UDP responsável pela receção desses dados. A fim de evitar o constante envio de dados, uma solução seria implementar uma memória local desses registos em que apenas seriam enviados para o servidor UDP apenas duas a três vezes por dia. Esta implementação, reduziria as interações com o servidor, o que não provocaria tanta sobrecarga ao servidor. Para que esta melhoria funcionasse bem, as aplicações para dispositivos móveis não podiam comunicar com o servidor ao mesmo tempo. Teria de haver uma dispersão temporal das comunicações.

Site sempre disponível online. Neste momento de desenvolvimento de todo o sistema, todos os servidores estão alojados localmente num computador pessoal. No próximo passo de desenvolvimento deste sistema, uma implementação seria colocar o sistema disponível a toda a hora.

Melhoria ao nível do front-end do site. O site foi criado com a necessidade de ver, em tempo real, todos o conteúdo presente nas bases de dados. Como é possível verificar nas imagens da seção 3.3, o front-end das páginas do site são baseados em simples HTML. Uma melhoria possível seria o embelezamento das páginas do site.

Criação de uma área de administração. No site, todas as páginas estão disponíveis a todos os seus utilizadores. Numa fase futura de desenvolvimento, será necessário haver uma restrição de quem pode aceder às páginas. Portanto, será necessário haver uma criação de credenciais para o acesso a essas páginas. As credenciais seriam divididas entre administradores do sistema e profissionais de saúde. Os administradores do sistema, teriam acesso a todo o conteúdo presente nas bases de dados e seriam responsáveis pela manutenção do sistema. Apenas os profissionais de saúde teriam acesso à página onde se inserem utilizadores positivos à doença. Os utilizadores comuns teriam acesso à página de estatísticas e ao mapa.

Melhoria do mapa. No mapa encontram-se todos os locais por onde os utilizadores positivos à doença estiveram. O mapa utilizado é um mapa fornecido pela Google, para o qual foi necessário adquirir credenciais para a sua utilização. Por ser para um trabalho escolar, no mapa aparece

escrito *For development purposes only*. Na próxima etapa, seria retirar esse texto. De seguida, uma melhoria seria mudar o tipo de mapa existente. Em vez de haver uma marca por cada coordenada existente, seria interessante implementar uma mapa de pontos quentes, em que as regiões mais quentes correspondem a zonas onde há mais infetados.

Comunicação de contactos de risco. Neste momento de desenvolvimento, os contactos de risco são disponibilizados apenas numa página do site. Com as melhorias de implementação, seria interessante haver uma recolha de mais dados relativos a cada utilizador, como já foi referido. Uma modificação a ser feita numa fase posterior de desenvolvimento, seria a mudança de como se avisa um utilizador que teve um contacto de risco. Ao haver uma recolha dos dados telefónicos, quando se deteta um contacto de risco, em vez de haver uma lista, podia ser enviada uma mensagem de texto.

6.2 Conclusão

O desenvolvimento da dissertação mostrou-se bastante exigente, tanto a nível do planeamento, como na parte do desenvolvimento e da conceção do sistema.

Inicialmente, efetuou-se toda a pesquisa necessária para desenvolver este sistema. Procurou-se saber os projetos já existentes a este nível bem como as tecnologias que usavam. Paralelamente, foi-se desenhando o sistema, que seria implementado mais tarde. Pensou-se nas tecnologias a usar e na arquitetura do sistema, tendo em conta as suas especificações.

De seguida, iniciou-se o desenvolvimento de todo o sistema. A primeira etapa foi a conceção da aplicação. Durante o desenvolvimento da aplicação, surgiram alguns problemas na obtenção das coordenadas GPS, que rapidamente foram solucionados. Após verificado o bom funcionamento da aplicação, desenvolveu-se os servidores UDP para a receção dos dados no sistema. Testaram-se os servidores e confirmou-se que os dados eram bem recebidos pelo sistema. Para que os dados fossem armazenado pelo sistema, implementou-se as bases de dados. A mesmo tempo que se desenvolviam as bases de dados, desenvolveu-se também o servidor HTTP e parte do site para que fosse possível ver, em tempo real o conteúdo das bases de dados. Por fim, implementaram-se as restantes páginas do site, nomeadamente as páginas de médicos e de estatísticas. Durante esta fase de execução foram sendo efetuadas correção de erros que foram prontamente detetados.

A fase seguinte foi dedicada ao teste do sistema como um todo. Testou-se o sistema em diversos cenários e, em todos eles, o sistema produziu os resultados expectáveis. Durante esta fase foram também levantados alguns aspetos que futuramente são suscetíveis a melhorias.

Este sistema, apesar de estar a funcionar corretamente e produzir os resultados corretos, apresenta fragilidades. Uma das fragilidades é a proteção de dados pessoais. Não se encontra implementado

qualquer tecnologia que proteja os dados pessoais de cada utilizador. Futuramente, este sistema terá que usar tecnologias que protejam os dados pessoais transferidos entre os diversos componentes do sistema. Outro aspeto tem a ver com a quantidade de dados recolhidos pelo sistema. Quantos mais utilizadores estiverem inscritos no sistema, maior a quantidade de dados recolhidos pelo mesmo. Uma maior diversidade de dados, implica uma melhor previsão de contactos de risco que, por conseguinte, credibiliza ainda mais o sistema. Contudo, devido à legislação em vigor, a população não pode ser obrigada a utilizar este sistema. Apenas com uma adesão massiva e voluntária da população é que se irá obter bons resultados.

Bibliografia

[1] Funcionamento das Aplicações. (Acedido a 09 Dez 2020). [Online]. Available: https://pplware.sapo.pt/internet/covid-19-afinal-como-funcionam-as-solucoes-para-rastrear-contactos/

[2] StayAway Covid. (Acedido a 17 Out 2020). [Online]. Available: https://stayawaycovid.pt/

[3] Informações acerca da StayAway Covid. (Acedido a 17 Out 2020). [Online]. Available: https://stayawaycovid.pt/wp-content/uploads/STAWAWAY-COVID-doc.pdf/

[4] DP-3T. (Acedido a 09 Dez 2020). [Online]. Available: https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing

[5] FollowMyHealth. (Acedido a 17 Out 2020). [Online]. Available: https://pplware.sapo.pt/informacao/followmyhealth-app-portuguesa-ja-disponivel-para-tracing-a-covid-19/

[6] monitorCovid19.pt. (Acedido a 17 Out 2020). [Online]. Available: https://pplware.sapo.pt/smartphones-tablets/monitorcovid19-pt-a-app-portuguesa-para-rastrear-contagios-de-covid-19/

[7] TraceTogether. (Acedido a 17 Out 2020). [Online]. Available: https://www.tracetogether.gov.sg/

[8] PEPP-PT. (Acedido a 17 Out 2020). [Online]. Available: https://pplware.sapo.pt/informacao/pepp-pt-app-para-monitorizar-movimentos-dos-cidadaos-por-causa-da-covid-19/

[9] COVIDSafe. (Acedido a 19 Out 2020). [Online]. Available: https://pplware.sapo.pt/smartphones-tablets/covidsafe-australia-lanca-uma-polemica-aplicacao-para-rastreio-da-doenca/

[10] Aplicação da COVIDSafe. (Acedido a 19 Out 2020). [Online]. Available: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#about-the-app

[11] Aplicação da SwissCovid. (Acedido a 19 Out 2020). [Online]. Available: https://play.google.com/store/apps/details?id=ch.admin.bag.dp3t

[12] SwissCovid. (Acedido a 19 Out 2020). [Online]. Available: https://en.wikipedia.org/wiki/SwissCovid

[13] Aplicação da Radar COVID. (Acedido a 19 Out 2020). [Online]. Available: https://play.google.com/store/apps/details?id=es.gob.radarcovid

[14] Radar COVID - Espanha. (Acedido a 19 Out 2020). [Online]. Available: https://www.dinheirovivo.pt/empresas/tecnologia/espanha-lanca-app-anti-covid-antes-de-portugal-app-nacional-esta-para-breve-12893789.html

[15] Aplicação da STOP COVID19 CAT. (Acedido a 19 Out 2020). [Online]. Available: https://play.google.com/store/apps/details?id=cat.gencat.mobi.StopCovid19Cat

[16] STOP COVID19 CAT. (Acedido a 19 Out 2020). [Online]. Available: https://stopcovid19.cat/en/stop-covid19-cat/

[17] Bluetooth Low Energy. (Acedido a 09 Dez 2020). [Online]. Available: https://pt.wikipedia.org/wiki/Bluetooth_Low_Energy#cite_note-2

[18] O que é o Bluetooth Low Energy. (Acedido a 09 Dez 2020). [Online]. Available: https://elainnovation.com/what-is-ble.html

[19] Visão geral de Bluetooth Low Energy. (Acedido a 09 Dez 2020). [Online]. Available: https://developer.android.com/guide/topics/connectivity/bluetooth-le

[20] Notificações de Exposição relativas à COVID-19. (Acedido a 09 Dez 2020). [Online]. Available: https://www.google.com/covid19/exposurenotifications/

[21] Notificações de Exposição. (Acedido a 09 Dez 2020). [Online]. Available: https://en.wikipedia.org/wiki/Exposure_Notification

[22] HMAC-SHA-256. (Acedido a 09 Dez 2020). [Online]. Available: https://pt.wikipedia.org/wiki/HMAC

[23] AES. (Acedido a 09 Dez 2020). [Online]. Available: https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard

[24] Global Positioning System. (Acedido a 03 Jan 2021). [Online]. Available: https://www.gps.gov/

[25] G. Maral and M. Bousquet, “Satellite Communications Systems: Systems, Techniques and Technology,” ser. 5th ed. West Sussex, England: John Wiley and Sons, Ltd., 2010.

[26] “Navstar GPS Space Segment/Navigation User Segment Interfaces, Interface Specification IS-GPS-200, Revision M, Global Positioning Systems Directorale,” 13 Abril 2021. [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf

[27] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, “GNSS - Global Navigation Satellite System: GPS, GLONASS, Galileo and more,” Wien: Springer, 2008.

[28] GLONASS. (Acedido a 03 Jan 2021). [Online]. Available: https://www.glonass-iac.ru/

[29] Beidou. (Acedido a 03 Jan 2021). [Online]. Available: http://en.beidou.gov.cn/

[30] Galileo. (Acedido a 03 Jan 2021). [Online]. Available: https://www.euspa.europa.eu/

[31] Protocolos de Comunicação TCP vs. UDP. (Acedido a 12 Ago 2021). [Online]. Available: https://www.lifesize.com/en/blog/tcp-vs-udp/

[32] Protocolos de Comunicação TCP e UDP. (Acedido a 29 Ago 2021). [Online]. Available: https://www.geeksforgeeks.org/differences-between-tcp-and-udp/

[33] JSVM Reference Software. (Acedido a 06 Set 2021). [Online]. Available: https://www.welivesecurity.com/br/2019/12/20/o-que-e-um-proxy-e-para-que-serve/