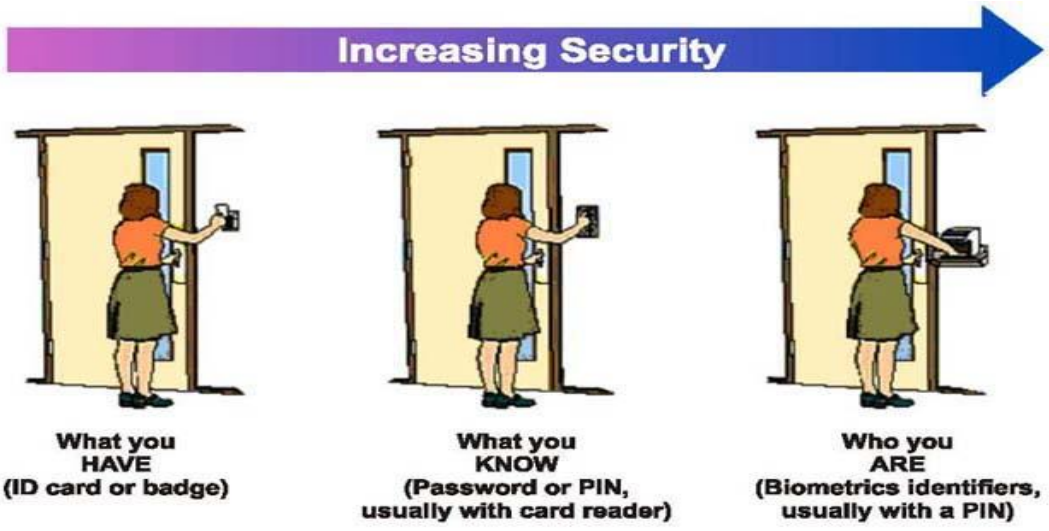
INSTITUTO SUPERIOR TÉCNICO

REDES MÓVEIS E SEM FIOS

PROJETO FINAL

Controlo de entrada e saída de pessoas de instalações críticas



[Source 1 - Referências]

Trabalho Realizado pelo Grupo 4:

- João Pedro Costa Luís Cardoso, nº 84096
- Matilde Pereira Moreira, nº84137

Docente: António Manuel Raminhos Cordeiro Grilo

2º Semestre 2018/2019

ÍNDICE

INTRODUÇÃO

Nos dias de hoje, a maioria das pessoas está familiarizada com dispositivos de acesso comuns que limitam, impedem e até mesmo controlam o movimento dentro de um edifício ou área, como fechaduras eletromagnéticas, a segurança tradicional (cartão e segurança), identificação biométrica, entre outros dispositivos.

Cada vez mais é importante monitorizar a entrada e saída das pessoas dos ambientes, não só para garantir a segurança das mesmas, mas também o sigilo das informações e a integridade dos bens. Contar com sistemas ou equipamentos efetivos para fazer este monitoramento é essencial e não é possível manter um profissional 100% do seu tempo a fazer gestão de acesso de todos os ambientes, essencialmente em instalações críticas. Para além disso, a gestão humana é suscetível de falha.

À medida que as novas tecnologias, como identificação biométrica, *iris scan* e o gerenciamento remoto de dados de segurança se tornam mais amplamente disponíveis, a segurança tradicional começa a ser substituída por esses sistemas de segurança eficientes, que fornecem a identificação e o rastreamento da atividade humana nas instalações críticas (e.g. *data centers*, hospitais, bancos, entre outros).

Dessa forma, é possível assegurar a entrada de pessoas autorizadas, bloquear os não autorizados, gerenciar diferentes níveis de acesso nas diversos zonas, garantir a segurança de todos e a integridade de bens e dados. Para além disso, é possível ter informações sobre o número de pessoas, qual o horário de maior fluxo e ainda quais as zonas com mais afluência de pessoas.

Neste projeto pretende-se implementar um sistema de controlo de entrada e saída de pessoas numa dada instalação crítica, considerámos como exemplo os edifícios governamentais. Para tal recorreu-se a um cartão RFID (identificação por radiofrequência), que usa a frequência de rádio para capturar dados e a uma câmara *VGA CMOS*, que irá capturar a fotografia da pessoa, caso essa pessoa não tenha acesso para entrar na dada zona.

Neste relatório vários assuntos irão ser abordados, nomeadamente:

- **Definição Generalista do Problema -** Uma análise geral a conceitos e perguntas importantes sobre sistemas de segurança que se cruzam com a nossa análise e pesquisa acerca do nosso projeto. Neste capítulo é feita uma abordagem sobre temáticas como : O que é preciso proteger? Quem és tu? Porque estás aqui?
- **Visão Geral –** Quais os componentes de *hardware* a utilizar? Identificação funcional, bibliotecas necessárias? O que fazer? De que forma se irá implementar?
- **Arquitetura da Solução –** Diagrama de Fritzing
- **Diferenças relativamente ao Projeto Intermédio –** Neste capítulo são listadas todas as alterações que se teve de fazer relativamente ao projeto intermédio.
- **Exemplos de Testes Realizados –** Neste setor são abordados casos realizados para testar a implementação do projeto
- **Conclusão / Estado da implementação do projeto –** O que falta fazer e o que já está feito?

DEFINIÇÃO GENERALISTA DO PROBLEMA

Dos temas fornecidos pelo professor, o que nos pareceu mais interessante para desenvolver ao longo do semestre foi o desenvolvimento de um sistema de controlo de entrada e saída de pessoas numa instalação crítica. Da análise sobre esta temática recorrendo a livros e à internet surgiu-nos alguns conceitos e perguntas que considerámos bastante importantes.

Neste capítulo definimos o problema: controlo de entrada e saída das pessoas de forma a promover a segurança das pessoas e dos edifícios, definindo as perguntas essenciais acerca da segurança.

Quando a segurança numa instalação crítica é mencionada, os primeiros aspetos que provavelmente vêm à mente são o medo do roubo de dados, a proteção contra sabotagem ou até mesmo espionagem. Embora surja a necessidade de proteção contra intrusos e possíveis danos intencionais, os riscos decorrentes da atividade diária dos trabalhadores nessas instalações representam um risco ainda maior.

A tecnologia de reconhecimento está a mudar tão rapidamente quanto as instalações e a informação e comunicação que protege, pelo que se torna fácil esquecer um dos maiores problemas que esta tecnologia está a tentar resolver: **manter pessoas não autorizadas e que representem um perigo para a empresa fora dos lugares interditos.**

O primeiro passo prende-se com o mapeamento das áreas seguras da instalação e definição de regras de acesso, pelo que os diretores devem definir as pessoas que têm de ter acesso e quais são as zonas que lhes são permitidas. O desafio é o segundo passo, isto é, o momento em que se decide quais as melhores tecnologias que produzem resultados mais eficientes. Surgem então duas grandes perguntas face ao problema: **Quem és tu? E porque estás aqui?**

Embora as tecnologias de segurança que tenham surgido possam parecer sofisticadas – *fingerprint, hand scans, eye scans, smart cards, facial geometry* – o objetivo subjacente de segurança é simples a todos nós: obter uma resposta plausível para as perguntas: **Quem és tu? E porque estás aqui?**

Quando se pretende projetar um sistema de segurança automatizado, a primeira pergunta – Quem és tu? – causa a maior parte dos problemas para a projeção. Nos dias de hoje, todas as tecnologias tentam avaliar a identidade de uma pessoa seja de uma forma ou de outra, e com diferentes graus de certeza, sendo o custo da tecnologia, um fator crucial na definição do grau. Por exemplo, um cartão magnético é barato e fornece uma identidade incerta, pois não temos a certeza de quem está a usar o cartão. Já a *iris scan* é bastante dispendiosa, mas precisa.

A resposta para a segunda pergunta: "Porque estás aqui?" – por outras palavras, qual é o teu papel neste dado ponto de acesso – pode estar implícito quando a identidade da pessoa já tiver sido estabelecida ou pode ser implementada em diversas formas: combinar as informações da pessoa na banda magnética do cartão; a identidade de uma pessoa poderia invocar informações de um arquivo de computador que listasse os acessos permitidos; ou pode haver diferentes métodos de acesso para diversas zonas da instalação crítica, projetadas para permitir diferentes acessos com diferentes finalidades.

VISÃO GERAL

Após uma análise aprofundada sobre os conceitos inerentes à implementação do projeto abordados no capítulo *Definição Generalista do Problema*, procede-se às respostas às perguntas feitas: **Quem és tu? E porque estás aqui?** Para responder a estas perguntas surge o módulo RFID – RC522 que deteta se a pessoa tem acesso ou não a uma dada zona no edifício (considerado hipoteticamente como o edifício governamental), identificando também a pessoa. Se a pessoa não tiver acesso é acionado um sensor complexo que é câmara OV7670 CMOS que captura a fotografia da pessoa para ficar registada a imagem na Cloud (Firebase).

Este projeto implica a construção de vários componentes hardware e software:

- RFID - RC522 Módulo de Sensor de Cartão, que irá ser controlado pelo Arduíno UNO Rev. 3.
- VGA OV7670 CMOS SCBS Módulo de Câmara, que se irá ligar ao arduíno.
- Módulo WiFi ESP8266 que permite a conexão do arduíno com a rede Wi-Fi.
- Base de Dados em tempo real da *Firebase* (produto da google) que irá servir como intermediário entre a aplicação e o arduíno em questão.
- Arduíno UNO Rev. 3 é um microcontrolador que irá ter acoplado um sensor RFID e um módulo de Câmara, que irá tirar uma fotografia caso o acesso da pessoa seja interdito.
- Aplicação Android que constitui a interface gráfica para o utilizador.

Na Figura 1 é apresentado um esquema geral do projeto e como os componentes se interligam entre si.

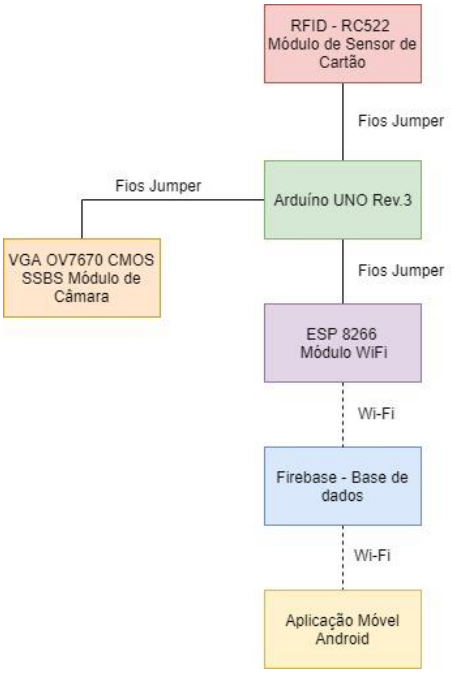


Figura 1 – Esquema geral do projeto a implementar

MÓDULOS

❖ Arduíno UNO Rev.3

O arduíno Uno Rev.3, que é apresentado na Figura 2, é um arduíno Uno **sem** módulo WiFi integrado e é a placa mais utilizada e vendida nos dias de hoje. A placa é baseada no microcontrolador ATmega328P. Tem 14 pinos digitais de entrada/saída (dos quais 6 podem ser usados como saídas PWM), 6 entradas analógicas, um cristal de 16 MHZ, uma conexão USB, um conector de alimentação, um ICSP e um botão reset. Contém tudo o que é necessário para apoiar o microcontrolador. Esta placa Arduíno Uno é a última versão disponível (também conhecida como Das3) traz melhorias em relação às anteriores:

- ATmega 16U2 de comunicação serial USB em substituição ao 8U2;
- Circuito de Reset mais robusto;
- Dois outros pinos adicionados próximos ao RESET, o IOREF que permite aos shields se adaptarem à voltagem fornecida pela placa. No futuro os shields serão compatíveis tanto com as placas que utilizam o AVR e operam a 5V, como com o Arduíno Due que operará a 3,3V. O segundo pino não está conectado e é reservado para propósitos futuros.

O ATmega328P oferece 2KB de SRAM, 32KB de Flash, 1 UART, 1 KB de EEPROM e um ADC de alta velocidade integrado. ATmega328 fornece comunicação serial UART TTL (5V) que está disponível nos pinos digitais 0 (RX) e 1 (TX). Um ATmega8U2 na placa canaliza esta comunicação para a USB e aparece como uma porta virtual para o software no computador.

Figura 2 - Arduíno UNO Wi-Fi Rev.2

Este arduíno irá ser acoplado através de fios Jumper a um módulo WiFi, a um sensor de cartão RFID e a um módulo de uma câmara que irá capturar a imagem da pessoa caso tente aceder a uma zona à qual não tem permissão, pelo que o arduíno é o cérebro do projeto, isto é, será aqui que as decisões irão ser tomadas (permitir o acesso ou não e se tira a fotografia).

Os componentes a desenvolver neste módulo são: comunicação com o exterior, controlo e configuração da câmara, executar a transmissão do stream de imagem por WiFi e o controlo de acesso das pessoas recorrendo a software arduíno.

Na Figura 3 é apresentado o esquema do arduíno com os módulos importantes que irão ser usados.

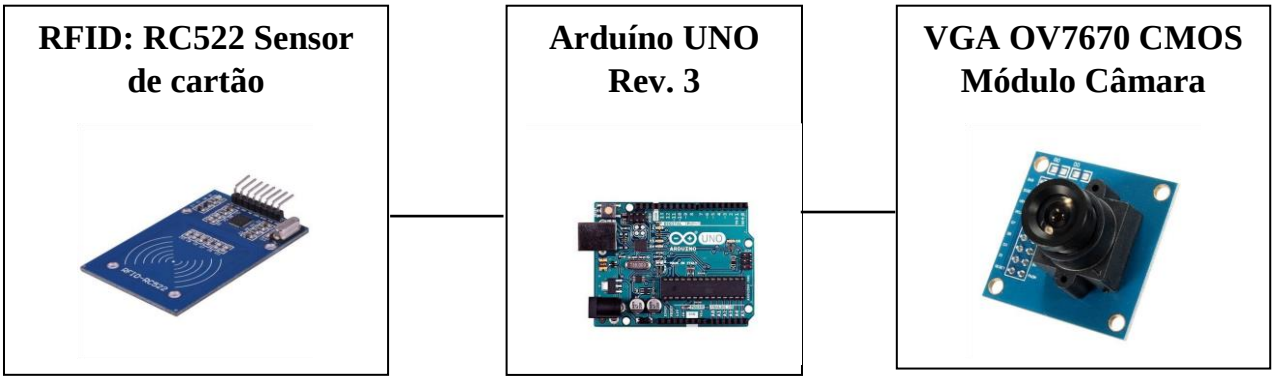


Figura 3 - Esquema do arduíno com os respetivos módulos a usar

❖ RFID: RC522 - Módulo de Sensor de Cartão

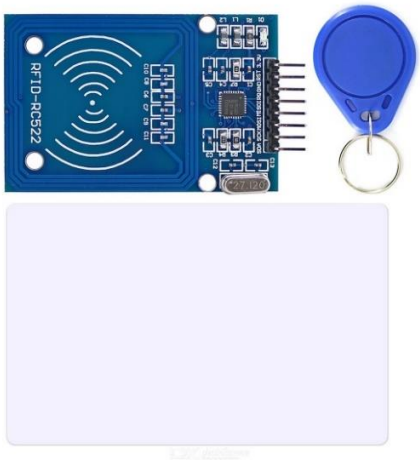


Figura 4 - Módulo RFID com as respetivas tags

O Módulo RFID, apresentado na Figura 4, é baseado no chip MFRC522 e é utilizado na comunicação sem fios a uma frequência de 13,56MHz. Este chip, de baixo consumo e pequeno tamanho, permite ler e escrever sem contacto em cartões que seguem o padrão Mifare. Ele possui as ferramentas que precisa para um projeto de controlo de acesso ou sistemas de segurança. As tags RFID podem conter vários dados sobre o proprietário do cartão, como o nome, o contacto e o departamento em que trabalha. Na Tabela 1, segue-se as especificações do módulo RFID.

Especificações:

• Consumo: 13-26mA / DC 3.3V;
• Consumo em Stand-By: 10-13mA / 3.3V;
• Consumo em Sleep: - Pico de corrente: <30mA;
• Frequência da operação: 13,56MHz;
• Tipos de cartões suportados: Mifare1 S50, S70 Mifare1, Mifare UltraLight, Mifare Pro, Mifare Desfire;

• Temperatura operacional: -20ºC a 80ºC;
• Temperatura de armazenamento: -40ºC a 85ºC;
• Taxa de transferência: 10 Mbit/s;
• Dimensões: 8,5 x 5,5 x 1,0cm;
• Peso: 21g.

Tabela 1 – Especificações do módulo RFID que é constituído pelas tags e pelo leitor RFID.

❖ VGA OV7670 CMOS SCBS Módulo de Câmara

Figura 5 - Módulo de Câmara VGA 640x480 com interface I2C

A câmara arduíno VGA, correspondente à Figura 5, trata-se de uma câmara digital baseada em OV7670 que possui a capacidade de tirar fotos ou fazer filmagens em conjunto com o Arduíno ou outro microcontrolador, com uma taxa de atualização de até 30 frames por segundo. A resolução máxima da câmara é de 640 x 480 pixéis. A Ladicha VGA OV7670 apresenta as seguintes características:

- Módulo Câmara OV7670 640x480 VGA CMOS SCCB para arduíno;
- Alta sensibilidade para a operação com pouca luz;

- Interface SCCB padrão compatível com a interface I2C; Raw RGB, RGB (GRB4:2:2, RGB565/555/444), YUV (4:02:02) e, YCbCr (04:02:02) formato de saída;
- Suporte VGA, CIF e de CIF a 40x30; Formato, método Pixel Vario para subamostragem; Autocontrolo de Imagem: AEC, AGC, AWB, ABF, ABLC;
- Controlo de Qualidade da Imagem: A saturação de cor, matiz, gama, nitidez e anti-blooming; ISP inclui redução de ruído e correção do ruído;
- Correção sombras Lens; Flicker 50/60Hz deteção automática; Cor de saturação com ajuste automático.

Especificações:

• Matriz fotossensível: 640 x 480;
• Tensão: 2.5V - 3.0V;
• Temperatura de operação: -30ºC to 70ºC;
• Potência de operação: 60mW/15fpsVGAYUV;
• Modo Sleep: Formato de Saída: YUV/YCbCr4: 2 2 RGB565/555/444 GRB4: 02:02 Raw RGB de Dados (8 dígitos);
• Tamanho da lente: 1/6";
• Ângulo de visão: 25 graus;
• Max frame Rate: 30fps VGA;
• Sensibilidade: 1,3 V / (Lux-sec);
• Signal to Noise Ratio: 46dB;
• DynamicRange: 52 dB; Modo de Browse: por linha;
• Exposição eletrónica: 1 - 510 linha;
• Cobertura Pixel: 3.6um x 3.6um.

Tabela 2 – Especificações do módulo da câmara OV7670

❖ ESP 8266 Módulo WiFi

Figura 5 Módulo WiFi - ESP8266-01

O módulo WiFi ESP 8266, cujo o modelo ESP-01 é o que está apresentado na Figura 6. É a peça chave de todo o projeto pois é ele que permite a conexão dos dados

captados pelos sensores e a base de dados para o armazenamento ou das informações do RFID ou até mesmo das imagens capturadas pelo módulo da câmara.

O ESP8266 é um chip. Um chip que revolucionou pelo seu baixo custo e rápida divulgação. O que mais chama a atenção é que ele possui WiFi possibilitando a conexão de diversos dispositivos a internet (ou rede local) como sensores, atuadores e etc.

O ESP8266-01, Figura 6, também conhecido como "Módulo WiFi", tem um potencial muito maior do que aparenta. Algumas das especificações são apresentadas de seguida:

CPU: 32bit RISC Tensilica Xtensa LX106, cuja frequência é 80/160 MHz.

RAM: 64 KB.

FLASH: QSPI Externo – de 512 KB até 4 MB.

WiFi: IEEE 802.11 – b/g/n.

Comparando diretamente com o Arduíno, o ESP8266 tem um poder de processamento maior, porem existem poucas GPIO's para usar nesta versão. Esta versão, conta apenas com 4 GPIO's para uso, sendo que dois são para comunicação Serial.

❖ Base de Dados em Tempo Real (Firebase)

O Servidor Web usado é o Firebase como é possível verificar na Figura 6, consiste numa base de dados em tempo real que se conecta através da API da Google e que irá receber pedidos de autentificação do arduíno Uno Rev.3 sempre que alguém passa a tag sob o módulo RFID. O servidor irá armazenar as permissões e as imagens obtidas pela câmara OV7670 caso a autorização não seja autorizada e enviará respostas para a aplicação Android com a fotografia no caso da permissão negada e os dados da pessoa, caso a permissão seja aceite.

O Firebase é uma plataforma de desenvolvimento mobile (e web) adquirida pela Google em 2014. Com foco em ser um back-end completo e de fácil usabilidade, esta ferramenta disponibiliza diversos serviços diferentes que auxiliam no desenvolvimento e gerenciamento de aplicativos.

Com o objetivo de poupar tempo e fornecer um aplicativo de alta qualidade, esta plataforma contém vários recursos para desenvolver código:

- **Cloud Messaging**: O Firebase Cloud Messaging – FCM permite a entrega/recebimento de mensagens e notificações entre as plataformas iOS, Android e Web. No nosso casso é usado para a comunicação com o android e receber os parâmetros.
- **Authentication**: Este recurso de autenticação é fundamental para as aplicações onde é necessário saber a identidade do usuário e manter o controle do acesso à aplicação.
- Realtime Database: O Firebase também disponibiliza um banco de dados NoSQL (Firebase Realtime Database) hospedado em nuvem, onde os dados

são armazenados como JSON e sincronizados em tempo real com todos os clientes conectados.

- Storage: Útil para armazenar arquivos como imagens capturadas pela câmara.
- Test Lab: O Firebase Test Lab fornece toda infraestrutura em nuvem que é preciso para testar a aplicação Android e mesmo que não tenha escrito o código de teste para a aplicação, o Test Lab pode operar aplicativo automaticamente procurando falhas. Todos os resultados do teste são disponibilizados no Firebase console.

Figura 6 – Servidor WEB

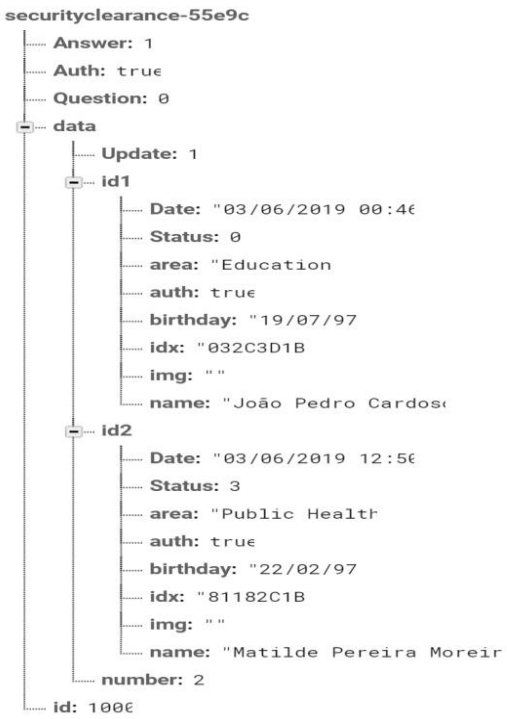


Figura 7 – Servidor Firebase com 2 tags identificadas com autorização de acesso

❖ Aplicação Android

A aplicação móvel android é desenvolvida em Android Studio e consiste num conjunto de vários ficheiros em que cada um representa uma atividade. Neste projeto serão usadas duas atividades que consideramos principais, uma é o ecrã inicial, em que haverá um botão "Conectar" e outra em que é possível controlar o acesso da pessoa e ver a stream imagem.

Ao pressionar-se o botão "Conectar", a aplicação envia um pedido ao servidor de forma a obter o IP do arduíno e conecta-se. Após o receber, para a atividade seguinte, na qual será apresentado a hipótese de a pessoa controlar o estado de acesso das pessoas com botões e verificar se a pessoa tem acesso ou não. Caso não tenha acesso, é enviada a fotografia da pessoa para a aplicação, caso contrário, os dados da pessoa serão enviados, nomeadamente o nome e os dados da pessoa que irão ser registados com auxílio da aplicação.

Na imagem seguinte é apresenta a ideia e layout para aplicação Android e que é usada no projeto. Relativamente à 2ª Atividade é possível verificar que houve comunicação entre o Firebase e a aplicação android, analisando, quer a figura 7, quer a figura 6.

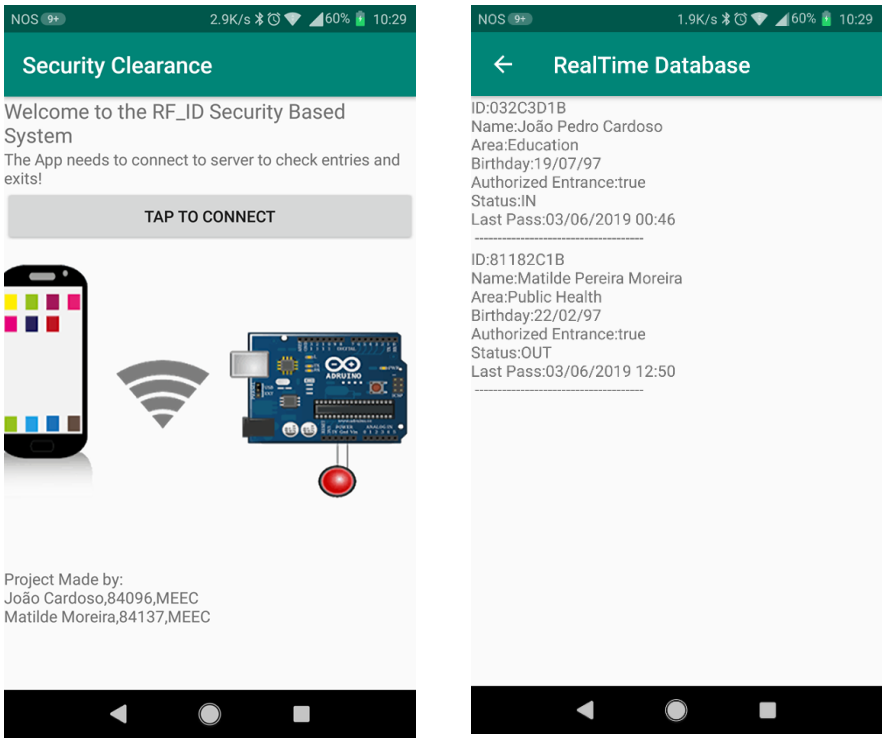


Figura 7 Layout inicial da aplicação android (1ª atividade- Esquerda, 2ª atividade- Direita)

ARQUITETURA DA SOLUÇÃO

Neste tópico é apresentado o diagrama de Fritzing da conexão dos três módulos (Leitor RFID, Módulo Wi-Fi ESP8266 e Câmara VGA 640x480) com o arduíno UNO Rev. 3, juntos (Figura 8) e considerando cada componente separado (Figura 9-11).

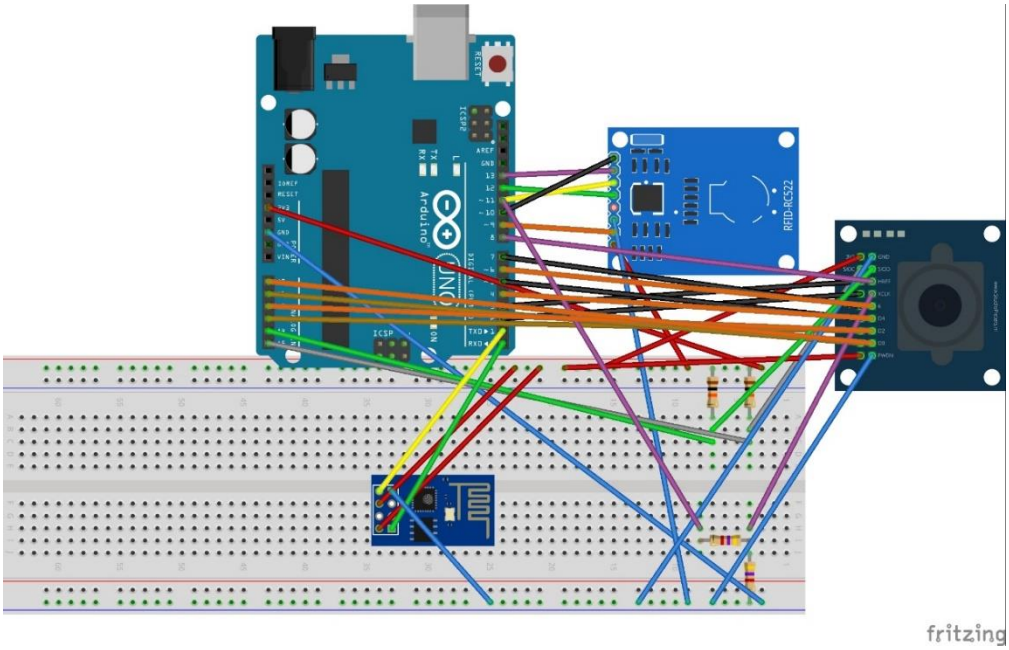


Figura 8 - Diagrama Fritzing dos módulos do sensor RFID, câmara, módulo WiFi ESP8266 e arduíno UNO Rev. 3

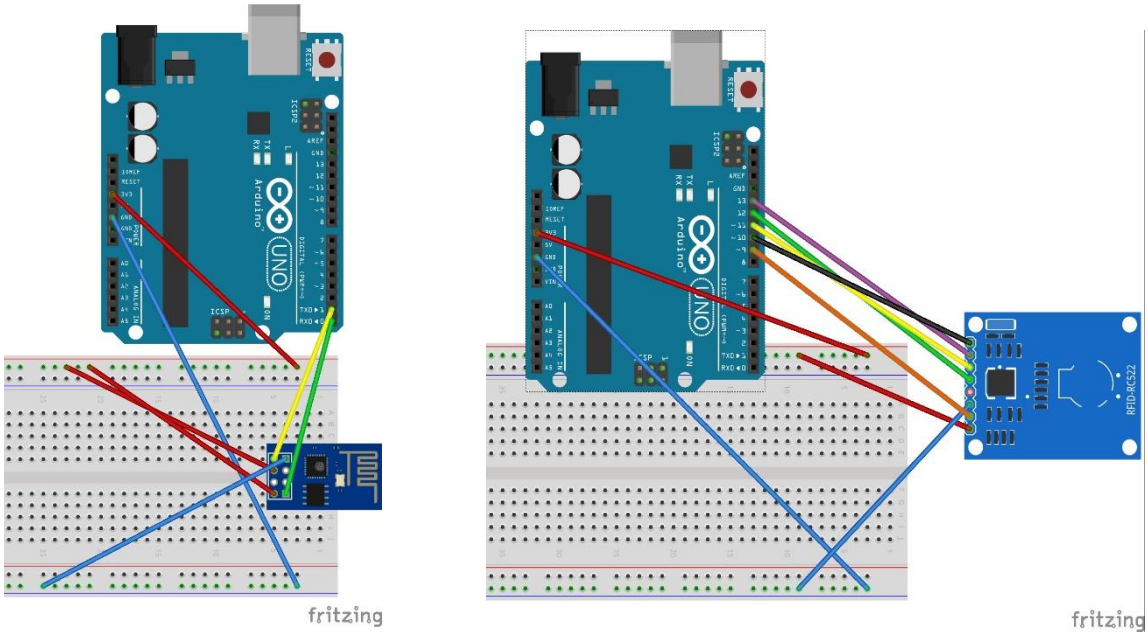


Figura 9 - Diagrama Fritzing dos módulos do sensor RFID (À direita) e módulo WiFi ESP8266 (À esquerda) e arduíno UNO Rev. 3

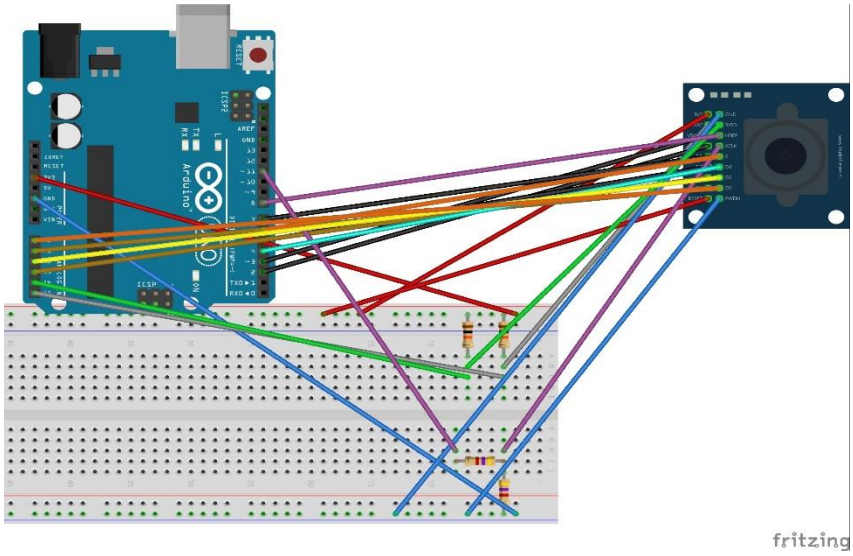


Figura 8 - Diagrama Fritizing do módulo da câmara OV7670 e arduíno UNO Rev. 3

DIFERENÇAS RELATIVAMENTE AO PROJETO INTERMÉDIO

No início do projeto tínhamos definido que iríamos usar um arduíno UNO WiFi Rev. 2 de forma a poder conectar os sensores simples (leitor RFID RC522) e complexo (câmara OV7670) diretamente ao servidor, sem ter de recorrer ao módulo Wi-Fi extra. No entanto, ao longo das nossas pesquisas verificámos que seria impossível a implementação desse arduíno devido à escassez de bibliotecas que conectassem os sensores ao arduíno. Isto levou a que tivéssemos de mudar para o arduíno UNO Rev..3 pois este tem as bibliotecas essenciais para a comunicação com os sensores.

Contudo tivemos de adicionar um módulo WiFi (ESP 8266- 01) ao arduíno para que este conseguisse comunicar com o Firebase.

Enquanto que não sentimos dificuldade em estabelecer as comunicações WiFi com o servidor recorrendo ao UNO WiFi, neste arduíno atual já sentimos bastante dificuldade não só pelo excesso de informação que existe na internet, como também muitos desses exemplos não são adaptáveis para o nosso caso.

Ao longo do projeto e devido à falta de informação sobre o módulo da câmara verificámos que este módulo também se iria tornar para nós um grande obstáculo. Pelo que tivemos de comprar uma outra câmara, devido à imagem captada estar desfocada. No entanto com a nova câmara e com a adição de 4 resistências, conseguimos resolver o problema.

CONCLUSÃO

Antes deste projeto, não tínhamos tido qualquer experiência na elaboração de sistemas de comunicação do tipo servidor, aplicação Android, arduíno e Wi-Fi, pelo que este projeto tem sido uma excelente oportunidade de aprendizagem e pesquisa sobre os componentes de hardware utilizados, assim como no desenvolvimento de software.

Relativamente ao ponto de situação do projeto e ao trabalho desenvolvido salienta-se os seguintes aspetos:

- O **Módulo de Leitor RFID** já se encontra concluído, isto é, já está montado ao arduíno com auxílio de uma breadboard e já temos o código de leitura do cartão com o arduíno implementado.
- O **Módulo da Câmara OV7670** já está montado ao arduíno. Consideramos esta parte o nosso maior desafio, devido à falta de informação sobre este módulo e da transmissão de imagem com o arduíno. Já captura fotografias.
- A **Aplicação móvel Android** está desenvolvida, também foi um desafio enorme, não pela dificuldade, mas pelo desconhecido, isto é, não tínhamos tido qualquer tipo de contacto com elaborações de aplicações via android.
- O **Servidor Web** já está quase pronta, faltando-nos comunicar com o Arduíno, já comunica com a aplicação

Organizações	Url	Contacto	Email	Contactado?	Informação Encontrada?
Prosegur	https://www.prosegur.pt/	707 22 23 22	[redacted]	Sim	Não
Securitas	https://www.securitasdirect.pt/	217155920	[redacted]	Sim	Não
Idonic	https://www.idonic.pt/	229428790 | 210131427	info@idonic.com	Não	Sim

Tabela 5 – Informações sobre as organizações analisadas e contactadas

BIBLIOGRAFIA / WEBGRAFIA

- Desafio Empreendedor IoT:
  →https://www.controlo-de-acessos.pt/leitores-biometricos-controlo-acessos-idonic-aeon-l202/
  →https://www.controlo-de-acessos.pt/terminal-control-acessos-idonic-aeon-109/

- Arduíno UNO Wi-Fi Rev.2:
  →https://store.arduino.cc/arduino-uno-wifi-rev2
  →https://pt.mouser.com/new/arduino/arduino-uno-wifi-rev2/
  →https://www.aibonline.org/aibOnline_/www.aibonline.org/newsletter/Magazine/Jul_Aug2013/Entry-Exit-Measures.pdf

- RFID:RC522 – Módulo Leitor de Cartões
  →https://books.google.pt/books?id=Gb6w54X7Kw0C&pg=PA164&dq=RFID&hl=ptzT&sa=X&ved=0ahUKEwiZo7P1uLzhAhV_BWMBHdPcBo0Q6AEIMjAB#v=onepage&q=RFID&f=false
  →https://github.com/miguelbalboa/rfid

- Ladicha VGA OV7670 CMOS – Módulo de Câmara
  → https://www.ptrobotics.com/cameras/3928-ov7670-camera-module.html
  →https://www.voti.nl/docs/OV7670.pdf
  → http://www.arducam.com/products/camera-breakout-board/0-3mp-ov7670/
  →https://www.instructables.com/id/OV7670-Arduino-Camera-Sensor-Module-Framecapture-T/

- ESP- 8266 – Módulo de WiFi
  →https://www.electrofun.pt/comunicacao/modulo-wifi-esp8266?utm_source=google&utm_medium=cpc&utm_campaign=1SearchDynamic&utm_term=Eletronica&gclid=CjwKCAjw583nBRBwEiwA7MKvoFZ4FOAv2jiHyzXwczX3GZDygy9Dbhk3xOgx4YHPsMX9dkmAvNrFRxoCU8wQAvD_BwE
  →https://www.filipeflop.com/blog/guia-do-usuario-do-esp8266/

- Aplicação Móvel Android

  → https://developer.android.com/guide/index.html

- Imagens

  → https://www.researchgate.net/figure/Access-control-techniques_fig5_224605168
  [Figura: capa]