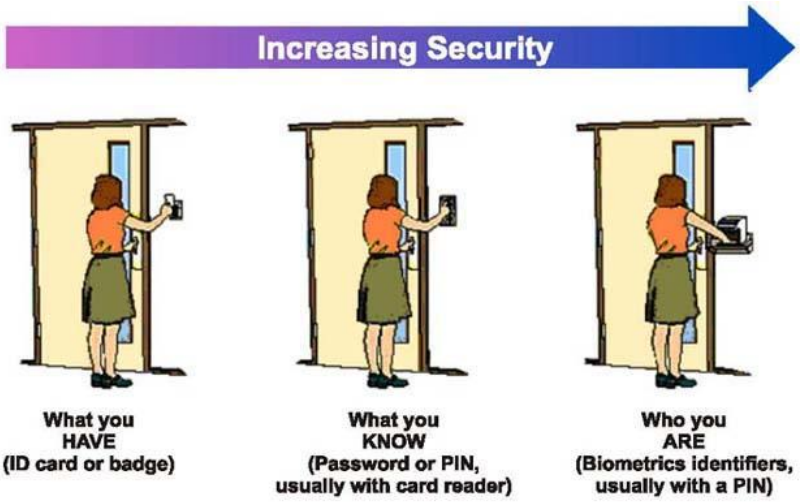
INSTITUTO SUPERIOR TÉCNICO

REDES MÓVEIS E SEM FIOS

PROJETO INTERMÉDIO

Controlo de entrada e saída de pessoas de instalações críticas



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 passível 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.

Os managers de tecnologia devem avaliar cuidadosamente as suas necessidades de segurança e determinar as medidas de segurança mais adequadas para as suas instalações, antes de investir nos equipamentos.

Neste projeto pretende-se implementar um sistema de controlo de entrada e saída de pessoas numa dada instalação, recorrendo 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 não tenha acesso para entrar na dada zona.

Neste relatório vários conteúdos irão ser abordados, tais como:

- **Definição do problema** – Áreas de Segurança: O que é preciso proteger?
- **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
- **Análise e especificação de requisitos de desempenho, através do feedback de algumas organizações contactadas**
- **Métodos de Identificação** – Dispositivos de controlo de acesso
- **Conclusão / Estado da implementação do projeto –** O que falta fazer e o que já está feito?

DEFINIÇÃO DO PROBLEMA

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 managers 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 inescrutáveis e até mesmo exóticas – *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.

Enquanto que os managers devem saber responder a estas duas perguntas, visto haver a necessidade de conhecerem as instalações de forma a poderem aumentarem a segurança, os consultores de sistemas de segurança não têm de saber os detalhes da instalação, embora tenham de conhecer as capacidades, custos e desvantagens das metodologias implementáveis. Combinando experiências de pessoas diferentes, o sistema pode ser projetado de forma a que os requisitos de acesso sejam válidos, a segurança seja máxima e os custos sejam os desejados.

Relativamente à definição de problema surge uma outra questão: **O que é que precisa de ser protegido?**

Um dos primeiros passos para delinear um plano de segurança é desenhar um mapa da instalação física e identificar as áreas e os pontos de entrada que precisam de diferentes **regras de acesso** ou **níveis de segurança**.

As áreas de segurança podem ter limites concêntricos: perímetro de construção, áreas de informática, balcões com equipamentos, ou limites lado a lado: escritórios, salas de serviço e áreas para visitantes. Em relação às áreas concêntricas, estas podem ter métodos de acesso diferentes umas das outras e até mais rigorosos, fornecendo proteção adicional designado por **profundidade de segurança**. Com profundidade de segurança, uma área interna é tanto protegida pelos seus métodos de acesso, quando pelas áreas que a delimitam.

No caso da figura 1. é possível verificar o que foi mencionado, isto é, cada prédio independentemente de acomodar empresas ou proprietários privados deve possuir sistemas de segurança para proteger bens valiosos. Esses sistemas de segurança física vão de simples controlo de acesso (portas, torniquetes), até sistemas de vigilância generalizados e diversos alarmes. Peça por peça, os sistemas de segurança estão on-line para permitir acesso mais rápido e um controlo mais fácil. Os edifícios inteligentes estão a ser construídos já com gerenciamento e monitoramento de segurança centralizada.

Maior conveniência e controle centralizado são vantagens de ter todos esses dispositivos acessíveis através da rede, mas também há riscos envolvidos. Eles se tornam suscetíveis a diferentes tipos de ataques de rede, e o recente incidente com os controladores de porta da HID prova que há uma possibilidade real de que vulnerabilidades nesses dispositivos possam ser exploradas.

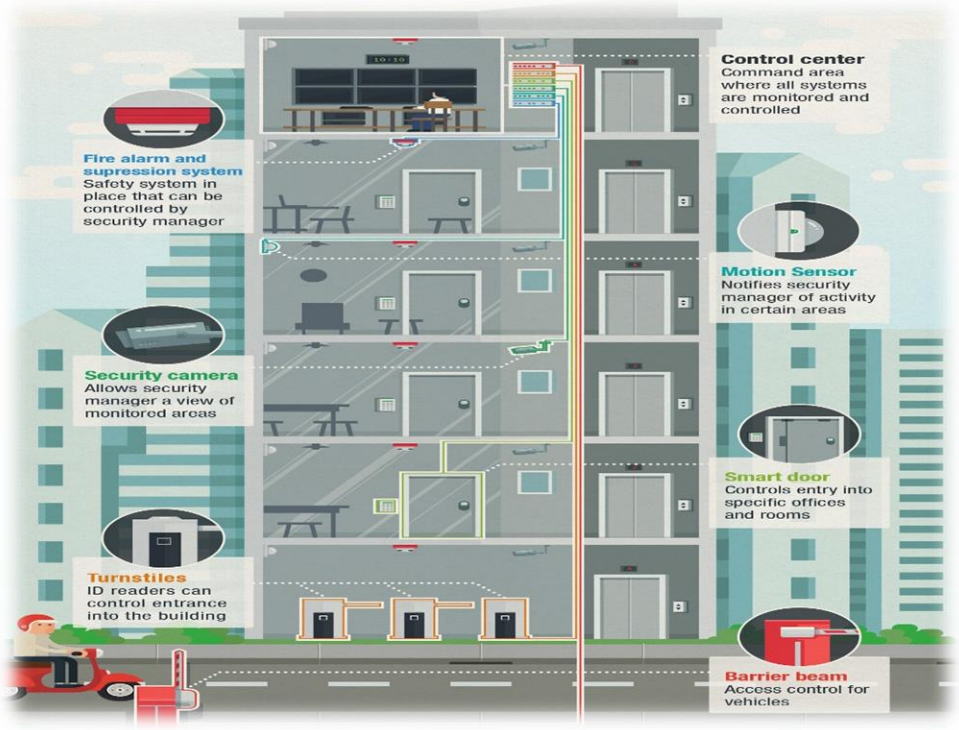


Figura 1- Edifício com controlo de entrada e saída de pessoas.

Na Figura 2 é apresentado um mapa de segurança de uma instalação crítica, abordando o conceito de profundidade de segurança. Nas zonas mais internas de profundidade de segurança (*Rack*) existem proteções contra o acesso não autorizado e de equipamentos que só devem de estar ao alcance de determinadas pessoas. O controlo de acesso pode ser configurado remotamente para permitir acesso apenas quando é necessário – a determinadas pessoas em períodos específicos – reduzindo riscos de acidente, sabotagem, extravio de dados.

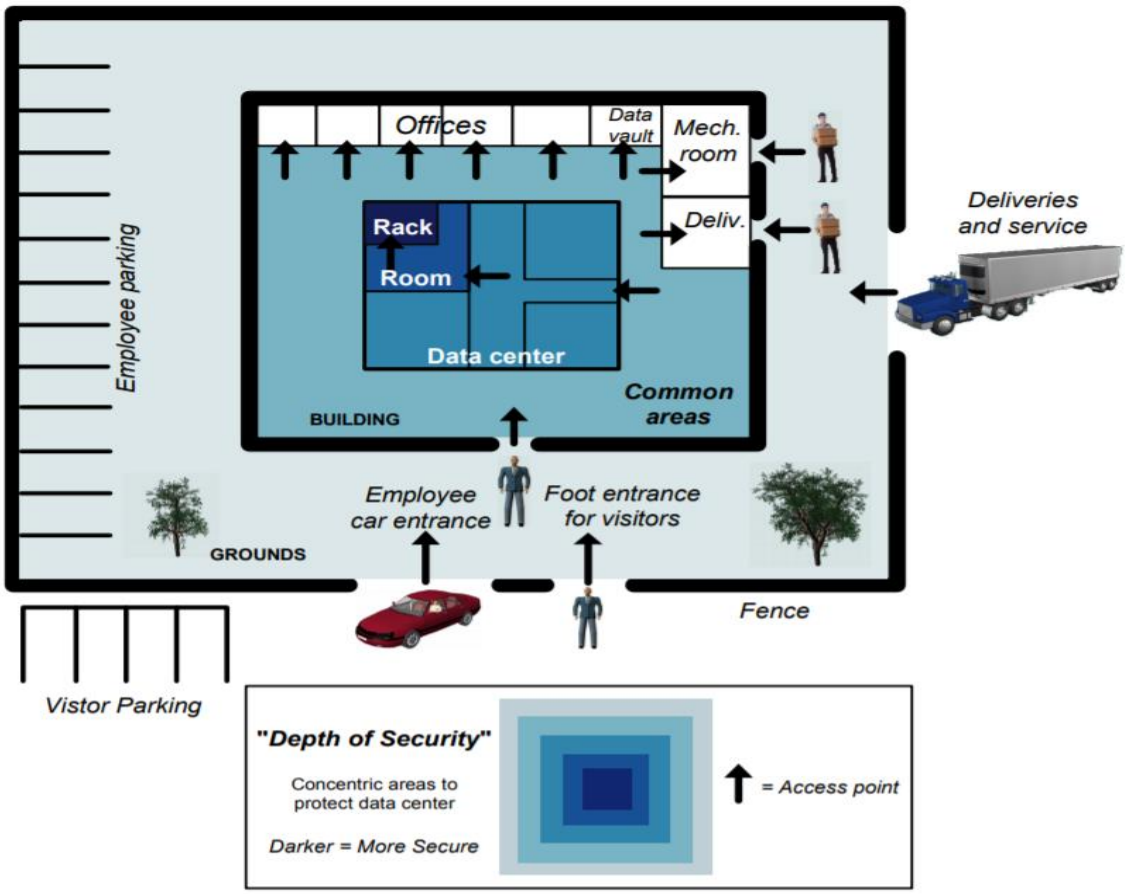


Figura 2 – Mapa de Segurança abordando o conceito de profundidade de segurança ("*Depth of Security*")

VISÃO GERAL

O projeto, Controlo de entrada de saída e entrada de pessoas em instalações críticas, implica a construção de vários componentes hardware e software:

- RFID - RC522 Módulo de Sensor de Cartão, que irá ser controlado pelo Arduíno UNO Wi-Fi Rev.2.
- Ladicha VGA OV7670 CMOS Módulo de Câmara, que se irá ligar ao arduíno.
- Servidor Web que irá servir como intermediário entre a aplicação e o arduíno em questão.
- Arduíno UNO Wi-Fi Rev.2 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 3 é apresentado um esquema geral do projeto e como os componentes se interligam entre si.

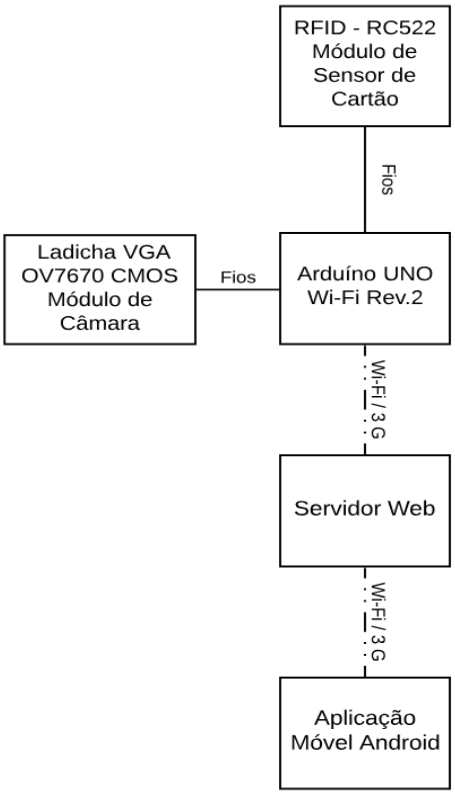


Figura 3 – Esquema geral do projeto a implementar

MÓDULOS

❖ Arduíno UNO Wi-Fi Rev.2

O arduíno Uno Wi-Fi Rev.2, que é apresentado na Figura 4, é um arduíno Uno com um módulo WiFi integrado. A placa é baseada no microchip ATMEGA4809 com um Módulo WiFi 802.11b /g /n NINA-W13 ESP32 u-blox integrado. O Módulo NINA-W13 é um SoC (System On Chip) autônomo com uma stack de protocolo TCP / IP integrada que pode fornecer acesso à rede Wi-Fi (ou o dispositivo pode atuar como um ponto de acesso). O arduíno Uno WiFi Rev2 é programado usando o Software arduíno (IDE).

O ATmega4809 oferece 6KB de RAM, 48KB de Flash, três UARTS, Core Independent Peripherals (CIPs) e um ADC de alta velocidade integrado. Combinado com o microchip ATECC608 CryptoAuthentication, o microcontrolador também fornece segurança baseada em hardware para conectar projetos a clouds, incluindo AWS e Google.

Figura 4 - Arduíno UNO Wi-Fi Rev.2

Este arduíno irá ser acoplado através de fios 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 5 é apresentado o esquema do arduíno com os módulos importantes que irão ser usados.

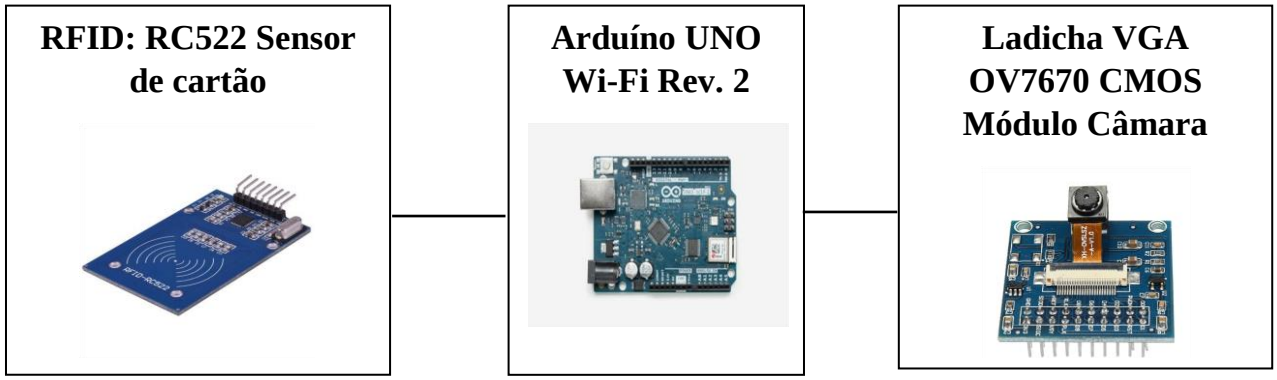


Figura 5 - Esquema do arduíno com os respetivos módulos a usar

❖ RFID: RC522 - Módulo de Sensor de Cartão

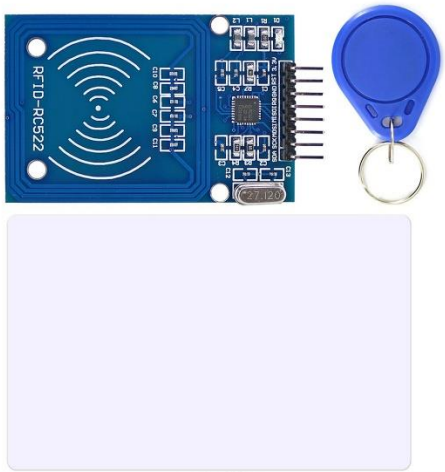


Figura 6 - Módulo RFID com as respetivas tags

O Módulo RFID, apresentado na Figura 6, 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.

❖ Ladicha VGA OV7670 CMOS Módulo de Câmara

Figura 7 - Módulo de Câmara VGA 640x480 com interface I2C

A câmara arduíno VGA, correspondente à Figura 7, 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

❖ Servidor Web

O servidor Web, como é possível verificar na Figura 8, consiste numa base de dados com um IP fixo, que irá receber atualizações periódicas Arduíno Uno Wi-Fi Rev.2 e da aplicação Android. 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.

Figura 8 – Servidor Web

❖ Aplicação Android

A aplicação móvel android está a ser 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 uma primeira ideia básica de layout para aplicação Android e que irá ser usada no projeto.

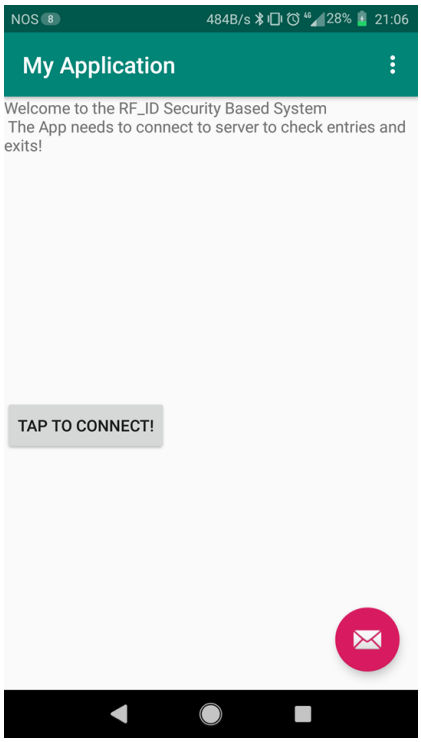


Figura 9 Layout inicial da aplicação android (1ª atividade)

ARQUITETURA DA SOLUÇÃO

Neste tópico irá ser apresentado o diagrama de Fritzing da conexão dos dois módulos (Leitor RFID e Câmara VGA 640x480) com o arduíno UNO Wi-Fi Rev. 2.

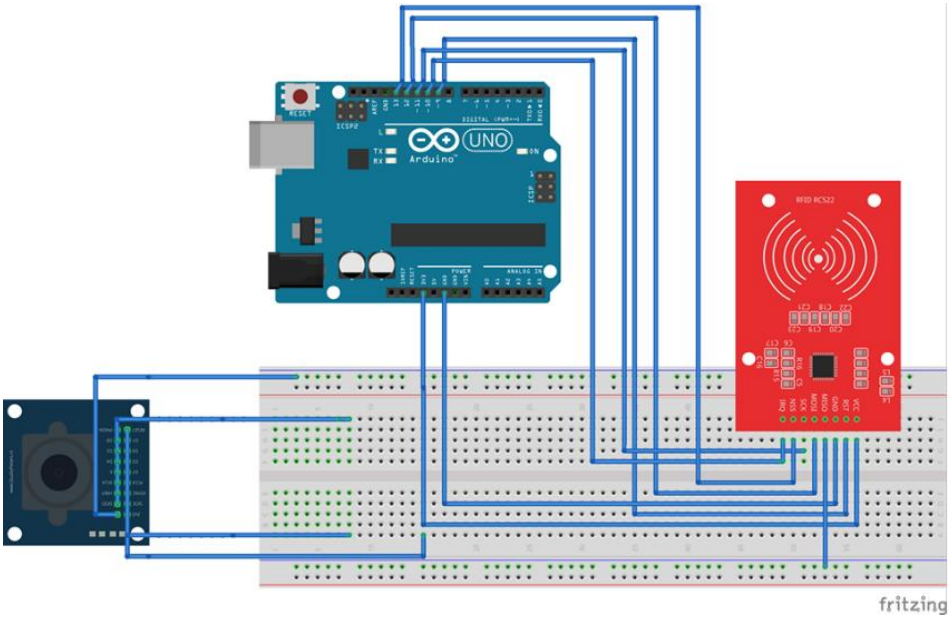


Figura 10 - Diagrama Fritizing dos módulos do sensor RFID, câmara e arduíno UNO Wi-Fi Ver. 2

DESAFIO EMPREENDEDOR IOT

Após tentarmos comunicar com algumas empresas, e não termos obtidos respostas às nossas perguntas via telefone ou email, como por exemplo: Prossegur ou Securitas, encontrámos na internet várias informações sobre diferentes estilos de sensores de RFID e especificações de leitores com informações sobre:

- distância máxima da leitura do cartão;
- tempo de verificação;
- tempo de registo;
- modo de verificação;
- tipo de comunicação;
- etc.

Contacto da Empresa IDONIC:

- E-mail: info@idonic.com
- Norte: 229 428 790 | Sul: 210 131 427

Leitores Biométricos de Controlo de Acessos IDONIC AEON L202 – Empresa IDONIC

"O IDONIC AEON L202 pertence à classe de leitores biométricos secundários com autenticação por leitura das impressões digitais e comunicação com recurso ao protocolo RS485. Tratando-se de leitores biométricos secundários, o seu funcionamento obriga à interligação com as placas controladoras de acessos. Tempo por forma de autenticação prioritária a Biometria, disponibiliza ainda como alternativa a esta, no caso de impossibilidade de registo das impressões digitais, **a leitura de cartões de acesso de tecnologia RFID (EM 125k, MIFARE ou HID).**

Figura 11 - IDONIC AEON L202

Com sua estrutura robusta e índice de proteção IP65, os leitores biométricos IDONIC AEON L202 estão preparados para funcionar no exterior, oferecendo uma maior durabilidade em todas as condições meteorológicas e ambientes agressivos. Ligando os leitores biométricos AEON L202 com o software de gestão de acessos Id Access, é possível registar todos os movimentos de acessos, estado de presença ou ausência dos utentes, tempo de permanência por zona, definição de perfis de acessos com restrições horárias e por zona, integração com controlo de assiduidade, gestão de acessos em modo anti-passaback, bloqueando passagens repetidas no mesmo sentido sem anterior passagem no sentido inverso."

Especificações Técnicas	
Distância leitura cartão	10cm
Tempo de leitura	1 seg. impressão digital; <300ms cartão
Impressão Digital	Sim
Reconhec. facial	Não
Cartão	RFID(opcional)
Impressora	Não
PinCode	Não
GPRS	Não
Wifi	Não
Tempo de registo	1 seg.
Tempo de verificação	1 seg.
Modo de verificação	1:1; 1:N
Comunicação	RS485
Câmara	Não
Voz	Não
Display	Não
Teclado	Não
Relé Alarme	Sim
Relé Porta	Sim
Alimentação	DC 12 V
Temperatura	0° a 50°C
Humidade	20% a 80%
Dimensões	102mmx50mmx37mm
Peso Bruto	0.12kg

Tabela 3 - Especificações Técnicas de um leitor biométrico - AEON L202

Terminal Controlo de Acessos IDONIC AEON 109 – Empresa IDONIC

Terminal com leitor de cartões RFID, desenhado para ligar a aplicação de controlo de acesso IdAccess. O IDONIC AEON 109 permite o controlo de acessos por cartão, tendo como alternativa a introdução de um código PIN, através de teclado digital, que surge no display. Está equipado com um ecrã touch de 3'', que permite programá-lo diretamente ou administrá-lo mediante com o software de controlo de acessos, comunicado através da sua interface de rede TCP/IP. Dispõe igualmente de porta USB como alternativa nos casos em que assume o funcionamento em modo stand-alone.

Na Tabela 4 é possível verificar as especificações técnicas deste leitor de cartões RFID.

Especificações Técnicas	
Capacidade Templates	30.000 RFID
Armazenamento/movimentos	Até 50.000
Impressão Digital	Não
Reconhec. facial	Não
Cartão	Sim
Impressora	Não
PinCode	Sim
GPRS	Não
Wifi	Não
Tempo de registo	<2 seg
Tempo de verificação	<1 seg
Modo de verificação	1:N
Comunicação	RS-232/485 e Ethernet
Câmara	Não
Voz	Sim
Display	Sim
Teclado	Sim
Relé Alarme	Não
Relé Porta	Sim
Alimentação	12V DC
Temperatura	0 °C a 50 °C
Humidade	20% a 80%
Dimensões	240mmx135mmx46mm
Peso Bruto	0.7kg
Controlo de Assiduidade	Não

Tabela 4 - Especificações Técnicas de um leitor RFID - AEON 109

MÉTODOS DE IDENTIFICAÇÃO

Nos dias de hoje, o mercado oferece diferentes opções para o controlo de acesso de pessoas. Para compreendermos quais as melhores formas para cada tipo de caso/negócio (seja empresa ou particular), é importante conhecer os diferentes métodos e as tecnologias disponíveis no mercado, que podem ser classificados em: Lógicos e Físicos.

CONTROLO DE ACESSO FÍSICO

- Este método de controlo é utilizado com o objetivo de vigiar o fluxo de pessoas num local, como edifícios comerciais e residenciais, salas, empresas, áreas internas e é normalmente controlado por um profissional.
- É constituído por uma barreira física (parede, muro ou cerca) e conta com um ou mais pontos de entrada, vigiados por meios eletrónicos (fechaduras, torniquetes, entre outros) ou mecânicos (cancelas, portões…).
- Apesar dos custos destes equipamentos serem inferiores aos de controlo de acesso lógico, requerem uma manutenção e compra constante, para além do treino e preparação de profissionais para administrar os equipamentos e as situações que possam vir a acontecer.

CONTROLO DE ACESSO LÓGICO

- O controlo de acesso lógico está dependente da tecnologia para controlar os locais e pode acontecer por meio de leitura biométrica, reconhecimento facial, de voz e íris, cartão mifare (RFID), entre outros.
- Para a pessoa poder aceder a locais, já tem de estar identificada no sistema/servidor, não sendo precisa uma pessoa para fazer a gestão do controlo de acessos.
- Este tipo de controlo é utilizado em espaços auto gerenciáveis, isto é, que funcionam sem ser necessário a gestão constante de um profissional.

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 a desenvolver salienta-se os seguintes aspetos:

- O **Módulo de Leitor RFID** já se encontra praticamente 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** ainda se encontra numa fase inicial, apesar de já termos o esquema de montagem 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. Conseguimos encontrar dados sobre uma outra câmara e estamos a tentar implementar nesta.
- A **Aplicação móvel Android** encontra-se em desenvolvimento, 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 em desenvolvimento, faltando-nos comunicar com o Arduíno e a aplicação, mas para terminarmos o servidor, queremos ter a aplicação concluída, para irmos testando.

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

Estado	Tarefas	Data de Início	Data de Conclusão
Feito	Levantamento de material para projeto	28/02/2019	08/03/2019
Feito	Divisão de Tarefas e Planeamento/ Estruturação do Projeto	01/03/2019	01/03/2019
Feito	Contactar as Organizações / Empresas	04/03/2019	15/04/2019
Feito	Estabelecer conexão do read carder com o arduíno usando breadboard	18/02/2019	19/02/2019
Feito	Programa em arduíno para comunicar com o RFID	02/03/2019	14/03/2019
Em desenvolvimento	Aplicação Android recorrendo ao Visual Studio	15/03/2019	Data prevista: 30/04/2019
Em desenvolvimento	Estabelecer conexão da câmara com o arduíno	15/03/2019	Comprar fios próprios e encontrar informações sobre a câmara
Em desenvolvimento	Servidor Web	20/03/2019	Data prevista: 03/05/2019
Por iniciar	Estabelecimento da conexão do arduíno com o servidor	05/05/2019 (*)	Data prevista: 15/05/2019
Por iniciar	Relatório Final	01/05/2019	02/06/2019
Por iniciar	Testar projeto	20/05/2019 (*)	02/06/2019

(*) se possível iniciar mais cedo

Tabela 6 – Planeamento das tarefas a concretizar para o projeto

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

- Ladicha VGA OV7670 CMOS – Módulo de Câmara
  →https://robokits.download/datasheets/OV7670.pdf
  →https://www.voti.nl/docs/OV7670.pdf

- Aplicação Móvel Android
  → https://developer.android.com/guide/index.html