



UNIVERSIDADE
LUSÓFONA

Fechadura Inteligente

Trabalho Final de curso

Relatório Final

Nome do Aluno: Gustavo Jorge, 21803634

Nome do Aluno: Tiago Pereira, 21803259

Nome do Orientador: Luís Gomes

Nome do Coorientador: Sérgio Ferreira

Trabalho Final de Curso | LEI | 17.07.2020

www.ulusofona.pt

Direitos de cópia

Fechadura Inteligente, Copyright de Gustavo Jorge e Tiago Pereira, ULHT.

A Escola de Comunicação, Arquitetura, Artes e Tecnologias da Informação (ECATI) e a Universidade Lusófona de Humanidades e Tecnologias (ULHT) têm o direito, perpétuo e sem limites geográficos, de arquivar e publicar esta dissertação através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, e de a divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

Índice

| | |
|--|----|
| Índices de Figuras | 4 |
| Resumo..... | 5 |
| Abstract | 6 |
| Identificação do Problema..... | 7 |
| Levantamento e Análise de Requisitos | 8 |
| Viabilidade e pertinência..... | 10 |
| Solução Desenvolvida..... | 11 |
| State of the Art..... | 14 |
| Benchmarking..... | 16 |
| Método e planeamento | 20 |
| Resultados | 21 |
| Conclusão e trabalhos futuros..... | 22 |
| Bibliografia..... | 23 |

Índices de Figuras

| | |
|--|----|
| Figura 1 - Fotografia do Modelo..... | 13 |
| Figura 2 - Fotografia do Circuito..... | 13 |
| Figura 3 - Exemplo da fechadura Yale Entr Kits..... | 17 |
| Figura 4 - Sistema instalado da fechadura inteligente HomeIt | 18 |

Resumo

Este relatório final constitui a elaboração e compreensão do trabalho – Fechadura Inteligente – que surge no âmbito da unidade curricular Trabalho Final de Curso da Licenciatura em Engenharia Informática da Universidade Lusófona de Humanidade e Tecnologias.

Com este relatório será possível compreender noções importantes sobre o trabalho, tais como, os cenários de aplicação, aplicabilidade do tema, possíveis evoluções, tecnologias associadas, comparação com outras soluções similares ou concorrentes.

Ainda é possível com este relatório aprofundar o resultado do desenvolvimento da fechadura, cuja implementação terá como base operar um microcomputador RaspberryPi que disponibiliza tecnologias como o GPIO (Linha de 40 pins I/O) e WebIOPi (controlador do GPIO disponibilizado para o RaspberryPi) que facilitam a implementação da fechadura. A fechadura terá acesso restrito por credenciais de utilizador, onde a gestão de acesso será administrada por uma página Web. O modo de acesso do utilizador para efetuar o destranque será feito manualmente através de um PIN fixo, de um PIN com auxílio de uma página Web ou através de uma App Mobile (QR Code).

Abstract

This final report consists in the preparation and the understanding of the work – Fechadura Inteligente – that comes within the scope of the course unit Trabalho Final de Curso of the Licenciatura em Engenharia Informática of the Universidade Lusófona de Humanidade e Tecnologias.

With this report it will be possible to understand important notions about the work such as, the application scenarios, applicability of the theme, possible evolutions, associated technologies, comparison with other similar solutions or solutions from another competitors.

It is still possible with this report to go deeper into the development result of the lock, which the implementation will be based on operating a RaspberryPi micro computer that offers technologies like GPIO (Set of 40 I/O pins) and WebIOPi (A controller for GPIO available for RaspberryPi), that facilitates the implementation of the lock. The lock will have access restricted by the user credentials, where the access management will be conducted by a web page. The user access mode to unlock will be conducted manually through a fixed PIN, through a PIN with the help of a web page or a Mobile App (QR Code).

Identificação do Problema

Com este trabalho pretende-se criar uma alternativa a fechaduras tradicionais que permita maior flexibilidade no controlo de entrada em espaços de acesso reservado, tirando proveito de novas tecnologias nomeadamente mobilidade e IoT.

Visto que, hoje em dia tentamos ser o mais seguros possível com os nossos smartphones e computadores, em nossos meios de transporte, nas ruas da cidade, etc.... E, principalmente, nas nossas casas. Neste último caso, a tecnologia envolvente neste trabalho ajuda bastante por meio de uma fechadura digital, sendo um produto útil para residências, escritórios, consultórios e estabelecimentos comerciais, entre outros.

Também residem vários problemas nas fechaduras mais tradicionais nos dias de hoje que são facilmente resolvidos através da solução proposta, tais como, por exemplo, a cópia de chaves em fechaduras mais tradicionais que podem causar problemas de assalto. Ao contrário destas a fechadura inteligente permite, se o utilizador quiser em situações mais domésticas, partilhar o seu PIN com outra pessoa para aceder ao local sem problemas. Outro problema mais recorrente seria a danificação das fechaduras por demasiada utilização ou por casos de humidade/temperatura ou até mesmo por situações mais imprevisíveis e inconvenientes como o “Deixei a chave do lado de dentro.”, que causaria transtorno pessoal ou até mesmo empresarial, levando ao próximo passo: chamar os bombeiros para abrir a porta.

Com respeito às várias soluções utilizadas hoje em dia, este trabalho proporciona uma solução bastante inteligente e prática, proporcionando ao utilizador uma forma de aceder a uma dada plataforma, cofre, quarto, etc.... através de 3 meios diferentes e complementares possíveis. Limitando-se a inserir o PIN registado no sistema, autenticar-se previamente através de uma página web para aceder ao seu código e ser-lhe concedido acesso no RPi ou por inserção de uma senha de segurança e por um PIN providenciado em QR Code gerado no RPi.

Em relação ao resultado do trabalho obtido, de um modo geral foram desenvolvidos todos os cenários referidos até um determinado ponto, sendo os maiores “issues” a base de dados que apenas foi criada, mas nunca devidamente utilizada e alguns dos mecanismos de funcionamento foram alterados face à explicação dos relatórios anteriores, como por exemplo, o caso da abertura da fechadura no terceiro cenário que será explicado mais à frente. As maiores diferenças serão explicadas com maior detalhe e análise nos próximos capítulos.

Levantamento e Análise de Requisitos

| Nome | Descrição | Estado |
|-------------|--|-------------------------|
| Requisito 1 | Implementação de uma fechadura tradicional através de um código. O RPi terá um ecrã, que permitirá a inserção de um PIN fixo para a abertura da fechadura, através de um teclado numérico. Caso o utilizador introduza o PIN corretamente, o RPi irá acionar a abertura pelo GPIO. | Implementado |
| Requisito 2 | Criação de uma interface gráfica de um Keypad, de modo a funcionar no ecrã embutido no RPi. Este Keypad irá proporcionar ao utilizador uma forma deste poder inserir os PINs/Senhas para desbloquear a fechadura, com um conjunto numérico de 0 a 9 e os botões entrar e cancelar, para validar a entrada do utilizador de modo a comparar os códigos introduzidos por este e cancelar a operação permitindo ao utilizador inserir o código novamente (incluindo um botão de voltar). O código de abertura é definido por acesso à página web e acedida mediante credenciais do utilizador. Através de um ficheiro Processing que irá conter o código, para o UI do Keypad da fechadura e as funções essenciais para introduzir os PINs/Senhas e estes serem validados, incluindo as bibliotecas e funcionalidades do GPIO para o funcionamento do Relay. Por último desenvolver o circuito físico do trabalho, com as ligações devidas entre o RPi e o Relay. | Implementado |
| Requisito 3 | Criação de uma página web própria com o auxílio da ferramenta WebIoPi para execução de comando em modo gráfico. Será desenvolvido a interface web sobre o WebIOPi de forma a aceitar identificação de utilizador (através do seu Username e Password), que após autenticado poderá abrir a porta, criando um mecanismo de forma a que vários utilizadores possam criar “contas” diferentes com credenciais diferentes para poderem aceder à fechadura. A página será otimizada para abrir em dispositivos móveis. Todos os acessos ficarão registados com utilizador e hora de acesso. | Não Implementado |
| Requisito 4 | A gestão da fechadura terá de ser realizada pela página web disponibilizada pelo RPi, ao contrário do cenário do PIN fixo, a página terá que efetuar gestão de utilizadores com credenciais individualizadas, ou seja, terá de se desenvolver a autenticação do utilizador mais a ligação à base de dados. | Não Implementado |
| Requisito 5 | O RPi (fechadura) terá de providenciar um QR Code, através do ecrã, que de seguida deverá ser lido por um sistema Android (chave). O QR Code será enviado de volta para o RPi que irá gerar e devolver um PIN ao utilizador do Android, finalmente o utilizador só precisará de inserir o PIN disponibilizado no ecrã do RPi para que o RPi acione a abertura da fechadura pelo GPIO. | Modificado/ Alterado |

Análise dos Requisitos: Quanto aos dois primeiros requisitos e ao quinto requisito estes foram implementados com sucesso como requisitado, com exceção da componente backend da base de dados, em que por exemplo casos que o utilizador necessite de aceder ao seu código através de um Login na sua conta. Referente ao quinto requisito este foi modificado pois inicialmente foi explicado nos relatórios anteriores, que no terceiro cenário seria suposto aparecer o QRCode no RPi e o dispositivo Android leria o código e deveria ser criado um mecanismo de forma a aparecer um código numérico no ecrã do RPi, mas por acharmos este mecanismo pouco seguro, pois proporciona a visibilidade a terceiros do código do utilizador, então foi criada a App Android de forma a aparecer o código no ecrã do dispositivo sempre que este aponte para o QRCode, de forma a contornar este problema. Quanto aos 4º e 5º requisitos apesar de estarem a vermelho, (como não implementados pois na nossa perspetiva não achamos que tenham atingido o mesmo nível de sucesso que outros feitos) foram criados de forma similar em relação ao pedido inicial através de uma página web construída em PHP que proporciona ao utilizador entrar na sua conta por um Login, através do seu nome de utilizador e password e aceder à janela consequente com a sua senha de segurança. Não conseguimos implementar a conexão com a base dados, com exceção da criação da mesma em MariaDB e criação da tabela do utilizador.

Viabilidade e pertinência

Existem inúmeros casos em este projeto poderia ser viável, como, por exemplo:

- Este trabalho lida com o acesso à fechadura, através de um sistema Mobile. Só com esta parte pode ser desenvolvido um sistema de validação de presenças dos alunos ao entrar na sala. O aluno através do telemóvel poder-se-ia registar previamente (antes da entrada na sala) na página web fornecida pelo RPi e assim que chegasse iria aceder, através de um QRCode associado ao aluno;
- Tal como o exemplo anterior, poderia ser usado no aluguer de veículos/meios de transporte (por exemplo: trotinetes e bicicletas elétricas ou até mesmo no futuro com carros autónomos), através do QRCode que iria redirecionar o utilizador para uma página onde irá efetuar os passos necessários para a utilização do veículo;
- Entradas em edifícios escolares, empresariais, áreas restritas em laboratórios, áreas residenciais, etc... através de validação de credenciais/PIN;
- Validação automática na porta de embarque dum aeroporto, permitindo maior rapidez e eficácia no serviço;
- No acesso a cofres bancários pessoais ou empresariais, no entanto, a segurança da fechadura pode não ser a mais fiável em comparação a outras soluções.

Este tema é bastante inovador e emergente, pois como foi visto nos exemplos de viabilidade anteriores este trabalho tem imensas possibilidades de evoluir e até mesmo no mercado futuro. No mundo em que a segurança hoje em dia é um dos temas mais discutido e de maior importância, qualquer projeto com base neste tema é de grande notoriedade.

Quanto à pertinência, este tema poderá ser incorporado, através de diferentes tecnologias/recursos disponíveis, como por exemplo, um meio de destranque recorrendo a um sensor de presença, ou seja, o RPi ou sistema semelhante que irá possuir um sensor capaz de ativar a fechadura sempre que captar a presença de um Chip/Telemóvel do utilizador dentro de um determinado raio. Ou até mesmo um leitor de impressões digitais ou oculares para permitir a ativação da fechadura.

Em introspeção não pensamos que neste momento a fechadura se encontre num estado que possa ser devidamente comparado, pois é um trabalho extenso que requer uma evolução gradual e aprofundada nas tecnologias referentes ao RPi, mas como começo alguns dos mecanismos implementados para a fechadura podem ser bem aplicados nas situações possíveis exemplares referidas acima, como a marcação de presença de alunos à entrada da sala pelo uso da funcionalidade da App produzida para a leitura de QRCode, em acessos de entradas em edifícios escolares, empresariais, áreas restritas em laboratórios, áreas residenciais e até mesmo para o acesso a cofres bancários pessoais ou empresariais por um PIN de acesso ou pelo mecanismo de QRCode como implementado para o cenário do código único do trabalho e para o cenário de abertura por App Android respetivamente.

Solução Desenvolvida

Foi desenvolvida uma interface gráfica de um Keypad através do Processing em linguagem Java, que contem o UI e a lógica de funcionamento de modo a funcionar no ecrã embutido no RPi. Tal como foi explicado no levantamento de requisitos o Keypad irá proporcionar ao utilizador uma forma deste poder inserir o PIN, a senha de verificação o código providenciado pelo QRCode para desbloquear a fechadura, ambas as subinterfaces têm um conjunto numérico de 0 a 9 e os botões entrar, cancelar, voltar. Inicialmente o utilizador tem duas escolhas, primeiro este pode escolher a opção de código tradicional onde irá encontrar um campo para preencher o PIN, cujo título do campo é “Introduza Aqui o Código”, por efeitos de segurança à medida que o utilizador insere o PIN este é mascarado no ecrã onde o Utilizador só poderá visualizar uma sequência de símbolos “*”.

Quanto à segunda opção, o utilizador poderá fazer o desbloqueamento da fechadura por um QRCode, mas por razões de segurança, este terá de inserir uma senha de segurança que o utilizador tem associado na sua conta antes de aceder à janela do QRCode (caso o utilizador não chegue a esta janela, só poderemos prever que este não é um utilizador com acesso autorizado), quanto à janela do QRCode esta providencia ao utilizador aleatoriamente um de quatro códigos para o utilizador visualizar com a App Android criada, claramente que existe uma quebra enorme de segurança pois qualquer pessoa com uma câmara especial ou um leitor de QRCodes tradicional embutidos nos seus telemóveis poderão aceder ao código, por isso o utilizador tem de passar pela janela de verificação primeiramente e os QRCodes são expostos aleatoriamente para simular o código de acesso valido no momento.

Também foram adicionadas as bibliotecas e funcionalidades do GPIO para o funcionamento do Relay. Sempre que o PIN ou código do QRCode se encontram corretos o Relay (que funciona como uma fechadura funcional/real) será acionado para abrir, emitindo uma luz e um som na abertura, e voltará a fechar 10 segundos depois da abertura, tempo suficiente para o utilizador “entrar”.

Consequentemente foi necessário a montagem de um circuito físico do modelo deste trabalho, com as ligações devidas entre o RPi e o Relay. Sendo que este modelo não se encontra totalmente completo, pois falta a ligação a uma fechadura funcional, porque é logisticamente muito complicado integrar a solução com hardware apropriado.

Inicialmente, foi proposto pelo orientador, para efeitos de demonstração implementar à solução final a ligação a uma lâmpada ao circuito do RPi em vez do Relay, para demonstrar a abertura e fecho da fechadura, mas a pandemia impossibilitou que se utilizasse o laboratório de eletrónica da ULHT para montar a demonstração.

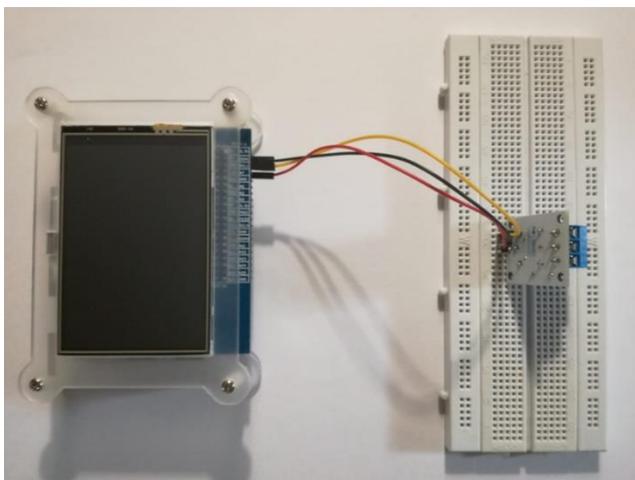
Quanto à página web de acesso ao utilizador, foi construída em PHP com auxílio da ferramenta PHPStorm, onde o utilizador terá acesso à sua senha de acesso consoante o Login à sua conta pela introdução do seu nome de utilizador e password, no entanto como não está realizada a conexão à base de dados a solução não permite múltiplos utilizadores.

Por último, foi criada uma aplicação Android para a leitura do QRCode multilinguagem (Português/Inglês) com auxílio da ferramenta Android Studio, em linguagem Kotlin; Apesar de inicialmente ter se referido nos relatórios anteriores que seria desenvolvida em linguagem Java decidimos alterar a linguagem para Kotlin com o único intuito de poder praticar esta linguagem que nos últimos anos tem vindo a ter mais impacto no mercado e por termos aperfeiçoado o nosso conhecimento desta linguagem ao longo deste semestre.

Esta aplicação de nome “TFC” inicializa com um Splash Screen de 2 segundos com o título de “Fechadura Inteligente” que de seguida irá direcionar o utilizador para a página de Login, este poderá efetuar o acesso através do seu nome de utilizador e password, (como referido anteriormente, como na página web, a conexão entre a App e a base de dados não foi realizada por isso a solução não permite múltiplos utilizadores).

Em caso das credenciais introduzidas não forem as corretas o utilizador será avisado através de um Pop-up (AlertDialog) que introduziu as credenciais erradas, caso contrário o utilizador será direcionado para uma página de informação sobre a leitura do QRCode e através do botão “Leia o Qr Code” o utilizador será direcionado para janela onde poderá ler através da câmara do seu dispositivo Android o QRCode exposto no ecrã do RPi e o código numérico embutido no QRCode irá aparecer no ecrã do dispositivo Android, que o utilizador só terá de introduzir para abrir a fechadura.

Fotografia do Circuito Físico:



| Materiais |
|---|
| - Raspberry Pi 3B+; |
| - Teclado/Rato/Monitor; |
| - Relay (VMA406); |
| - Breadboard; |
| - 3 Fios de Conexão (Jumper Cables Male to Female); |
| - Carregador |

Figura 1 - Fotografia do Modelo

Fotografia do Circuito:

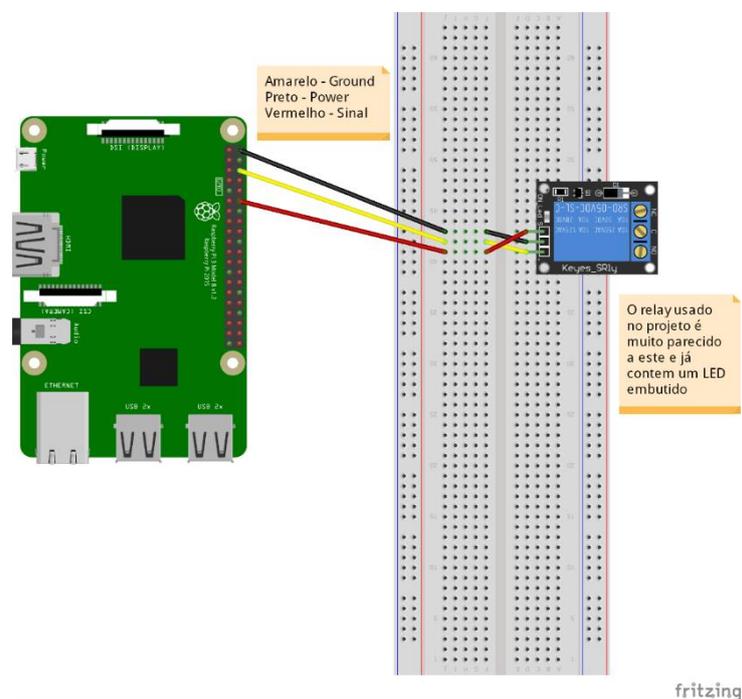


Figura 2 - Fotografia do Circuito

State of the Art

Quanto à tecnologia usada neste trabalho podemos referir que este contempla várias tecnologias de ponta bastante uteis, como por exemplo, o **Raspberry Pi**, peça chave no nosso trabalho, que é útil hoje em dia para tarefas computacionais como, por exemplo, a de um web server, extensor de wi-fi, um emulador de jogos, como “cérebro” de um carro robot, ou até mesmo usado para funções mais triviais, como por exemplo, um dispositivo de armazenamento ou pesquisa em internet, o que provavelmente novas versões no futuro poderão ser ainda mais poderosas em termos de funcionalidades, visto que a última versão deste produto RaspberryPi 4 possibilita fazer tarefas, que pensávamos que seriam só possíveis em computadores com maior capacidade computacional, como por exemplo, edição de vídeo e edição de imagem. A **Leitura de um QR Code**, que são bastante conhecidos atualmente e podem ser usados de diversas formas e feitos desde experiências/passatempos, cupões de desconto, informação de produtos em uma determinada loja, a pagamentos de passeios de Scooters eletrónicas pela cidade.

É usada a **Tecnologia Android**, tecnologia open source, ótima para o desenvolvimento de aplicações móveis e sendo o sistema mais popular entre fabricantes de smartphones o que torna a sua presença no mercado ainda mais rica em termos de hardware, existe liberdade na personalização da interface do sistema e compatibilidade com smartphones mais baratos. Também integra a **Linguagem Kotlin**, sendo esta uma linguagem de programação multiplataforma, orientada a objetos e funcional desenvolvida pela Google como linguagem oficial do sistema Android e projetada para ter uma interoperabilidade total com a linguagem Java, agilizando assim a sua adoção no mercado. Existem já algumas empresas que adotaram esta linguagem, sendo alguns dos exemplos as seguintes empresas: de acordo com o site da Kotlin, a Prezi já usa o Kotlin no seu backend e de acordo com o blog da JetBrains, o Kotlin é usado pela Amazon Web Services, Coursera, Netflix, Uber, Trello, Basecamp, entre outras.

Segundo a Google, esta linguagem já foi adotada por vários grandes desenvolvedores, como Expedia, Flipboard, Pinterest, Square entre outros, nas suas aplicações de produção para Android.

Entre outras tecnologias, que conjugadas entre si proporcionam uma solução para o nosso problema diferente e mais eficaz.

Também pode incorporar **IoT (Internet of Things)** que está cada vez mais presente no nosso cotidiano. Com a proposta de interligar coisas tornando-as inteligentes, através de recursos que estão a revolucionar o mercado de dispositivos inteligentes. Sendo um destes recursos a **WebIOPi** que é uma excelente interface web gratuita para o RPi, que pode ser usada em diversos projetos que tenham como base este microcomputador (que apesar de ter sido referida em relatórios anteriores para o desenvolvimento desta solução, não foi implementada neste trabalho), que possibilita no final do seu setup um servidor HTTP pronto a ser executado, disponível para acesso através de um navegador, com uma página web padrão onde o desenvolvedor poderá controlar todas as GPIOs do Raspberry Pi. Outro recurso IoT que pode muito bem ser usado neste trabalho é **Eclipse Kura**, framework que faz parte do projeto Eclipse IoT que visa criar soluções open source para facilitar o desenvolvimento IoT. O framework é composto por serviços Java e OSGi que são normalmente utilizados no desenvolvimento de aplicações IoT como serviços de Entrada/Saída, arquivos, conteúdo remoto e de rede. O Eclipse Kura propõe uma fácil criação de gateways que permitem gerenciar diversos dispositivos simultaneamente. A proposta deste gateway é fazer uma ponte entre os hardwares, que são os sensores e atuadores, com os dados de todos os dispositivos apresentados e processados.

Também existem diferentes tecnologias possíveis para o aperfeiçoamento e evolução deste projeto, como um **Leitor de Cartões** utilizado para cartões de memória, multibanco, de cidadão etc...., que pode ter as suas desvantagens como o funcionamento indevido, falta de atualizações, software maligno, ou por simples encrave do cartão, mas poderia ser adiciona ao RPi como mais um nível de segurança. **Tecnologia RFID** (Identificação por Radio Frequência) que hoje em dia muito utilizada, por exemplo em inventários em lojas e armazéns nos quais as mercadorias são etiquetadas com RFID, onde os leitores de dados podem localizar em poucos minutos todos os itens e fazer o levantamento dos mesmos com máxima assertividade, pode ter as suas desvantagens tais como o custo e a sua sensibilidade a interferências, mas seria outra solução possível para além da leitura por QR Code,.

Existem também outras soluções mais modernas como a **Biometria** bastante popular na identificação e a autenticação de um utilizador, uma vez que é efetuada logo na leitura da impressão digital na plataforma/sistema. O mesmo acontece com a leitura dos olhos e das características faciais, ou com a identificação da voz. Mas, na realidade, estes podem ser enganados com alguma facilidade, pois para um sistema deste género é muito difícil distinguir entre um dedo verdadeiro e uma réplica artificial bem feita do mesmo. Também existe o caso de estarmos constantemente a deixar impressões digitais nos mais diversos locais (copos, portas, mesas, etc.) que eventualmente podem vir a ser utilizadas para criar duplicações destinadas a enganar o sistema de leitura, mas apesar dos problemas óbvios também seria útil como mais um nível de segurança adicional neste trabalho.

Tecnologia Beacon, muito parecida à leitura por QR Code, é uma forma fantástica, rápida e eficaz de proporcionar uma experiência com aplicações nativas. Depois de chegar ao alcance de um beacon (farol), ele pode acionar uma notificação no smartphone e ativar a aplicação compatível. Este sistema está a começar a ser cada vez mais popular e é utilizado, por exemplo, por várias lojas de retalho para análise de passos / trilha de clientes, mapas de calor das zonas das lojas, análise de eficácia do merchandising e tipo de conteúdo que compele um cliente a comprar um certo produto, lealdade do cliente.

E tecnologia **NFC** (Comunicação por Proximidade), também muito parecido à leitura de QR Codes, NFC não requer nenhum ecrã para ser lido e maioria dos telemóveis mais recentes já apresentam nativamente esta funcionalidade. Utilizações mais populares são as de pagamento “contactless”, onde o utilizador apresenta meios desde cartões de crédito/débito até porta-chaves (ou até mesmo anéis), ou mesmo pagamentos através do telemóvel (como o Apple Pay ou Google Pay, por exemplo), o NFC permite realizar pagamentos rápidos encostando simplesmente um dispositivo com NFC ao terminal.

Dentro destas tecnologias acima referidas seria possível adicioná-las para evoluir e aumentar a complexidade da segurança base deste projeto, dado que o objetivo do trabalho é garantir uma forma eficaz, de confiança e diferente das fechaduras tradicionais e modernas no mercado.

Benchmarking

Neste tópico será demonstrado alguns casos no mercado atual e será efetuada a análise da solução final face à concorrência identificada.

Tecnologias Concorrentes:

- **Fechadura comum:**

Como sabemos uma fechadura comum é capaz da abertura/fecho de uma porta através do uso de uma chave.

Mesmo sendo este o tipo de fechadura mais usado atualmente apresenta várias falhas, tais como:

- Pouca interatividade, ou seja, não dá opções no tipo de abertura de uma porta;
- Pouca segurança, podendo a chave em questão ser replicada e usada para destrancar a porta por outrem;
- Pouco prático, pois no mundo em que vivemos cada vez mais é salientado o aspeto prático dos instrumentos a que temos acesso no nosso dia-a-dia, e o uso de uma fechadura tradicional é tudo menos prático e rápido.

Tendo em conta estes aspetos, à primeira vista a nossa fechadura inteligente apresenta pelo menos 2 métodos diferentes de abertura de uma fechadura (maior interatividade), assim como, uma proteção elevada devida à necessidade da inserção de um PIN ou através da leitura de um QRCode.

Por último, este trabalho encontra-se mais perto dos padrões tecnológicos desejáveis, sendo a única desvantagem mais óbvia, o custo mais elevado pelo tipo de tecnologia (RPi, fechadura customizada, ecrã, custo de implementação, etc...) embutido.

- **Fechadura digital não inteligente (Fechadura de único PIN):**

Neste caso, comparamos um tipo de fechadura um pouco mais avançada, em que o seu uso apresenta mais vantagens de segurança em relação à fechadura comum, garantindo a necessidade do uso de um PIN digitalmente.

Mesmo assim, este não apresenta grandes avanços em termos de interatividade ou opções, limitando o acesso do utilizador com apenas um PIN.

Em contrapartida, a fechadura inteligente além de permitir a abertura da fechadura através de PIN e através de um sistema de QR Code que devolve um código ao utilizador.

Economicamente, a fechadura inteligente trabalhada possivelmente será mais dispendiosa que esta opção, mas em alguns casos até a fechadura inteligente poderá ser a opção mais barata dependendo dos materiais utilizados na construção da fechadura digital não inteligente.

- **Fechaduras digitais inteligentes (Vendidas atualmente):**

Existem múltiplos tipos de fechaduras inteligentes no mercado atual, cada uma com várias interações e tecnologias diferentes, mas de forma a não tornar esta lista muito extensiva iremos apresentar apenas 2 modelos de fechaduras a serem comparadas com modelo trabalhado.

Yale Entr: [8][10]

Custo - 508,00€ (com instalação)

A Yale Entr é uma fechadura inteligente que permite fazer o controlo da porta através de várias formas: smartphone, comando à distância, impressões digitais ou ecrã tátil. A instalação desta fechadura inteligente requer modificar a fechadura ou canhão.

A Entr não possibilita fazer uma gestão remota e permite guardar apenas 20 códigos de acesso.



Figura 3 - Exemplo da fechadura Yale Entr Kits

HomeIt: [9][10]

Custo - 399,99€

A fechadura inteligente da HomeIt inclui teclado não digital.

O seu software é simples e intuitivo, permitindo a gestão de 500 códigos de acesso. O pacote inclui uma componente Nuki “plug-n-play” a ser montada na fechadura, ou seja, permite-lhe fazer a instalação em menos de 3 minutos e sem necessidade de trocar a existente, bastando montar o dispositivo em cima da fechadura atual (ver site da referência [10]).

A HomeIt tem a capacidade de abrir a porta de entrada de um edifício ou apartamento, através de uma ligação ao intercomunicador da casa. Também inclui ligação wi-fi, ou seja, permite gerir os acessos remotamente.



Figura 4 - Sistema instalado da fechadura inteligente HomeIt

Solução final face à concorrência identificada:

Como foi dito no capítulo da *viabilidade e pertinência* não é possível fazer uma comparação justa neste momento entre algumas das fechaduras apresentadas acima e a fechadura trabalhada pois esta última não se encontra completamente concluída, apenas podemos compor algumas análises óbvias ao modelo deste projeto como por exemplo este incorporar um RPi com capacidade de controlo de pelo menos uma porta, sendo o limite máximo o controlo total de 10 portas entre outros componentes controláveis, através do GPIO. Adicionalmente, o RPi como um mini computador pode fazer muito mais do que abrir uma fechadura, sendo alguns dos exemplos possíveis, o Login de aberturas com identificação de utilizador (controlo de credenciais) como é o caso neste trabalho; comando para a abertura e fecho à distância de motores de portas ou até mesmo uma abertura programável (por exemplo, para efeitos de casos de emergência); sensores de passagem/proximidade por NFC (uma tecnologia que permite comunicação sem fios e de forma segura entre dispositivos que estejam próximos um do outro), incorporação de sinalética ou alarmística, adição de câmaras ou de biometria, etc.

Outro aspeto importante a ter em conta é o custo de hardware total deste projeto que poderá rondar um custo máximo de 100€, sem contar com o custo de produção e manutenção. E tendo em conta o nível de segurança desejado, os custos também poderão ser mais elevados. Considerando as tecnologias concorrentes mais sofisticadas apresentadas acima uma das maiores vantagens que a fechadura implementada tem em comparação a estas será o seu baixo custo.

A questão da segurança também é outro tópico de extrema relevância, pois comparando às fechaduras concorrentes mais sofisticadas anteriormente referidas, os mecanismos realizados neste projeto não podem ser considerados particularmente seguros, pois por exemplo, a falta de conexão à base de dados irá provocar a falta de privacidade aos utilizadores, ou seja, na salvaguarda das suas credenciais. Outro exemplo seria o acesso de entidades maliciosas exteriores ao RPi, pois este poderá não ter uma caixa protetora ou uma personalizada o suficiente para proteger toda a configuração da fechadura.

Concluindo, comparando com as soluções concorrentes referidas acima, a solução proposta pode ser superior à fechadura comum, mas em comparação às soluções concorrentes mais sofisticadas será considerada inferior, devido ao software e hardware complexo da concorrência.

No entanto, não quer dizer que o sistema da fechadura inteligente seja uma má opção, pois apresenta opções de acesso diferentes e em termos financeiros e técnicos seria uma opção acessível em comparação às mais complexas e dispendiosas.

Método e planeamento

Em relação à calendarização definida nos relatórios anteriores podemos afirmar que não foi estritamente cumprida da forma esperada, mas tentamos ao máximo implementar os requisitos conforme os nossos conhecimentos até ao tempo limite. Apesar da entrega não ter sido completamente realizada por termos encontrado vários obstáculos, sendo alguns deles a conexão à base de dados e a aplicação de conceitos não abordados no curso - Electrónica, Robótica, etc. - para o funcionamento devido do RPi, achamos que foram desenvolvidos os requisitos essenciais para o desempenho da fechadura através do mesmo e por meio de pesquisa e dos diferentes trabalhos de outras cadeira fomos adaptando o trabalho de forma a implementar os pedidos iniciais.

Resultados

Num modo geral, deparámo-nos com dificuldades com a conexão da base de dados ao trabalho em todos os requisitos necessários o que significa que algumas das particularidades do funcionamento inicialmente definidas não foram concretizadas, como a utilização de múltiplos utilizadores com credenciais diferentes. Apenas conseguimos implementar a base de dados em MariaDB e a criação da tabela do utilizador, mas nunca a conexão ao trabalho num todo.

Como foi explicado no segundo capítulo o quinto requisito foi modificado por acharmos este mecanismo pouco seguro, pois proporciona a terceiros verem o código do utilizador no ecrã, por essa razão foi criada a aplicação Android de forma a aparecer o código no ecrã do dispositivo Android sempre que este aponte para o QR Code. Também foi criado de forma similar em relação ao pedido inicial uma página web construída em PHP que proporciona ao utilizador entrar pela mesma através de um Login, com o seu nome de utilizador e password e consequentemente aceder à janela com o código de segurança.

No entanto, apesar das adversidades que encontramos, foi criada a interface gráfica do Keypad, que contem o UI e a lógica de funcionamento da fechadura, de modo a trabalhar no ecrã do RPi, e o utilizador poder inserir a senha de verificação e o código providenciado pelo QRCode.

Também foi criada a App Android para a leitura do QRCode em linguagem Kotlin. Em linguagem Kotlin como explicado no quarto capítulo da *Solução Desenvolvida*.

A aplicação permite ao utilizador entrar pela sua conta e caso seja um utilizador autenticado poderá aceder às janelas seguintes onde este poderá ler o código do QRCode disponibilizado no ecrã do RPi.

Conclusão e trabalhos futuros

Com este trabalho concluímos que nos permitiu aprender mais sobre algumas das tecnologias referidas neste trabalho e aperfeiçoar competências já adquiridas ao longo da licenciatura como por exemplo, o dispositivo físico RPi e os seus possíveis componentes que ajudam a este mini computador comportar-se de forma dependente e ter capacidade de implementar sistemas com um propósito específico e necessário do utilizador e a tecnologia Android que é uma competência descoberta este semestre através da cadeira de Computação Móvel que podemos usar e aperfeiçoar neste trabalho para desenvolver a aplicação Android.

Apesar de não termos sido bem sucedidos a implementar as funcionalidades relativas à base de dados e a componente Web, achamos que aprendemos maioritariamente mais sobre esta área através de pesquisa web e referências a outros projetos de outras cadeiras.

Em relação à possível evolução deste trabalho, caso venha a haver outros alunos que assumam a continuidade deste projeto, aconselhamos a começarem pela implementação da base dados adequados ao funcionamento dos requisitos e a devida conexão da mesma a este trabalho. Sendo esta a maior desvantagem pois não proporciona a capacidade de obter múltiplos utilizadores e consequentemente a autenticação própria dos mesmos.

Em conclusão, independentemente dos obstáculos encontrados, de um modo geral, pensamos que o conhecimento adquirido ao longo do desenvolvimento deste trabalho deu uma ajuda para o início da nossa carreira e/ou para o seguimento dos nossos estudos no nosso futuro.

Bibliografia

- [1] Fundação Raspberry Pi, “raspberrypi,” Fundação Raspberry Pi, [Online]. Available: <https://www.raspberrypi.org/documentation/usage/gpio/>. [Acedido em 22 11 2019].
- [2] Fundação Raspberry Pi, “raspberrypi,” Fundação Raspberry Pi, [Online]. Available: <https://www.raspberrypi.org/>. [Acedido em 22 11 2019].
- [3] Fundação Wikimedia, “wikipedia,” Fundação Wikimedia, [Online]. Available: https://en.wikipedia.org/wiki/General-purpose_input/output. [Acedido em 22 11 2019].
- [4] P. Pinto, “pplware,” PPLWARE.COM – TECNOLOGIAS DE INFORMAÇÃO E SERVIÇOS WEB, LDA, [Online]. Available: <https://pplware.sapo.pt/linux/webiopi-controle-o-gpio-do-rpi-via-browser/>. [Acedido em 22 11 2019].
- [5] RaspberryPiVBeginners, “youtube,” Google (2006–presente), [Online]. Available: <https://www.youtube.com/watch?v=wGahWkjettw>. [Acedido em 22 11 2019].
- [6] Fundação Raspberry Pi, “raspberrypi,” Fundação RaspberryPi, [Online]. Available: <https://www.raspberrypi.org/downloads/raspbian/>. [Acedido em 22 11 2019].
- [7] Fundação Raspberry Pi, “webiopi,” Fundação RaspberryPi, [Online]. Available: <http://webiopi.trouch.com/>. [Acedido em 22 11 2019].
- [8] Yale, “yale,” Assa Abloy, [Online]. Available: <https://www.yale.pt/pt-PT/yale/portugal/produtos/smart-living/fechaduras-digitais/entr-smart-lock-solution/entr-kits/>. [Acedido em 22 11 2019].
- [9] Blue Planet Technologies, SA, “homeit,” Blue Planet Technologies, SA, [Online]. Available: <https://homeit.io/pt/>. [Acedido em 22 11 2019].
- [10] Blue Planet Technologies, SA, “homeit,” Blue Planet Technologies, SA, [Online]. Available: <https://homeit.io/pt/as-melhores-fechaduras-inteligentes-do-mercado/>. [Acedido em 22 11 2019].
- [11] B. F. Casey Reas, “processing.org,” [Online]. Available: <https://processing.org/>. [Acedido em 29 01 2020].
- [12] Eclipse Foundation, “eclipse.org,” [Online]. Available: <https://www.eclipse.org/kura/>. [Acedido em 17 07 2020].
- [13] Fundação Wikimedia, “wikipedia,” Fundação Wikimedia, [Online]. Available: <https://pt.wikipedia.org/wiki/Kotlin>. [Acedido em 17 07 2020].
- [14] Fundação Wikimedia, “wikipedia,” Fundação Wikimedia, [Online]. Available: <https://pt.wikipedia.org/wiki/OSGi>. [Acedido em 17 07 2020].