UNIVERSIDADE D
COIMBRA

Raquel Conde Margalho

SISTEMA DE GESTÃO DE FECHADURAS INTELIGENTES USANDO IOT PARA APLICAÇÃO EM CACIFOS DE UNIVERSIDADE

Dissertação no âmbito do Mestrado Integrado em Engenharia Electrotécnica e de Computadores, na especialização de Automação, orientada pelo Professor Doutor Humberto Manuel Matos Jorge e apresentada ao Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Ciências e Tecnologias da Universidade de Coimbra.

Julho de 2019

“Old ways won’t open new doors.”

[Author Unknown]

[Aos meus pais.]

Agradecimentos

Obrigada, Universidade de Coimbra por me teres acolhido por mais tempo do que o previsto, por me teres apresentado a algumas das pessoas mais importantes da minha vida e pelas experiências vividas naqueles que foram, até agora, os melhores anos da minha vida.

Agradeço ao Professor Humberto Jorge pela sua constante disponibilidade e flexibilidade que fez com que pudesse seguir com este projecto.

Obrigada aos meus pais, Luísa e Rui, pela paciência, por sempre me terem ensinado a pensar fora da caixa, e pelo apoio incondicional que me deram em qualquer fase da minha vida. Agradeço-vos do fundo do coração, são os melhores pais do mundo.

Ao meu mano mais velho, Ricardo, obrigada pelos sábios conselhos, pela disponibilidade total para me esclareceres qualquer dúvida e por me fazeres querer ser como tu.

Um obrigada ao meu mano mais novo, Rodrigo e à restante família.

Obrigada aos que fizeram parte da minha vida académica, com foco especial para a Joana, Cata, Daniel, Bruna e Clara que sempre me deram juízo e bons conselhos.

Obrigada ao meu parceiro do projecto de onde surgiu esta dissertação, Simão Dias (Mandarim) pela constante moleta que me foi apoiando durante todos estes anos e pela pessoa lógica e singular que és.

Obrigada ao BEST por todas as experiências, que sem dúvida tornaram a minha vida de hoje tão cheia de histórias e às pessoas incríveis que fazem o BEST Spirit.

Aos meus Erasmus que me abriram muitas portas e noções do mundo lá fora, um obrigada especial ao João, à Iolanda e ao Gusmão que me fizeram sentir em casa em todos os momentos.

Por último, obrigada Andrea por acreditares tanto em mim, por teres aguentado todos os meus delírios durante este último ano e por me tornares uma pessoa melhor todos os dias.

Que venham muitos mais desafios e que os possa partilhar com todos vocês.

Raquel

Resumo

Uma fechadura inteligente é uma fechadura electromecânica que tem o objectivo de fornecer um acesso fácil a uma porta quando recebe informação via *wireless* (comunicação sem fios) de um dispositivo autorizado e uma chave criptográfica para executar o processo de autorização. (Pandit et al. 2018)

Tal como outros dispositivos de automação, geram grandes quantidades de dados que podem ser usados e estudados para criar novas e interessantes funcionalidades para os seus utilizadores.

Tal como as fechaduras tradicionais, uma fechadura inteligente necessita de um mecanismo de tranca e de uma chave.

A chave utilizada para desbloquear um cacifo com fechadura inteligente é uma chave digital gerada para cada utilização e armazenada num dispositivo de autenticação como um *smartphone* ou um dispositivo configurado explicitamente para este efeito e que funciona sem fios no processo de autenticação (cartão, button, etc).

Deste modo, é possível substituir os porta-chaves físicos com várias chaves para diferentes fechaduras e ter acesso a diferentes fechaduras com um único dispositivo.

O sistema desenvolvido compreende uma componente de computação na *cloud* que é responsável por todas as comunicações entre os módulos do sistema e pelo armazenamento de dados bem como pela segurança dos acessos concedidos.

Com o objetivo de gerir os acessos a cacifos públicos universitários, foi proposto e desenvolvido um sistema de gestão de fechaduras inteligentes. Os utilizadores deste sistema podem controlar a fechadura inteligente através de uma aplicação móvel que inclui várias funcionalidades úteis ou do cartão universitário que também pode ser usado para aceder a edifícios.

Palavras-chave: Internet das Coisas, Sistema de Fechaduras Inteligentes, Gestão de Cacifos, Plataformas *Cloud*, Dispositivos de Autenticação, Controlo de Acessos

Abstract

A smart lock is an electromechanical lock that aims to provide easy access to a door when it receives wireless information from an authorized device and an encrypted key to perform the authorization process. (Pandit et al. 2018)

Like other automation devices, this process generates large amounts of data that can be used and analysed to create new and interesting features for the users.

Like traditional locks, a smart lock requires a locking mechanism and a key.

The key used to unlock a locker with a smart lock is a digital key generated for each use and stored in an authentication device such as a smartphone or a device configured explicitly for this purpose and that works wireless in the authentication process (card, button, etc.).

This way it is possible to replace the physical keys for each locker and have access to different lockers with a single device.

The developed system includes a cloud computing component that is responsible for all the communications between the system modules and the data stored as well as the security of the authorized access requests.

In order to manage the accesses requests to university lockers, a smart lock management system was proposed and developed. Users of this system can control the smart lock through a mobile application that includes several features or using the university identification card that can also be used to access buildings.

Keywords: Internet of Things, Smart Lock System, Lockers Management, Cloud Platforms, Authentication Devices, Access Control

Índice

Lista de Figuras

Siglas e Acrónimos

AWS	Amazon Web Services
BLE	Bluetooth Low Energy
CPU	Unidade Central de Processamento
DIY	"*Do it Yourself*"
FK	Chave Estrangeira
GAP	Perfil de Acesso Genérico
GATT	Perfil de Atributo Genérico
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IAPMEI	Instituto de Apoio às Pequenas e Médias Empresas e à Inovação
ID	Identidade
IoT	Internet das Coisas
LAN	Rede de Área Local
NFC	Near Field Communication
PIN	Número de Identificação Pessoal
PK	Chave Primária
RFID	Radio Frenquency Identification
SQL	Structured Query Language
TCP/IP	Protocolo de Controlo de Transmissão/Protocolo de Internet
URL	Uniform Resourse Locator
USB	Porta Universal

Introdução

A tecnologia está a evoluir progressivamente a cada dia. Na maioria dos casos, a tecnologia melhora a vida quotidiana de cada pessoa, tornando os processos mais fáceis ou simplesmente mais produtivos.

Esta Dissertação derivou de um programa do IAPMEI inserido numa das medidas da Estratégia Nacional de Promoção do Empreendedorismo designada por "Startup Portugal", que visou a dinamização de um ecossistema coerente que incentivasse as start-ups e a aceleração do seu crescimento.

O programa teve por objectivo promover o desenvolvimento de projectos de empreendedorismo inovador que se encontrassem em fase de ideia, facultando um conjunto de ferramentas técnicas e financeiras. O projecto apresentado por mim e por um colega (Simão Dias) foi de uma fechadura inteligente controlada por *smartphone* para o qual construímos um protótipo funcional e desenvolvemos um modelo de negócio.

A automação de fechaduras é um ramo da tecnologia que tem como objectivo simplificar a vida dos utilizadores automatizando os processos que uma pessoa precisa de seguir para aceder a um cacifo para guardar bens temporariamente.

O tradicional cacifo é um compartimento onde um utilizador pode guardar objectos durante um determinado tempo abrindo e fechando com uma chave física fabricada para cada fechadura.

Para além dos custos de fabricação, cópia e distribuição de chaves, as chaves físicas são pouco seguras porque podem facilmente ser copiadas ou perdidas e não guardam nenhum registo de utilizações.

A automação de fechaduras para cacifos dá aos utilizadores mais tempo para coisas realmente importantes, tornando o dia dos utilizadores mais eficiente e produtivo e é dividida em várias áreas. Uma das mais relevantes é a segurança.

Estes dispositivos são relevantes porque oferecem aos utilizadores acesso a um compartimento para guardar aos seus bens mas como são dispositivos inteligentes que

podem ser conectados à Web, devem ser desenvolvidos e projectados adequadamente para oferecer segurança real aos utilizadores do produto.

A utilização de um sistema de fechaduras inteligente permite acabar com os problemas de gestão de acessos aos cacifos por parte de quem os administra e trazer segurança para os seus utilizadores por ser gerada uma chave nova para cada utilização. (Kassem et al. 2016)

1.1. Motivação

Num futuro próximo, tudo à nossa volta estará a armazenar, enviar e receber dados constantemente para muitos propósitos e objectivos diferentes.

Com a forte presença da Internet das Coisas (IoT) em muitos dos objectos do nosso dia-a-dia e a existência de várias tecnologias a funcionar de forma adequada e sem interrupções, tendo como objectivo implementar um sistema de gestão de fechaduras inteligentes em cacifos de Universidade, há a necessidade de analisar algumas das tecnologias mais comuns usadas neste tipo de produtos, como protocolos de comunicação sem fios, protocolos de segurança, hardware, etc. (Urien 2014)

Esta análise pretende ser geral, a fim de seleccionar as tecnologias mais adequadas e com o melhor custo para aplicar num sistema de fechaduras inteligentes.

A necessidade de sentir segurança não é uma novidade para os seres humanos, mas os dispositivos que o fornecem têm percorrido um longo caminho até aos que temos no presente.

Com o crescimento e a expansão da Internet das Coisas e com a procura de dispositivos que garantam mais segurança e automação da vida pessoal, dispositivos como fechaduras inteligentes construídos para as suas próprias necessidades farão com que as pessoas fiquem mais focadas nas coisas que realmente importam nas suas vidas.

Para além disso, anula custos de fabricação e de cópia de chaves ou substituição da fechadura em caso de perda da chave como poderia acontecer com o sistema tradicional chave-fechadura.

1.2. Objectivos.

Com este projecto, pretende-se estudar a hipótese de utilizar as tecnologias actuais de fechaduras inteligentes para aplicação num conjunto de cacifos, substituindo as fechaduras tradicionais e pouco seguras e tornar a utilização dos cacifos mais segura e intuitiva para os utilizadores e administradores simplificando a atribuição dos acessos e o desbloqueio de cada fechadura de maneira autenticada e simples

O sistema de fechaduras inteligentes deverá ser suficientemente simples e eficiente para que possa ser utilizado por qualquer pessoa, e seguro suficiente de maneira a prevenir o acesso indesejado e/ou não autorizado a um cacifo.

O sistema deve ser controlado por meio de uma aplicação de *smartphone* e por meio dos cartões identificativos de estudante/docente. Deve existir uma plataforma *cloud* para controlar as interacções dos módulos do sistema e armazenar todos os dados gerados.

A fim de contribuir adequadamente, deve ser feita uma abordagem do mercado existente neste campo para avaliar as soluções existentes e concluir como desenvolver uma solução que possa complementar as que estão à venda bem como ser concorrente ao seu preço.

Para desenvolver uma solução para o sistema, é também necessário estudar as tecnologias que possam ser usadas e pesar as suas vantagens e desvantagens para alcançar a meta final.

1.3. Estrutura do Documento

O Capítulo 2 revela o estado de arte do mercado e tecnologias IoT. O capítulo está focado em fazer uma avaliação do mercado de fechaduras inteligentes para avaliar os recursos e o modo de operação de várias fechaduras inteligentes que existem à venda e qual o seu preço actual. O foco também está na tecnologia presente nos dispositivos de autenticação na forma de uma visão geral de várias tecnologias disponíveis.

O Capítulo 3 descreve sucintamente uma solução proposta, as suas funcionalidades e como o sistema se deve comportar;

O Capítulo 4 fornece uma visão interna de como o sistema de gestão é aplicado e as tecnologias usadas para fazer isso acontecer;

O Capítulo 5 está focado nos resultados de trabalho e numa abordagem de desenvolvimento sustentável.

2. Estado de Arte

O mercado de fechaduras automatizadas e respectivo software de gestão está em crescimento. Novas soluções são lançadas com uma frequência crescente no mercado com o objectivo de suprimir todas as necessidades dos utilizadores ou mesmo criar novos produtos.

Neste capítulo, é apresentada uma abordagem do mercado de fechaduras automatizadas de recentes soluções de bloqueio inteligente que estão a contribuir para o crescimento deste mercado. O objectivo é avaliar o que já foi feito e qual o valor que este trabalho tem no mercado.

As soluções apresentadas definem a referência para os mercados de fechaduras inteligentes na Europa devido aos seus altos padrões de segurança, quantidade e qualidade de recursos, como desbloqueio automático e desbloqueio remoto.

2.1. Visão Geral do Mercado de Fechaduras Inteligentes e de Sistemas de Gestão

As soluções apresentadas nesta secção são algumas das melhores no mercado de fechaduras automatizadas em desenvolvimento. Apesar de todas as soluções apresentadas fornecerem funções úteis para o utilizador, têm custos de material e manutenção excessivos e algumas delas apresentam uma manutenção periódica.

Neste estudo é proposto um modelo de sistema de gestão de fechaduras inteligentes para atribuição temporária de cacifos colocados em vários locais de uma universidade recorrendo à Internet das Coisas (IoT) e juntando as melhores ferramentas de cada produto do mercado para criar uma solução mais eficaz e económica que permita aos utilizadores usar cacifos temporariamente de maneira segura, tendo um registo dos acessos feitos bem como a sua gestão por parte de um administrador.

2.1.1. Empresa A

A empresa contactada desenvolve sistemas de fechaduras automatizadas para locais de armazenamento de bens. As suas soluções procuram ser simples para o utilizador, seguras e necessitarem de pouca manutenção.

É possível usar a sua solução com *Bluetooth Low Energy* (BLE) ou Wi-Fi de maneira a conectar a fechadura inteligente à aplicação de *smartphone* e poder fazer uso de todas as ferramentas disponíveis.

A solução de fechadura inteligente deverá estar conectada à rede local de Wi-Fi para se conectar ao servidor onde serão armazenados os dados de utilização.

Para usar a fechadura inteligente, o utilizador deve ter um *smartphone* com a app instalada. O *smartphone* do utilizador contacta directamente com o servidor da empresa por Wi-fi ou BLE.

É também possível ter acesso a um cacifo utilizando um cartão com tecnologia RFID como chave e sistema central de atribuição de cacifos. O sistema central tem cablagem ao servidor e a cada cacifo e neste caso funciona por proximidade com o leitor RFID.

As fechaduras funcionam a 12V por cablagem.

A segurança é uma das especificações mais importantes quando tratamos de cacifos para guardar bens.

A empresa contactada dispõe de fechaduras inteligentes com BLE para comunicar com a aplicação, mas não depende apenas do protocolo de segurança Bluetooth: existe uma camada adicional de segurança com criptografia *end-to-end* que significa que apenas mensagens criptografadas são enviadas para a aplicação de *smartphone* e a fechadura inteligente conhece a chave para decifrar a mensagem e executar o desbloqueio do cacifo.

As soluções desta empresa podem ser usadas com armários novos ou já existentes (retrofit).

Esta solução tem várias ferramentas disponíveis:

Uso da Aplicação - A aplicação para *smartphone* funciona como qualquer cartão inteligente RFID ou tag e pode ainda abrir remotamente ou gerir um cacifo sem uma interface de utilizador RFID. Tudo que precisa é de um sinal móvel de Wi-Fi.

Central ou On-door - Os leitores podem ser centrais e fazer uma distribuição aleatória dos cacifos disponíveis a atribuir ao utilizador ou podem ser on-door com leitores RFID.

Gestão Completa e Controlo - O software de gestão e interface de utilizador fácil de usar e intuitiva, dá aos utilizadores e administradores uma visão geral completa, gestão e controlo remoto sobre o seu cacifo em tempo real.

Todas as informações sobre actividades (no caso de partilha de cacifos) também estão disponíveis por meio de vários relatórios que fornecem uma análise mais detalhada, o que pode ajudar a identificar e optimizar a ocupação e a disponibilidade de cacifos.

Algumas das principais características:

- Visão geral central remota, administração e gestão
- Bloqueio e estado de bloqueio de cada armário
- Controlo completo do cacifo remotamente - adicionar, remover, atribuir cacifos
- Vários utilizadores de um cacifo para projectos e reuniões
- Modo de manutenção - armários a serem limpos antes do próximo utilizador
- Estatísticas e relatórios abrangentes sobre o uso de cacifos

Todos os Padrões RFID - As soluções de fechadura electrónica suportam os principais padrões de cartões inteligentes RFID (diferentes marcas: Mifare, LEGIC, CEPAS, Sony FeliCa, SRx, etc.).

Modos de Acesso Alternativos - Código de barras, código QR, código PIN, impressão digital ou app também podem ser usados como chaves de cacifo para instalações de armários.

A combinação de alguns deles proporciona um nível ainda mais alto de segurança no uso de cacifos de fácil utilização.

Budget para 50 cacifos e sistema de gestão:

14798€ + 303€ mensais durante 5 anos

2.1.2. Empresa B

A empresa contactada é pioneira no campo das tecnologias RFID/NFC para soluções de fechaduras automatizadas de cacifos/armários.

Esta empresa dispõe de sistemas de fechadura alimentados por bateria e sistemas com cablagem de rede (software incorporado).

Para o caso de estudo, interessa analisar os produtos com software de gestão incorporado que possibilite armazenar e gerir os dados das utilizações.

Os seus principais produtos são o produto que dispõe de um leitor em cada porta e o produto cujo leitor central atribui um cacifo disponível ao utilizador e a gestão dos dados é feita através do software de gestão por parte de um administrador.

Produto com leitor por porta:

O sistema de fechadura com leitor por porta é uma solução para instalações de cacifos de tamanho médio a grande, exigindo uma solução abrangente de gestão de cacifos. Os armários são conectados em rede a um computador onde o software de gestão opera. Todos os componentes da fechadura estão instalados completamente dentro do armário.

Produto com leitor central:

O sistema de fechadura com leitor central é especialmente projectado para bloqueio electrónico para armazenamento.

Para abrir um armário, o usuário é identificado no terminal central apresentando a sua credencial. A porta é aberta automaticamente por meio de um sinal electrónico em rede e é bloqueada novamente simplesmente pressionando-se a porta do armário. O sistema de leitor central é gerido pelo software de gestão e é compatível com vários componentes de hardware e software.

A identificação e o controlo do utilizador são obtidos através de um terminal central.

Gestão Completa e Controlo através do Software Gestão:

O software de gestão é uma solução para gerir os sistemas com leitor por porta e com leitor central. As características do software incluem alarme de rede, monitoramento de ocupação e controlo remoto de armários. Além desses recursos principais, o software

fornece informações detalhadas sobre o uso de cacifos e a capacidade de integração com outros servidores/*clouds*, como o controlo de acesso a edifícios, de modo a criar uma solução de sistema inovadora e completa.

Os recursos do software incluem monitorização de uso em tempo real, um alarme em rede e controlo remoto dos cacifos.

Através da interface web, os administradores podem monitorizar a ocupação, estado do alarme e adicionar utilizadores.

Esta solução tem várias ferramentas disponíveis:

Fácil gestão - Os administradores podem facilmente substituir as chaves perdidas. Se um utilizador se esquecer que cacifo usou, os terminais de informação exibem o número do cacifo usado, não precisando de staff.

Simplicidade - Sem PINs para lembrar, sem chaves mecânicas e cadeados para gerir ou transportar.

Flexibilidade - Flexibilidade de disponibilizar todos os cacifos ou de atribuir individualmente ou alugar cacifos por um período de tempo definido.

Segurança - Todas as aberturas e fechos são registados, o que significa que um administrador pode verificar facilmente quem abriu o cacifo e quando. Para segurança adicional, o sistema com leitor por porta tem alarme.

Dispositivos de chave NFC - Todos os sistemas de fechadura desta empresa operam com *smartphone*s, cartões e pulseiras com NFC e são construídos para trabalhar com abrangentes tecnologias baseadas em padrões internacionais. Para esse fim, os sistemas de fechadura da empresa contactada são compatíveis com muitas credenciais de terceiros.

Fácil de usar - Todas os sistemas de fechadura são fáceis e intuitivos de usar. Cada fechadura fornece um visor de estado claro, mostrando quais cacifos estão disponíveis e quais estão em uso e um som é gerado ao abrir e fechar o cacifo.

Budget para 50 cacifos e sistema de gestão:

18189,46€

2.1.3. Empresa C

Os cacifos desta empresa têm antenas integradas que permitem aos utilizadores fechar ou abrir um cacifo aproximando um dispositivo de identificação da fechadura.

O LoXS é o sistema de gestão dos cacifos electrónicos desta empresa. Outros métodos de identificação podem ser usados no terminal LoXS, incluindo código PIN, chave Technogym ou cartão MIFARE.

Na **figura 1** pode observar-se o funcionamento do sistema de cacifos desta empresa.

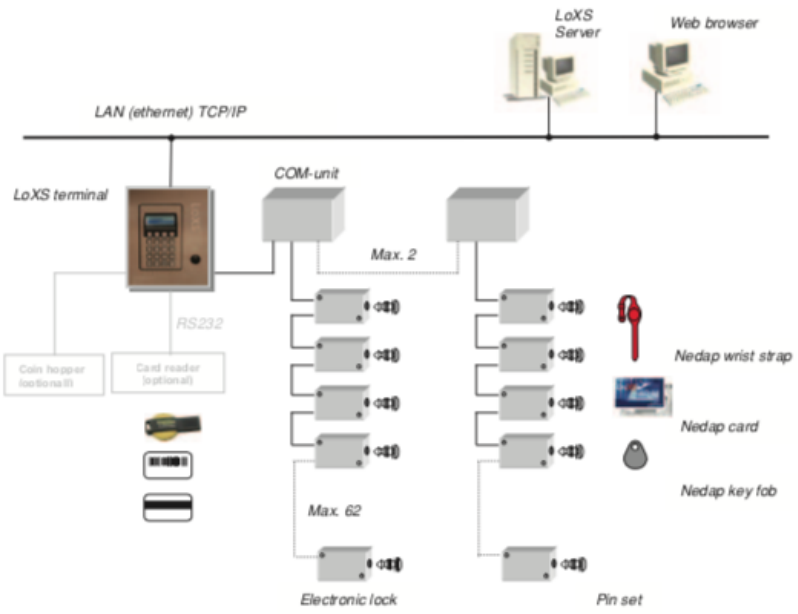

Figura 1: Funcionamento do Sistema de Cacifos da Empresa C

O sistema consiste basicamente em quatro elementos, como pode ser visto na figura acima:

- LoXS Terminal central - pode operar, no máximo, com 124 armários.
- COM-unit - A fonte de alimentação pode fornecer electricidade para, no máximo, 62 fechaduras.
- Fechadura electrónica - com antena integrada para enviar / receber dados.
- Conjunto de pinos - enroscados na porta do armário e prendidos à fechadura.

Além disso, os seguintes elementos são opcionais:

- Leitores de cartões de série - para código de barras, cartão magnético, *Technogym* ou *Mifare.*
- LoXS server application - para administrar vários terminais através de uma rede.

O terminal, as fechaduras electrónicas e os conjuntos de pinos são as únicas partes visíveis do sistema para os utilizadores.

A administração do sistema é possível através do uso do servidor LoXS. Os administradores podem aceder ao servidor através da web.

O LoXS Server está conectado ao terminal LoXS e à rede de clientes usando uma LAN com TCP / IP .

Funcionamento do servidor LoXS:

- Hardware do servidor (1GB memória, Intel Pentium 2.8GHz, 500mb free disk space)
- Software servidor (Windows server, Microsoft SQL server)
- Uma Local Area Network operacional baseada em TCP/IP

O servidor LoXS é um sistema "web based": será necessário um browser para aceder ao servidor LoXS e administrar o sistema LoXS.

2.2. Revisão das Tecnologias

De modo a construir o sistema de gestão de fechaduras inteligentes para aplicação em cacifos, é necessário fazer uma análise das tecnologias mais usadas neste tipo de produtos, tal como protocolos de comunicação sem fio para dispositivos de autenticação, sensores e actuadores necessários, plataformas *cloud* e software de gestão. Esta análise pretende ser geral de modo a ser possível seleccionar as tecnologias mais adequadas e económicas para aplicar num sistema de fechaduras inteligentes em cacifos.

2.2.1. Protocolos de Comunicação sem fios para Dispositivos de Autenticação

Os protocolos de comunicação sem fios tornaram-se muito populares pela redução de custos de implementação de tecnologias em edifícios, reduzindo a quantidade de cablagem necessária para instalar dispositivos como sensores. Este tipo de tecnologia também proporciona facilidade de associação de *smartphones* com o sistema de automação, desde que seja possível conectar o dispositivo à rede. (Reinisch 2007)

O principal objectivo de uma fechadura inteligente é prevenir o acesso não autorizado a um cacifo.

Há vários dispositivos de autenticação que podem ser utilizados para gerar e armazenar chaves como um *smartphone*, tags ou cartões, previamente configurados para tal. (Sousa et al. 2016)

A cada dispositivo podemos associar uma ou mais tecnologias de controlo e protocolos de segurança.

A integração de *smartphones* para aplicação de sistemas de segurança é uma tendência cada vez maior dada a simplicidade de controlar um sistema de fechaduras inteligentes com uma ferramenta do dia-a-dia. (Yunge et al. 2015)

A análise das tecnologias actuais de dispositivos de autenticação permite ter uma melhor noção do seu modo de funcionamento para poder escolher a/as mais adequada/s ao objectivo deste projecto.

2.2.1.1. Near Field Communication (NFC)

Podemos usar o protocolo de comunicação sem fios NFC usando como dispositivo de autenticação cartões que contenham NFC ou *smartphones* com esta tecnologia disponível para uso. (Sousa et al. 2016)

As soluções de chave digital com NFC para *smartphone* envolvem maior segurança e mais ferramentas do que as tradicionais chaves possibilitando a partilha de chaves entre utilizadores, a definição de alertas de tempo de uso, etc.

Para o caso dos *smartphones*: tem de haver uma compatibilidade do sistema de fechadura com o sistema operativo dos *smartphones* existentes para que esta solução seja aplicável. (Bonaventure et al. 2017)

A implementação segura de um sistema de fechaduras com NFC controlado por *smartphone* é uma opção viável com as desvantagens do sistema operativo do *smartphone* ter de ser compatível com NFC e de ter de haver uma alternativa caso o *smartphone* se encontre sem bateria no momento do check-out da utilização.

Segurança:

- Para definir que um dado utilizador é o dono temporário de um cacifo é necessária uma autenticação como utilizador "dono" de cacifo.
- Para prevenir o acesso não autorizado é necessário haver controlo dos acessos feitos a cada cacifo de maneira a que apenas um utilizador "dono" possa controlar a fechadura do cacifo que reservou e onde guardou os seus bens.
- Um utilizador "dono" de um cacifo, deverá ser capaz de transmitir a sua função a outro utilizador de maneira segura usando o *smartphone* como dispositivo de autenticação.
- Um utilizador "dono" de um cacifo, deverá receber notificações de abertura do seu cacifo por outro utilizador a quem tenha transmitido a sua função de "dono" (no caso do uso de *smartphone* como dispositivo de autenticação).

No sistema de *smart lock* baseado em NFC, a segurança depende da chave digital gerada no dispositivo de autenticação. No entanto, é necessário analisar como é que a chave digital é segura e se essa abordagem exige hardware com segurança especial ou outras características específicas.

O objectivo principal de segurança de um sistema de fechadura é garantir a autenticação segura do "dono" temporário da fechadura de um cacifo.

Requisitos específicos:

- As plataformas móveis geralmente hospedam um sistema operativo que pode ser comprometido e expor todos os dados armazenados na plataforma. Para evitar esses problemas, os dados sensíveis à segurança usados nos protocolos subjacentes devem ser protegidos contra códigos não confiáveis.

- O armazenamento de dados relativos aos utilizadores tem de ser seguro: os dados sensíveis à segurança não devem ser acessíveis por componentes de software não confiáveis enquanto armazenados na plataforma.
- Os componentes do sistema que operam em dados sensíveis à segurança devem ser confiáveis e isolados dos componentes não confiáveis.

Além disso, é preciso garantir que as operações sensíveis à segurança, como a autenticação de uma fechadura, sejam acções provenientes do utilizador "dono" e não por *malware*.

Atribuição de cacifo supondo que os cacifos se encontram todos fechados:

- Um leitor de NFC de uma fechadura conecta-se a um Arduino e lê os detalhes do dispositivo de autenticação do utilizador.
- O Arduino confirma se o utilizador é o dono dessa fechadura ou não.
- Se não for o dono da fechadura e o cacifo estiver livre, verifica o utilizador e envia um sinal para abrir a fechadura e guardar o utilizador como dono.

O sinal é sempre enviado ao servidor tanto para abrir como para trancar a fechadura.

A implementação do protocolo de autenticação usando NFC aquando do check-out ocorre entre o dispositivo de autenticação e a fechadura e é avaliado de acordo com o descrito acima. (Sunny, n.d.)

Para completar o protocolo de autenticação e como medida de protecção/ segurança, deverá ser definido um tempo de resposta da fechadura para verificar a resposta do dispositivo de autenticação.

2.2.1.2. Identificação por Radio-Frequência (RFID)

RFID é uma tecnologia de baixo custo que pode ser usada para diversas aplicações entre as quais o controlo de acessos e o sistema digital de segurança de uma fechadura, aplicações necessárias para este estudo. (Verma and Tripathi 2010)

A tecnologia RFID permite a transmissão de dados de maneira eficiente e segura por comunicação sem fios.

A identificação automática e sem fios é feita através de um código identificador (RFID tag) marcado no dispositivo de autenticação que servirá como chave (cartão, tag, etc) e que será usado para identificação do utilizador na fechadura.

A segurança é um tópico muito importante quando se trata de compartimentos para guardar bens pessoais.

Segurança:

- Com RFID é possível autenticar os utilizadores para que apenas o utilizador autorizado possa desbloquear a fechadura que lhe foi atribuída.
- Para a implementação do sistema de segurança para tranca e abertura de fechadura deverá ser usado um tipo passivo de RFID que tem como função activar, autenticar e validar utilizadores e desbloquear a fechadura em tempo real para um acesso seguro.

Ao usar um tipo de RFID passivo, poupa o uso de bateria uma vez que a energia é obtida a partir do leitor e permite o uso de identificadores também passivos que são de menor custo e peso que os identificadores activos. (Verma and Tripathi 2010)

As principais vantagens do RFID passivo são seu custo e pequeno tamanho.

Requisitos específicos:

- Os pedidos de acesso, autenticação e operação são controlados por um sistema central que guarda a informação dos acessos de cada utilizador, check-in e check-out e informação do utilizador que deverá estar associada ao registo prévio de cada pessoa.
- Um sistema de fechaduras inteligentes a funcionar com RFID usa hardware e software. Os componentes hardware são *tags* RFID, leitores, USB, cabos de conexão, etc. Os componentes de software são bases de dados que exigem suporte da rede de computadores para fazer a gestão e manutenção de registos dos utilizadores.

A fechadura de um cacifo ocupado desbloqueia quando o utilizador aproxima dispositivo de autenticação com o *tag* RFID do leitor e as informações coincidem com as informações já armazenadas na base de dados como utilizador “dono” do cacifo.

Atribuição de cacifo supondo que os cacifos se encontram todos fechados:

- Um utilizador aproxima o dispositivo que contém o *tag* RFID do leitor e o sistema verifica se é um utilizador registado.
- Se o utilizador estiver registado, as informações do dispositivo serão correspondidas com as informações do utilizador armazenadas na base de dados do sistema.
- Se um cacifo estiver livre, a fechadura desbloqueia para que o utilizador possa colocar os seus bens no cacifo e fecha automaticamente após um intervalo de tempo especificado.
- As informações de check-in são armazenadas na base de dados com data e hora e é gerado um registo de acesso.

O RFID controla o bloqueio e desbloqueio da fechadura de cada cacifo.

O registo de acessos de um utilizador é mantido numa base de dados indicando check-in, tempo de utilização (check-out – check-in), número identificador do cacifo, etc.

O administrador pode aceder ao servidor de base de dados remotamente e pode ver todos os registos.

O sistema de fechaduras inteligentes usando RFID permite que um utilizador faça o check-in e o check-out em condições rápidas, seguras e práticas.

2.2.1.3. Bluetooth Low Energy (BLE)

Bluetooth é um tipo de comunicação sem fios que permite conectar qualquer dispositivo à internet por meio de ondas de rádio de curto alcance.

Bluetooth Low Energy (BLE) é um modelo de Bluetooth de baixa potência que foi construído no âmbito da Internet das Coisas (IoT).

BLE destina-se a dispositivos que exigem menor consumo de corrente, menor complexidade e menor custo e pode ser utilizado em dispositivos que fornecem informações, mas também em dispositivos que aceitam comandos (como o desbloqueio). (Prada-Delgado, Vázquez-Reyes, and Baturone 2016)

Segurança:

Esta tecnologia conta com as seguintes fases:

- Emparelhamento - Processo para criar um código/chave secreto partilhado entre o dispositivo de autenticação e a fechadura.
- Ligação – Armazenamento da chave digital criada durante o emparelhamento para uso aquando da abertura da fechadura
- Autenticação – Processo para verificar que tanto o dispositivo como a fechadura têm a mesma chave.
- Criptografia – Para garantir a confidencialidade da mensagem entre dispositivo de autenticação e fechadura.
- Integridade da mensagem - Protecção contra falsificações de mensagens

A segurança da tecnologia é o aspecto mais importante neste estudo para uso de cacifos.

Ao utilizar, sobre o protocolo de segurança Bluetooth, criptografia end-to-end, apenas mensagens criptografadas são enviadas entre a fechadura e o dispositivo de autenticação de modo a tornar o sistema de fechaduras inteligentes ainda mais eficiente.

Requisitos específicos:

Os requisitos básicos de um dispositivo Bluetooth são definidos pelo Perfil de Acesso Genérico (GAP).

O GAP determina se o dispositivo BLE tem uma função periférica (dispositivo que anuncia sua presença para que o dispositivo central possa estabelecer uma conexão) ou uma função central (dispositivo que procura por dispositivos que se conectem e inicia a conexão).

No cenário de um sistema de fechaduras inteligentes o dispositivo de autenticação normalmente actua como periférico e a fechadura como central.

O Perfil de Atributo Genérico (GATT) determina se o dispositivo é um cliente ou um servidor (independentemente das funções GAP).

No cenário de um sistema de fechaduras inteligentes, o dispositivo de autenticação geralmente actua como um cliente e a fechadura como um servidor que lê dados do dispositivo usado como chave.

O GAP assegura as fases de segurança da conexão BLE (emparelhamento, ligação, autenticação de dispositivos, criptografia e integridade de mensagens). (Prakash et al. 2018)

Atribuição de cacifo supondo que os cacifos se encontram todos fechados:

- Para atribuição de um cacifo a um utilizador é necessário que o *smartphone* seja emparelhado com o dispositivo da fechadura para gerar um código/chave secreto.
- O BLE segue o mesmo princípio do NFC mas tem a vantagem de estar disponível em maior número de modelos de *smartphone*.

2.2.1.4. Wi-Fi

Os padrões Wi-Fi são baseados nas especificações IEEE 802.11. As implementações mais comuns têm um alcance de 30m em interiores, e 90m em exteriores.

O protocolo de comunicação sem fios Wi-Fi está sujeito a fortes interferências de equipamentos e dispositivos.

Os dispositivos Wi-Fi têm um consumo baixo que, em alguns casos, não são adequados para os requisitos de redes de sensores e actuadores. No entanto, Wi-Fi é uma tecnologia madura e promissora para integração vertical nos campos da automação. (Roorda et al. 2007)

Podemos usar o protocolo de comunicação sem fios Wi-Fi usando como dispositivo de autenticação um *smartphone* conectado à rede.

A tecnologia Wi-Fi fornece uma alta taxa de dados, tornando-os adequados para sistemas que necessitam enviar / receber uma quantidade considerável de dados tal como será necessário para o sistema de fechaduras inteligentes.

2.2.1.5. Outras Tecnologias / Protocolos de Comunicação sem Fios

Existem vários protocolos de comunicação sem fios que podem ser usados para um sistema de fechaduras inteligentes.

A escolha da tecnologia mais adequada para este projecto vai depender dos dispositivos, sensores e actuadores utilizados e também das características que o sistema deve fornecer.

Nesta análise foi feita uma visão geral e comparação de alguns protocolos de comunicação sem fios de curto alcance com baixo consumo de energia usados em soluções semelhantes (NFC, RFID, BLE, Wi-Fi).

Considerando o facto de que os protocolos de comunicação operam num meio aberto, a segurança tem que ser uma das maiores preocupações ao criar soluções de automação para aplicação em cacifos em espaços públicos que fazem uso desses protocolos. Especialmente se essas soluções forem focadas em segurança, como uma fechadura de porta ou um sistema de alarme, já que os invasores podem penetrar o sistema sem forçar a fechadura.

Como uma questão adicional, os recursos de segurança são limitados pelo requisito de baixo consumo de energia nos dispositivos, o que significa que uma boa relação segurança/consumo de energia tem que ser alcançada para atingir os requisitos do dispositivo/sistema, como preço, consumo de energia entre outras. (Pothuganti and Chitneni 2014)

2.2.2. Plataformas *Cloud*

O sistema de gestão de fechaduras inteligentes concentra-se na gestão fácil e na atribuição de cacifos aos utilizadores, usando os fundamentos da Internet das Coisas (IoT), conectando todo o mecanismo da fechadura à *cloud*.

De modo a conectar todos os cacifos e armazenar e estudar os dados gerados pelo seu uso, existe a necessidade de usar uma solução de *cloud* para este trabalho.

Os cacifos podem estar ligados à Internet por *Ehternet* ou por meio de protocolos de comunicação sem fios (BLE / Wi-Fi).

A plataforma *cloud* selecionada será o coração de todo o sistema, fazendo a gestão dos pedidos de acesso a partir dos dispositivos usados como chave e todas as interações com o hardware da fechadura inteligente.

Para selecionar a solução mais adequada disponível, é necessário avaliar as diferentes especificações de cada uma delas, como a capacidade de armazenamento oferecida, número de movimentos de dados GET e POST disponíveis e o preço geral de uso do serviço.

Apesar do grande número de soluções de *cloud* disponíveis, é necessário considerar as características apresentadas para escolher a solução certa para este trabalho.

Plataformas *Cloud*:

Amazon Web Services (AWS): Este serviço da Amazon tem produtos específicos para soluções de IoT com grande foco na gestão de dispositivos de IoT e na segurança de dados. Para além disso, possui um serviço integrado de análise de dados para ajudar qualquer pessoa a recolher informações dos dados gerados pelos seus dispositivos. Cada produto diferente da Amazon tem um preço próprio, dependendo das soluções exigidas pelo trabalho. Os produtos e serviços da AWS estão disponíveis em escala mundial. ("Amazon Web Services (AWS) - *Cloud* Computing Services," n.d.)

EasyIoT: A plataforma de *cloud EasyIoT* tem como objectivo fornecer uma plataforma segura, confiável e barata para IoT, focada principalmente nos métodos "*Do it Yourself*" (DIY). O *EasyIoT* parece simples de usar para o utilizador independente, mas não fornece tantos serviços e funções como os grandes nomes do mercado. A sua utilização é gratuita a não ser que o utilizador queira ampliar sua solução. É ideal para utilizadores únicos com implementação simples num único espaço. ("Easy IoT," n.d.)

Google *Cloud*: A *Google Cloud* fornece uma solução de *cloud* mundial. Tal como a AWS, a *Google Cloud* oferece uma vasta gama de produtos e serviços, incluindo soluções de IoT, como a *Cloud IoT* Core, que fornece conexão e gestão segura dos dispositivos. Outros produtos para calcular e estudar dados também estão disponíveis nesta solução. Cada produto diferente da Google *Cloud* tem um preço próprio, dependendo das soluções exigidas pelo trabalho. ("Google Cloud Computing, Hosting Services & APIs | Google Cloud Platform," n.d.)

IBM *Cloud*: Assim como os outros grandes nomes da indústria de plataformas de *cloud*, a IBM tem muitos serviços e produtos disponíveis em escala mundial. A *Internet of Things Platform*, da IBM, ajuda a desenvolver e conectar as soluções de IoT. Além disso, possui várias funções de análise de dados, nas quais o utilizador pode definir suas próprias regras e accionar alertas e outras funções. Cada produto diferente da IBM *Cloud* tem um preço próprio, dependendo das soluções exigidas pelo trabalho. ("IBM *Cloud*," n.d.)

Microsoft Azure: A Microsoft não se conseguiu afastar do setor das *clouds* e tem disponíveis muitos serviços e produtos, incluindo soluções focadas em IoT. Assim como o Mercado concorrente, a Microsoft possui gestão de dispositivos e análise de dados criada especificamente para melhorar soluções e dispositivos IoT. Cada produto diferente da Microsolf Azure tem um preço próprio, dependendo das soluções exigidas pelo trabalho. ("Plataforma de Informática Na Cloud e Serviços Do Microsoft Azure," n.d.)

2.2.3. Sensores e Actuadores

A fechadura da porta dos cacifos, contará com um sensor, um actuador e um microcontrolador que controlará os cacifos de um armário. Para tal é necessária uma tecnologia de detecção de movimento que permita ao sistema entender se a porta está aberta ou fechada para evitar acções desnecessárias de bloqueio / desbloqueio, um actuador que deve executar a acção de desbloqueio em si e um microcontrolador que será usado para desencadear o sistema da fechadura e decidir que cacifo deverá ser aberto.

- **A posição da porta (Sensor)**

O sensor de posição da porta serve para avaliar o estado da porta: aberta ou fechada. Ao ler o sensor evitam-se acções desnecessárias de desbloqueio/ bloqueio, como trancar a porta enquanto a porta estiver aberta.

O sensor também desenvolve um papel importante no registo de novas actividades de entrada na base de dados sempre que a porta é desbloqueada e aberta por um utilizador. Duas tecnologias diferentes de sensores magnéticos foram pesquisadas: o sensor de efeito hall e o sensor de *switch reed*. Ambos são activados por uma influência magnética externa e não há grande diferença entre eles.

Apesar desse facto, o sensor *switch reed* é conhecido por ser mais forte e robusto do que os sensores de efeito hall (Effect 1940) e existem tipos de sensores *switch reed* feitos para utilização em portas e janelas. (“Magnetic Contact Switch (Door Sensor).,” n.d.)

Para saber se a porta está aberta ou fechada, pode ser usado o sinal de *switch reed* 1 ou 0. O sinal 1 representa a porta aberta e o sinal 0 representa a porta fechada.

- **Desbloqueio/Bloqueio da fechadura da porta (Actuador)**

O método mais simples para trancar a porta é conectar um pequeno solenóide ao microcontrolador. O solenoide bloqueia a porta com segurança até receber energia. Quando recebe energia, encolhe e a porta fica desbloqueada.

- **Microcontrolador**

O microcontrolador é o coração de todo o sistema, pois é responsável por todo o controlo do hardware e pela manutenção dos pedidos de acesso e dados digitais. Deverá ser colocado numa parte do armário de cacifos que não seja visível nem possível de aceder pelo utilizador. (Sayar and Pawar 2016)

O microcontrolador (Arduino/Raspberry) controla todo o mecanismo do software e funciona como uma ponte entre os componentes de hardware e software essencialmente usado para que possam trabalhar em conjunto.

Para controlar e conectar o sensor e o actuador e para receber/enviar dados entre a fechadura do cacifo e a *cloud*, é necessário um microcontrolador que possa fornecer essa informação.

Através do microcontrolador é possível conectar a resposta do switch reed e o pulso de energia do solenóide à cloud através de um cabo ethernet ou de comunicações sem fios (Wi-Fi/Bluetooth).

As acções do hardware na fechadura do cacifo são processadas e enviadas pelo microcontrolador. (Sarp et al. 2015)

Microcontrolador (Arduino/Raspberry pi): Um microcontrolador é um pequeno computador de circuito integrado contendo um ou mais CPUs, memória e periféricos de entrada / saída programáveis. No contexto, é usado para conetar o software ao hardware.

Vários microcontroladores estão disponíveis no mercado, como Arduino Raspberry PI, Orange PI, Intel Joule, Ada Feather, Autonomo, Beagle Bone, etc. (Basha, Jilani, and Arun 2016)

Para selecionar o microcontrolador dentre os disponíveis no mercado, há a necessidade de definir as especificações que são cruciais para o desenvolvimento deste trabalho, como, por exemplo, incluir, pelo menos, a capacidade de se conectar a outros dispositivos via Bluetooth, Wi-Fi ou outro protocolo de comunicação sem fios. O preço e a facilidade de compra também são relevantes para a selecção do microcontrolador.

3. Modelação do Sistema

Para atingir os objetivos deste trabalho mencionados no capítulo 1 é necessário definir a solução a implementar.

Para melhor compreensão, o sistema está dividido em módulos: cada um explicado separadamente.

Os módulos são: O Sistema de Atribuição de Cacifos, O Hardware de Fechadura Inteligente, O Dispositivo de Autenticação, O Utilizador e O Administrador.

- **O Sistema de Atribuição de Cacifos através da Plataforma *Cloud***

A *Cloud* é o centro de operações do sistema. O trabalho da *cloud* é responder e gerir os pedidos de acesso dos utilizadores, interagir com o hardware da fechadura inteligente, armazenar e analisar os dados gerados pela actividade.

- **O Hardware de Fechadura Inteligente**

Cada cacifo será um cacifo "tradicional" com a adição de componentes como um microcontrolador, um sensor e um actuador , que o tornam "inteligente".

O microcontrolador faz a conexão à *cloud* pela internet através de comunicações sem fios ou ligação *ethernet* e será responsável por todo o controlo do hardware e manutenção dos pedidos de acesso e tratamento de dados. Um microcontrolador controla um armário de cacifos.

- **O Dispositivo de Autenticação**

O dispositivo de autenticação é a chave utilizada para desbloquear uma fechadura inteligente. Para cada utilização é gerada uma chave temporária correspondente ao dispositivo de autenticação que permite ao utilizador ter acesso a um determinado cacifo durante a sua utilização.

O dispositivo de autenticação tem de ser configurado previamente e comunicará com a *cloud* através de um processo de autenticação *contactless* enviando e recebendo solicitações de acesso à *cloud*.

- **O Utilizador**

O utilizador é a pessoa que vai usar os cacifos. Um utilizador pode desbloquear um cacifo com o dispositivo de autenticação previamente registado.

O utilizador poderá ter acesso ao registo da sua actividade de modo a estar consciente do uso que faz dos cacifos.

- **O Administrador**

O Administrador é um Utilizador com direitos de gestão. O Administrador tem acesso directo aos dados armazenados na *cloud* e pode editar elementos da base de dados, como por exemplo consultar o histórico de interações dos utilizadores com os cacifos, alocar cacifos, mudar o estado de um cacifo (desbloquear um cacifo sem a presença do utilizador), entre outras interações.

Conectando estes cinco módulos, tornando a plataforma *Cloud* o centro de todas as operações do sistema, obtemos o sistema de gestão de fechaduras inteligentes a aplicar em cacifos.

Para entender todos os recursos do sistema e desenvolver o próprio sistema, é importante começar com a modelagem do sistema.

A **secção 3.1** está focada na explicação do funcionamento de cada um dos principais módulos para melhor compreensão da importância de cada um deles no sistema.

A **secção 3.2** apresenta um modelo de sistema que descreve o comportamento do sistema com um todo.

A **secção 3.3** faz uma abordagem a todas as diferentes funções do sistema com o objectivo de entender o que acontece por trás de cada função do sistema.

A **secção 3.4** tem como objectivo descrever o modelo de base de dados que é necessário implementar para que o sistema funcione sem falhas e, ao mesmo tempo, garantir que todas as funções são cumpridas.

3.1. Funcionamento dos Módulos Principais

Esta secção tem como objectivo descrever as diferentes funcionalidades, funções e casos de uso que definem cada um dos principais módulos do sistema.

3.1.1. Plataformas *Cloud*

O papel da *cloud* neste trabalho é ser o centro de operações de todo o sistema. A *cloud* tem a capacidade de gerir a aplicação de *smartphone* e os pedidos HTTP ao hardware da fechadura inteligente e armazenar toda a actividade dos cacifos e os dados dos utilizadores.

Os pedidos HTTP são enviados dos dispositivos de autenticação para a cloud através do microcontrolador e a cloud enviará a resposta ao microcontrolador que vai alocar um cacifo ao utilizador caso o pedido de acesso seja autorizado. Na **figura 2** está representado o esquema de comunicações com a cloud.

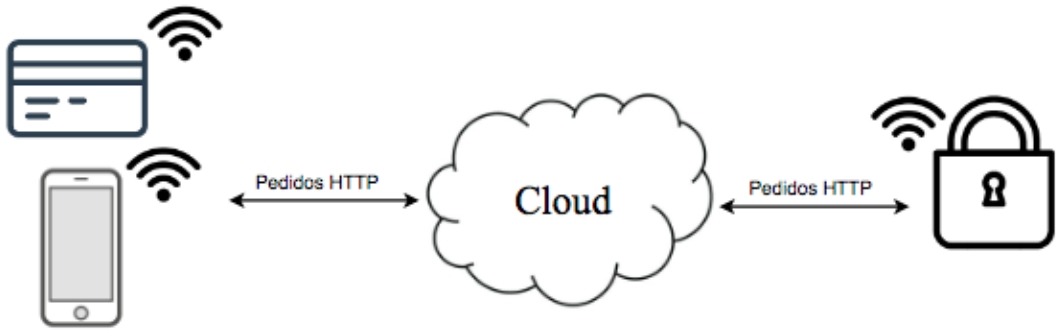

Figura 2: Diagrama de Comunicações com a *Cloud*

3.1.2. Hardware de Fechadura Inteligente

Um armário tem vários cacifos. A cada armário é associado um:

- Microcontrolador com comunicação sem fios ou via *ethernet*;
- Leitor RFID central
- Display numérico para indicar o cacifo atribuído

O microcontrolador está conectado à fechadura de cada cacifo, onde são afixados:

- Actuador de bloqueio de porta;
- Sensor de posição da porta;
- Mola que faz com que a posição da porta por *default* seja "fechada"

O microcontrolador é programado para conectar-se, através da tecnologia Wi-Fi ou cabo *ethernet* à web para receber pedidos de desbloqueio de utilizadores e poder realizar acções de desbloqueio e bloqueio através do actuador de bloqueio e, ao mesmo tempo, ler o sensor de posição da porta para entender se a porta está aberta ou fechada.

O hardware de fechadura inteligente conecta-se diretamente à *cloud* por meio de pedidos HTTP como é possível observar na **figura 3**.

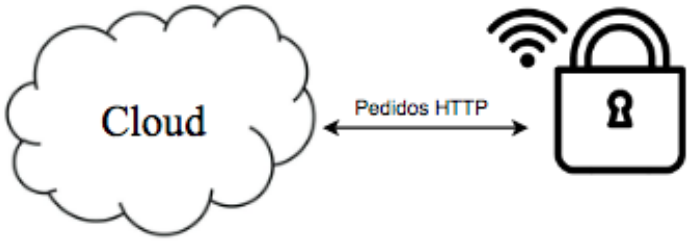

Figura 3: Diagrama de comunicações do hardware à *Cloud*.

3.1.3. Dispositivo de Autenticação

Pretende implementar-se este sistema de gestão de cacifos numa Universidade, e como tal, será possível utilizar tanto o *smartphone* como o cartão de estudante/docente como dispositivo de autenticação.

Toda a informação será guardada no número único de identificação do estudante/docente.

É possível combinar o uso do cartão com o uso do *smartphone* sendo que todos os acessos de qualquer um destes dispositivos de autenticação são armazenados para um mesmo número(ID) de estudante/docente.

Após analisar as tecnologias disponíveis no mercado para dispositivos de autenticação foram então comparadas.

Para o uso do cartão universitário:

- Uma vez que a maior parte dos cartões de Universidade são Mifare, a tecnologia mais adequada para estes dispositivos é o RFID.

Para o uso do Smartphone:

- NFC nao está disponível para uso em todos os Smartphones

BLE comparando com Wi-Fi:

- Wi-fi é melhor para transferencias de grandes quantidades de dados.
- A segurança no BLE é a nivel de protocolo.

3.1.3.1. Aplicação para *Smartphone*

De modo a comunicar com o sistema de fechaduras inteligentes através de um *smartphone* e ao mesmo tempo, com o desenvolvimento de uma base de dados para estudar os dados gerados pelo uso das fechaduras inteligentes e toda a comunicação web para garantir a integração de todos os diferentes módulos, a tecnologia mais adequada para suportar as comunicações do projecto é o Wi-Fi.

O protocolo de comunicação Wi-Fi fornece uma maneira confiável comunicações que se pode conectar facilmente à Web para comunicar com a *cloud*.

Através da aplicação para *smartphone*, o utilizador pode realizar várias acções. Depois de se inscrever na aplicação, associando o seu número de identificação da universidade, será validado por um administrador que vai verificar que os dados introduzidos estão correctos (nome e número de identificação) e, enquanto estiver com o login activo, o utilizador deve ser capaz de controlar a fechadura do cacifo para executar uma acção de desbloqueio.

Também é possível verificar um registo de actividades do uso dos cacifos (número do cacifo, hora de acesso e saída, alterar dados pessoais (email e palavra-passe).

Resumindo através da aplicação para *smartphone* é possível fazer:

- Registo de utilizador / login / logout;
- Edição de perfil de utilizador;
- Controlo de acção de desbloqueio inteligente;
- Resumo de actividade dos cacifos.

Esta aplicação para *smartphones* é desenvolvida a partir das opções da *cloud* na qual as operações são baseadas em pedidos HTTP feitos na *cloud* através da web como é possível observar na **figura 4**.

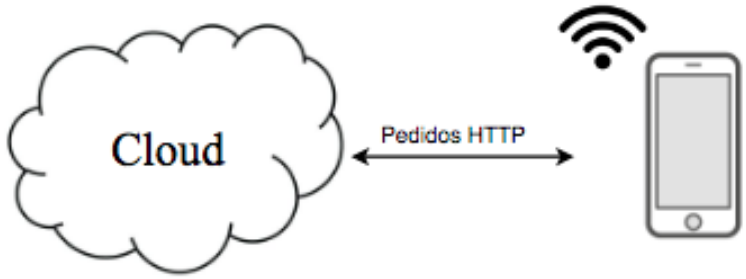

Figura 4: Diagrama de comunicação do *Smartphone* à *Cloud*.

3.1.3.2. Cartão da Universidade RFID

Uma vez que a maior parte dos cartões de Universidade são Mifare, a tecnologia a ser usada para estes dispositivos de autenticação será o RFID. O uso do cartão da universidade como dispositivo de autenticação tem de ser configurado previamente de modo a ser feito, tal como na aplicação, a associação do número de identificação ao nome do aluno/docente bem como, no caso do cartão, ao número identificativo da *tag* RFID.

Ao registar o cartão, passa a ser possível fazer um pedido de acesso pela aproximação do mesmo com o painel central de leitura RFID que comunicará com a *cloud* enviando um pedido de acesso. Após validação do registo do ID do cartão, um cacifo será alocado ao utilizador através do display.

Na **figura 5** é possível observar como são feitas as comunicações entre o cartão da universidade e a cloud.

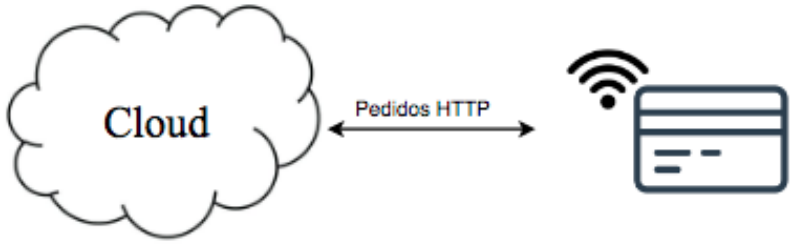

Figura 5: Diagrama de comunicação do cartão da Universidade RFID à *Cloud*.

3.2. Modelo do Sistema

A **Secção 3.1** está focada em descrever as funcionalidades dos principais módulos individuais do trabalho para obter uma melhor percepção do papel de cada um dos módulos no sistema global.

Esta secção tem como objectivo descrever todo o comportamento do sistema com o fim de modular e implementar adequadamente cada um dos módulos deste trabalho e procurar uma fácil integração entre eles. Descrever o comportamento do sistema também é importante para entender as interações entre todos os módulos e o fluxo de acções que definem a implementação correcta do sistema.

Conforme explicado na seção 3.1 e mostrado na **figura 6**, o utilizador controla o hardware da fechadura inteligente por meio da aplicação para smartphone ou do cartão da universidade RFID com a *cloud* agindo como o intermediário que coordena todo os pedidos do sistema entre todos os módulos. Isto significa que tudo o que acontece em todo o sistema é controlado, verificado, registado ou até autorizado pela *cloud*.

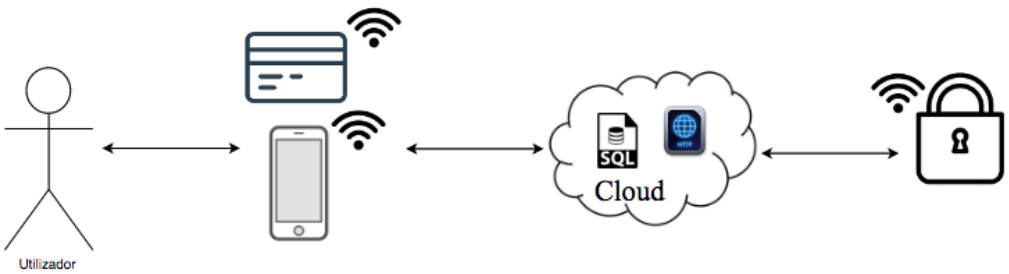

Figura 6: Diagrama do Modelo de Comunicações

3.3. Funções do Sistema

Com todo o modelo do sistema descrito na secção anterior, é importante definir e descrever o comportamento específico das diferentes funcionalidades do sistema, mencionado resumidamente em 3.1.

3.3.1. Função de Registo

O utilizador deve registar-se no sistema antes da primeira utilização. A acção de registo é executada, através da aplicação para *smartphone* pelo utilizador ou através do registo do cartão da universidade por um administrador.

Aplicação para *smartphone*: Inserindo os seus dados pessoais (nome, número de estudante/docente, mail, palavra-passe) e pressionando o botão que prossegue com a acção que cria uma nova conta de utilizador.

Após essa acção, os dados inseridos são verificados por um administrador e, se tudo estiver certo, o novo utilizador fica activo e pode fazer login no *smartphone* e usar livremente as funções da aplicação de fechadura inteligente.

A **figura 7** apresenta o fluxograma para a função de registo no smartphone.

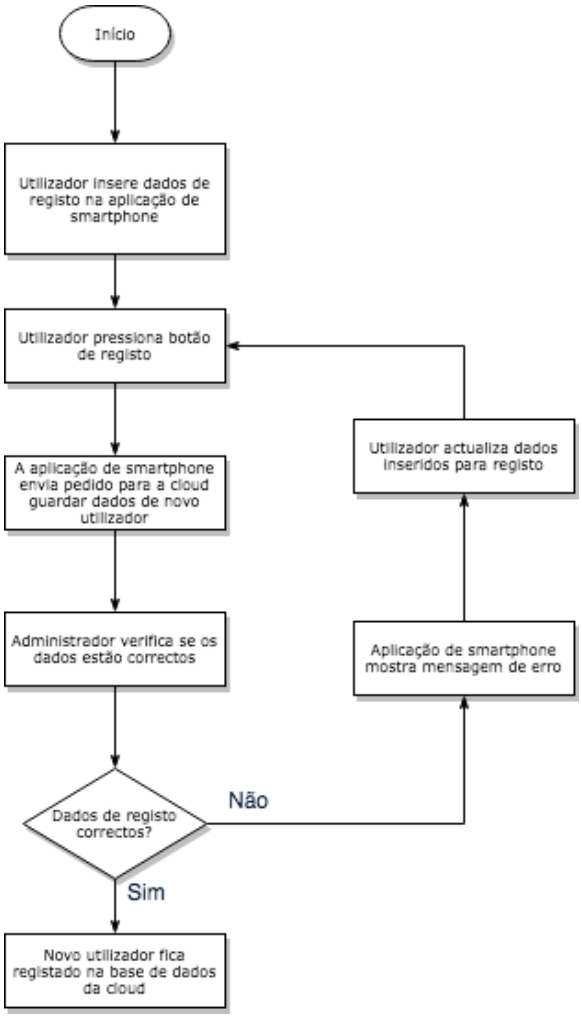

Figura 7: Diagrama de Fluxo da Função de Registo no *Smartphone*

Cartão da Universidade RFID: Um administrador faz a leitura do cartão e associa número único da tag RFID do mesmo os dados pessoais do utilizador (nome, número de estudante/docente, mail, palavra-passe) e prossegue com a acção que cria uma nova conta de utilizador. Após essa acção, os dados são inseridos directamente na *cloud* e o cartão do utilizador fica registado para uso dos cacifos de fechadura inteligente.

Se esta acção for realizada antes do registo na aplicação para *smartphone*, é necessário apenas fazer login na aplicação para usar o smartphone como dispositivo de autenticação.

3.3.2. Função de Login

Esta acção é apenas necessária para o uso da aplicação para *smartphone*.

Depois de se registar, o utilizador pode efetuar login e aceder a todas as funcionalidades de aplicação. Para fazer login, o utilizador tem de preencher os campos de nome de utilizador e palavra-passe com as credenciais correctas para a aplicação saber quem está a fazer login. Após pressionar o botão de login, a *cloud* recebe um pedido de login e verifica se os dados introduzidos estão corretos. Se a resposta for positiva, a sessão de utilizador fica activa. Se o utilizador não inserir as credenciais correctamente, recebe uma mensagem de erro.

A **figura 8** apresenta o fluxograma para a função de login para início de sessão do utilizador registado no smartphone.

Figura 8: Diagrama de Fluxo da Função de Login no Smartphone

3.3.3. Função de Histórico de Acessos/Actividade

A aplicação para *smartphone* do sistema oferece aos utilizadores a possibilidade de verificar seu próprio registo de atividades de uso dos cacifos. Esta função tem como objectivo mostrar ao utilizador as acções de desbloqueio realizadas por ele apresentando a data e hora de acesso, o número e local do cacifo acedido e a data e hora de fim de utilização. Como mencionado acima, os utilizadores podem ver apenas sua própria actividade, embora o administrador do sistema possa verificar não apenas as suas próprias actividades, mas também as actividades de outros utilizadores.

A **figura 9** apresenta o fluxograma para o acesso ao registo de actividade de cada utilizador.

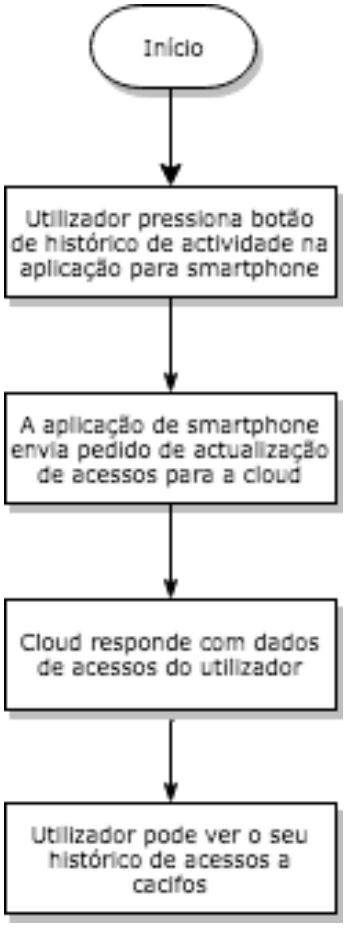

Figura 9: Diagrama de Fluxo da Função de Histórico de Acessos

3.3.4. Função de Desbloqueio de Fechadura

Desbloquear um cacifo é uma das principais funções do sistema.

Assumindo um utilizador já registado:

Com *smartphone*: Para usar este recurso, o utilizador deve pressionar o botão de desbloqueio na aplicação para enviar um pedido de acesso para a *cloud* que dará ao hardware autorização para desbloquear e mostrará na aplicação o número do cacifo alocado ao utilizador. Após este processo, o sensor lê o estado da porta com o objectivo

de entender se o utilizador abriu ou não a porta, durante um intervalo de tempo curto. Se o utilizador abrir a porta, o hardware envia um pedido à *cloud* para guardar um novo registo na base de dados de actividades da fechadura inteligente. Caso contrário, após esse intervalo de tempo definido, a porta é novamente bloqueada. ***(Figura 10)***

Com cartão da Universidade RFID: Para usar este recurso, o utilizador deve aproximar o cartão do painel de leitura RFID para enviar um pedido de acesso para a *cloud* que dará ao hardware autorização para desbloquear e mostrará no display junto ao painel o número do cacifo alocado ao utilizador.

Após este processo, o sensor lê o estado da porta com o objectivo de entender se o utilizador abriu ou não a porta, durante um intervalo de tempo curto. Se o utilizador abrir a porta, o hardware envia um pedido à *cloud* para guardar um novo registo na base de dados de actividades da fechadura inteligente. Caso contrário, após o intervalo de tempo, a porta é novamente bloqueada. ***(Figura 11)***

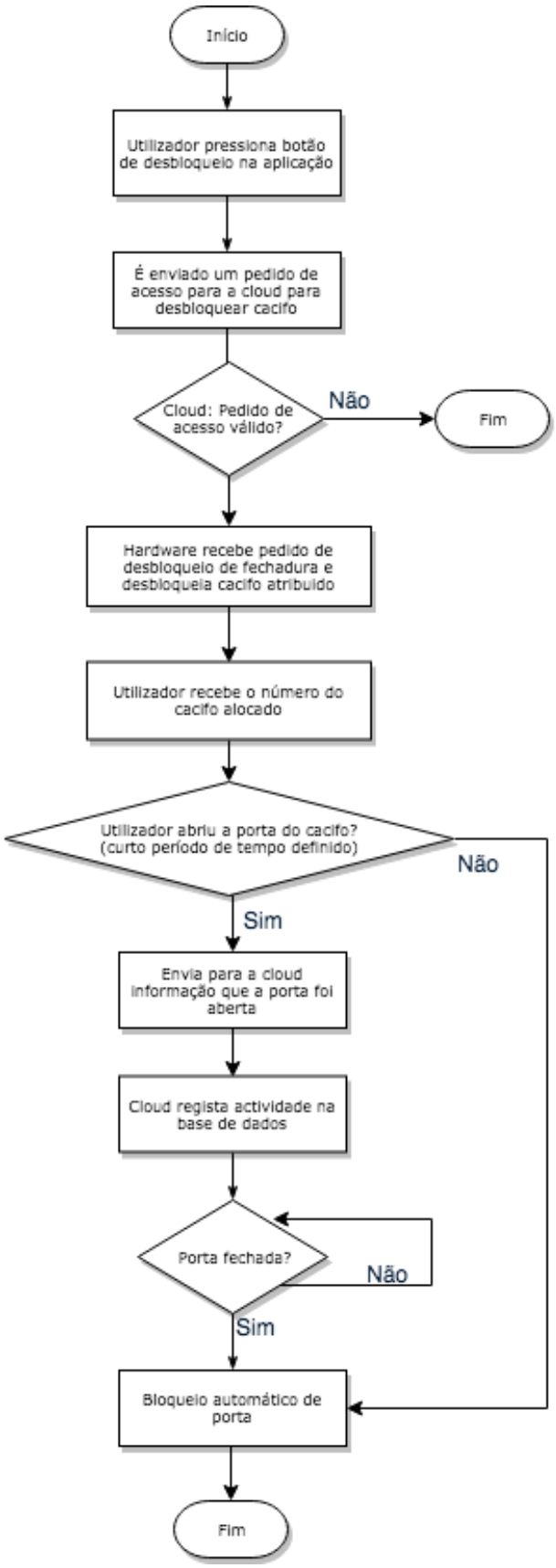

Figura 10: Diagrama de Fluxo da Função de Desbloqueio com *Smartphone*

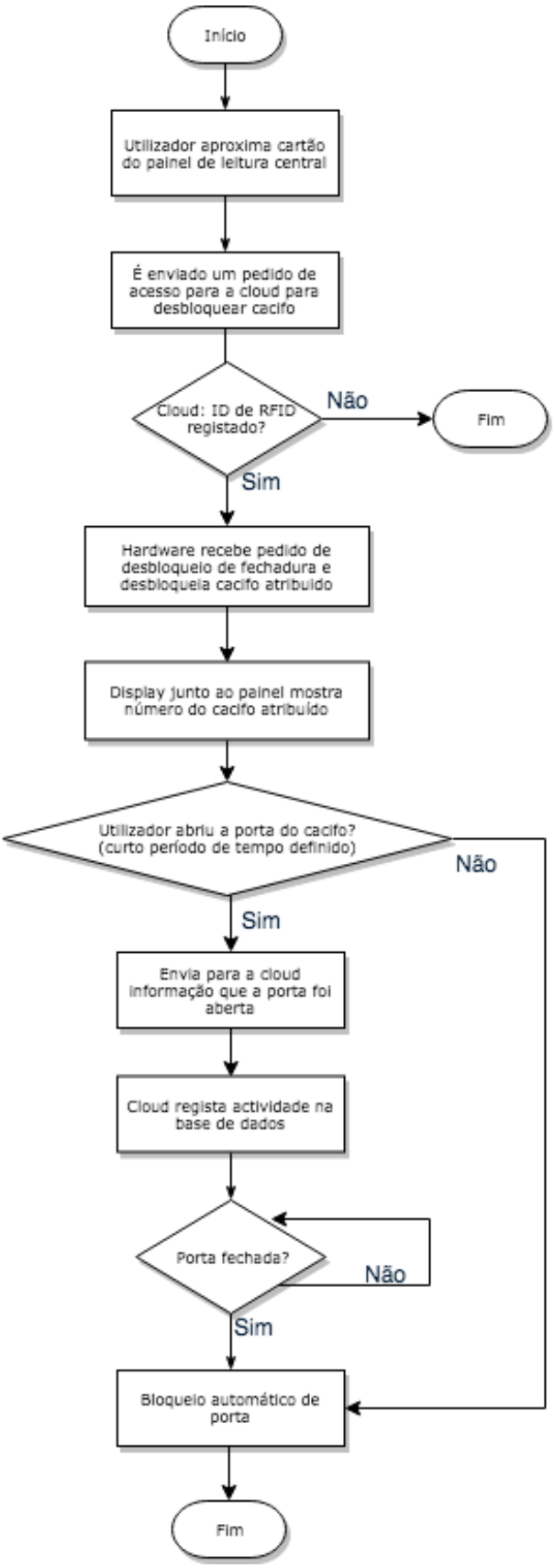

Figura 11: Diagrama de Fluxo da Função de Desbloqueio com Cartão de Universidade

3.3.5. Hardware de Fechadura Inteligente

O módulo de hardware desempenha um papel importante em todo o sistema. O hardware representa a fechadura inteligente em si, vai ajudar o sistema a ter uma representação física da própria acção de desbloqueio e é extremamente importante, garantindo que os dados gerados sejam confiáveis. Conforme mencionado, o hardware é composto pelo microcontrolador, um actuador de bloqueio de porta e um sensor de posição de porta. Para funcionar corretamente, o hardware executa uma calibração para garantir que o actuador da porta esteja na posição de bloqueio e se conecte à rede predefinida.

Depois disso, fica à espera até que haja um pedido de acesso na *cloud*. Após a chegada do pedido, é alocado um cacifo disponível por um método de alocação aleatória e a porta do cacifo é desbloqueada. Depois, o sensor de posição da porta aguarda a abertura da porta durante um determinado curto período de tempo para enviar à *cloud* a permissão para registar uma nova actividade do utilizador na base de dados. Se a porta for aberta, a actividade é registada. Caso contrário, a porta bloqueia novamente após o período de tempo determinado ter passado. O sensor de posição da porta ajuda a evitar acções desnecessárias de bloqueio / desbloqueio.

Quando houver novo pedido de acesso, caso o utilizador tenha um check-in registado na tabela de actividade, é-lhe alocado o mesmo cacifo do pedido de acesso anterior para que seja possível retirar os seus bens do cacifo e então é registado na tabela de actividade a data e hora de acesso (*check-out*).

Na **figura 12** é apresentado o fluxograma do funcionamento do hardware da fechadura quando é feito um pedido de acesso por parte de um utilizador.

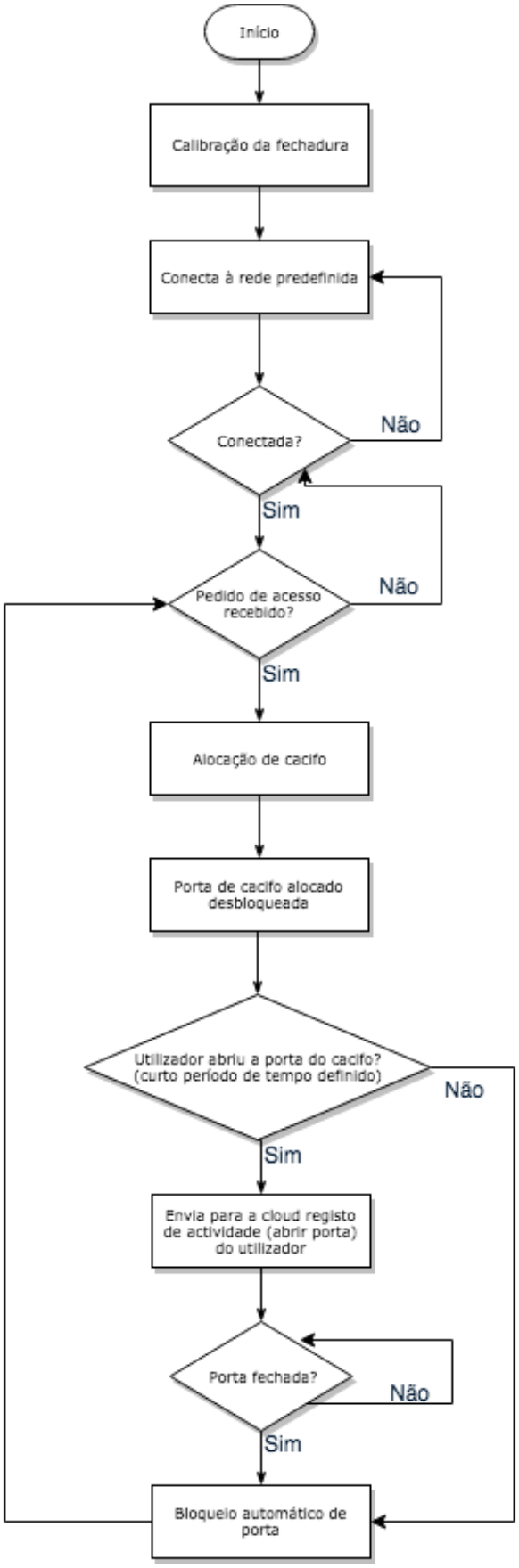

Figura 12: Diagrama de Fluxo do Hardware de Fechadura Inteligente

3.4. Modelo da Base de Dados

Para suportar as funções e operações do sistema, acima abordadas, este trabalho precisa de ter um modelo de dados sólido. O modelo de dados tem a capacidade de armazenar diferentes tipos de dados com diferentes propósitos e funções em todas as operações do sistema. Nesta secção são detalhados e descritos os diferentes conjuntos de dados que são necessários para o sistema funcionar como descrito anteriormente nas secções 3.2 e 3.3.

Tabela de dados Utilizadores - Armazena os dados pessoais de todos os utilizadores do sistema. Cada utilizador é identificado pelo seu número único de estudante/docente e os dados pessoais são compostos pelo nome, apelidos, mail e palavra-passe.

Tabela de dados Admin - Armazena as duas funções diferentes do sistema, utilizador normal ou administrador do sistema. Esta tabela está ligada diretamente à tabela "Utilizadores" para identificar a função de cada utilizador.

Tabela de dados Chaves - Garante que todos os pedidos feitos no sistema sejam conectados à fechadura do cacifo correcto. Isto é garantido gerando um ID exclusivo para cada acesso a um cacifo que possa existir na rede e que identifica o hardware físico daquela utilização. Assim, evita que os utilizadores se cruzem com outras fechaduras inteligentes às quais não devem ter acesso, pois os pedidos são direcionados apenas para um cacifo específico. Esta tabela é composta por um ID de cacifo que identifica o hardware de fechadura inteligente e uma variável que armazena o nome do cacifo. Esta tabela está ligada diretamente às tabelas “Pedido Acesso” e “Actividade”.

Tabela de dados Pedido Acesso - Recebe uma entrada sempre que é feito um pedido de acesso por um utilizador registado e, como o pedido de acesso, após aceite, é válido apenas por um curto período de tempo, a tabela é usada principalmente para verificar se o pedido de acesso expirou ou não. A tabela é composta por um ID de acesso, uma variável *datetime* que armazena a data e a hora em que o pedido foi feito e conecta-se às tabelas Utilizador e Chaves para associar o pedido a um utilizador e uma chave específicos.

Tabela de dados Actividade - Tem como principal tarefa guardar todo o histórico de actividades do utilizador. Para tal, essa tabela armazena a data e a hora da primeira acção de desbloqueio (abrir o cacifo para colocar bens) e da segunda acção de desbloqueio (abrir o cacifo e retirar bens). Isso faz com que fiquem guardadas as datas de check-in e check-out de cada utilização. Esta tabela está ligada à tabela "Utilizadores" e "Chaves" para designar o utilizador que acedeu, e o cacifo associado a cada utilização.

4. Implementação do Sistema

Este capítulo descreve o desenvolvimento do sistema em termos de segurança, hardware, atribuição de cacifo e implementação dos diferentes módulos.

A **Secção 4.1** apresenta o desenvolvimento do Sistema de Gestão e todas as funcionalidades que são executadas na plataforma *cloud*.

A **Secção 4.2** é focada na atribuição de cacifo e desenvolvimento das funções para *smartphone*.

4.1. Sistema de Gestão

O Sistema de Gestão é desenvolvido dentro da plataforma *cloud*.

Esta secção descreve o desenvolvimento do sistema para entender completamente o que acontece por trás do sistema de gestão, dividindo a secção em três partes: a base de dados da cloud, pedidos de acesso e comunicações do sistema e segurança do sistema.

Quando um utilizador executa uma acção de desbloqueio e abertura de cacifo, um novo registo é criado na tabela Actividade para check-in de utilizador num determinado cacifo.

Na segunda vez que o utilizador executa uma acção de desbloqueio e abertura de cacifo, um novo registo é criado na tabela Actividade para check-out desse mesmo cacifo deixando o cacifo disponível para nova utilização por outro (ou o mesmo) utilizador.

4.1.1. Base de Dados da *Cloud*

As soluções apresentadas para plataformas *cloud* em 2.2.2 incluem um período de teste gratuito com movimentos GET e POST limitados, com a AWS e a IBM *Cloud* oferecendo o maior número desses movimentos.

Considerando a pesquisa feita sobre essas tecnologias e também a qualidade / quantidade de suporte online para iniciantes em cada uma das soluções apresentadas, foi selecionada a plataforma *cloud* Amazon *Web Services* para este projecto.

Os algoritmos executados no servidor dedicado na plataforma *cloud* da Amazon *Web Services* são responsáveis por manter todo o sistema em funcionamento e, ao mesmo tempo, por uma conexão estável que permite que os dados fluam pelo sistema.

A base de dados em *cloud* do sistema é uma parte importante deste trabalho, pois funciona como suporte de muitas das funções do sistema.

A base de dados do sistema é construída em SQL (*Structured Query Language*), utilizada para armazenar e manipular dados de bases de dados e é hospedada no servidor na plataforma *cloud* da AWS.

As tabelas da base de dados e o modelo relacional foram construídos com as especificações do sistema em mente. O modelo relacional da base de dados desenvolvido para este trabalho é o mostrado na **figura 13**.

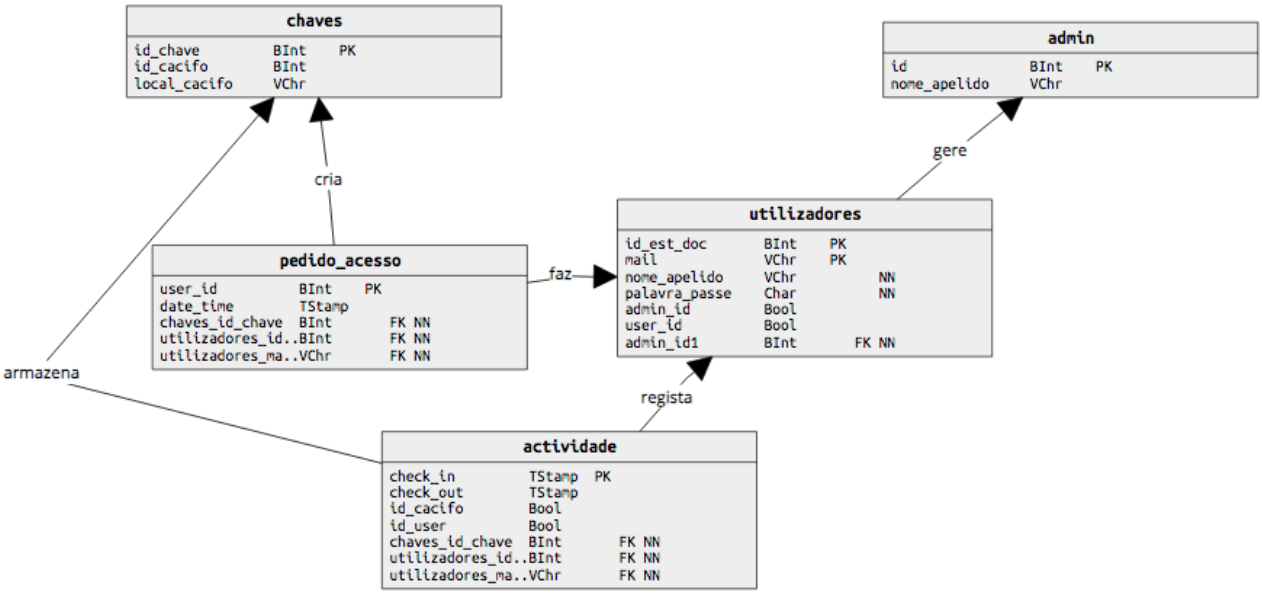

Figura 13: Modelo Físico Relacional de Dados

A tabela Utilizadores serve para guardar os dados pessoais dos utilizadores com foco nas variáveis ID de estudante/docente e mail que identificam cada utilizador.

Cada uma dessas variáveis é definida como Chave Primária (PK) para que o valor que elas guardem seja exclusivo.

O ID de Admin é uma Chave Estrangeira (FK) nesta tabela para que o sistema possa identificar o utilizador como um utilizador normal ou um administrador do sistema. Esta identificação é feita com dois valores possíveis, zero ou um.

A tabela Utilizadores está conectada a quase todas as outras tabelas da base de dados.

Um utilizador pode ser utilizador normal ou utilizador administrador e pode haver mais do que um utilizador com função de Administrador.

Tem também um relacionamento "um-para-muitos" com as tabelas "pedido_acesso" e "actividade" que permite ligar cada utilizador às acções realizadas e, consequentemente, guardadas na base de dados.

Na tabela "pedido_acesso" são guardados todos os pedidos de desbloqueio feitos pelos utilizadores por meio da aplicação para *smartphone* ou cartão RFID.

Está ligada à tabela "utilizadores" para identificar quem fez o pedido e apenas regista os dados se o utilizador abrir a porta do cacifo no curto espaço de tempo a definir. Caso contrário o pedido de acesso expira e é apagado o registo da tabela.

Essa tabela também é conectada à tabela "chaves" a fim de identificar, por meio do ID de Chave FK, a fechadura inteligente para o qual a solicitação foi feita.

Esta tabela também apresenta uma variável "*datetime*", para verificar se a solicitação de desbloqueio ainda é válida ou não. Isto evita que o hardware da fechadura inteligente execute a acção de desbloqueio de pedidos de acesso antigos.

A tabela "actividade" é semelhante à tabela "pedido_acesso", mas só guarda as acções de desbloqueio, quando são seguidas por uma acção de abertura de porta (lida pelo sensor).

Esta tabela apresenta a mesma FK que a anterior para identificar o utilizador que realizou a acção de desbloqueio e abertura e também para identificar o cacifo que foi usado.

Esta tabela tem uma variável chamada "check_in" para guardar a data e hora em que a acção de abertura de cacifo atribuído foi feita e uma variável de "check_out" que guarda a segunda acção de abertura de cacifo (para retirar bens guardados), conforme explicado em **4.1.**

Após um utilizador fazer um segundo acesso e realizar a abertura do cacifo, este deixa de estar atribuído a esse mesmo Utilizador (registo na tabela "actividade" de check-out).

4.1.2. Solicitações e Comunicações do Sistema

As solicitações do sistema são essenciais para as comunicações e interacções dos módulos do sistema.

As comunicações com o sistema são o suporte para funções como quando um utilizador faz login ou desbloqueia a porta por meio da aplicação ou do leitor central ou mesmo quando o hardware da fechadura inteligente notifica a plataforma de *cloud* que a

porta foi aberta para registrar uma nova acção de desbloqueio e acesso de um utilizador na base de dados da *cloud*.

Solicitações HTTP são usadas para estabelecer a comunicação entre cliente e servidor e possuem vários métodos diferentes. Essas solicitações do sistema são baseadas nos métodos GET e POST.

O método GET como a função para solicitar dados, enquanto o método POST tem a função de enviar dados. (“HTTP Methods GET vs POST,” n.d.)

Existem solicitações HTTP envolvidas em quase todas as acções do sistema. Essas solicitações são descritas nesta secção.

4.1.2.1. Solicitações Relacionadas com o Utilizador

Criar Utilizador Na aplicação - essa solicitação POST é accionada quando um novo registo de utilizador acontece na aplicação do *smartphone*. Os dados inseridos no registo na aplicação são enviados para a *cloud*. Uma verificação de existência de mail e ID de estudante/docente é feita na base de dados do utilizador para evitar o registo em duplicado. Se o ID de estudante/docente e mail não existir, uma nova entrada na tabela da base de dados Utilizadores é criada com os dados que foram enviados para a *cloud* por meio dessa solicitação e aguarda uma validação por parte de um administrador (para comprovar a existência desse ID de estudante/docente.

```
-insert into Utilizadores (ID_est_doc,
Palavra_passe,mail,Nome_Apelido, Utilizador_Normal, User_Admin) values
('".$newPalavra_passe."',
'".ID_est_doc."','".$mail."','".$Nome_Apelido."',".$Utilizador_Normal."
,".$User_Admin.");
```

Login - O login acontece quando o utilizador insere os dados (mail e palavra-passe) na aplicação de *smartphone* e pressiona o botão Entrar. Depois disso, as credenciais são enviadas, com o método POST para a *cloud* por meio de uma Solicitação de *token OAuth* (“Token Request - OAuth 2.0 Servers,” n.d.) que responde, se os dados corresponderem à base de dados, com um *token* de sessão que permitirá ao utilizador fazer pedidos de acesso e/ou ver o seu registo de actividade.

```
-select Palavra_passe from Utilizadores where Utilizadores.mail =\"".$mail.'"'.";
```

Obter/Editar informação do utilizador - essa solicitação GET é usada na aplicação de *smartphone* para mostrar os dados pessoais de registo do utilizador conectados no seu perfil da aplicação. A resposta dessa solicitação inclui o mail e palavra-passe do utilizador. Essa solicitação deve ser feita com o respectivo login activo do utilizador.

```
-update Utilizadores set mail =\"".$newmail."\" where Utilizadores.mail =\"".$oldmail.'"'.";

-update Utilizadores set Palavra_passe =\"".$newPalavra_passe."\" where  Utilizadores.mail =\"".$mail.'"'.";

=\"".$mail.'"'.";
```

Histórico de Actividade - essa solicitação GET é usada para recuperar todo o histórico de desbloqueios de fechaduras inteligentes associadas ao local e número de cacifo. Essa solicitação é feita após ter sessão iniciada na aplicação de *smartphone* e mostra as actividades do utilizador. Essa solicitação apresenta a data e hora da primeira abertura do cacifo(check-in), a data e hora da segunda abertura do cacifo (*check-out*), o ID do cacifo e local bem como o ID de estudante/docente e o seu mail. Esta solicitação requer um *token* de sessão para evitar que os utilizadores desconhecidos possam ter acesso aos dados do sistema.

```
-select accao from PedeAcesso where PedeAcesso.ID_est_doc =\"".$ID_est_doc.'"'.";
```

4.1.2.2. Solicitações Relacionadas com o Hardware da Fechadura Inteligente

Pedir Acesso a Cacifo/ Devolver Cacifo - Esta é a solicitação GET que é enviada através da aplicação de *smartphone* ou do painel central de cada vez que um utilizador deseja desbloquear um cacifo para o seu uso. Esta solicitação devolve um valor verdadeiro se o pedido de acesso for autorizado. Na aplicação de *smartphone*, é necessário um token de sessão iniciada e para uso do cartão RFID é necessário o registo prévio do ID do cartão para executar este pedido e evitar que pessoas não registadas obtenham acesso. O URL (Uniform Resource Locator) da solicitação necessita de ter o ID de Chave incluído para que a solicitação seja feita à fechadura correcta na segunda vez que o utilizador fizer o pedido (check-out). Na primeira solicitação é atribuido um ID de Chave ao utilizador que vai corresponder a um cacifo.

Porta aberta - Quando o hardware da fechadura inteligente é desbloqueado e detecta, através do sensor, que a porta foi aberta, é enviada essa informação para a *cloud* indicando que alguém abriu a porta do cacifo X e enviando o valor booleano verdadeiro. Depois disso, a *cloud* regista uma nova entrada na tabela "actividade" da base de dados com os dados do utilizador que fez o pedido de acesso e abriu a porta do cacifo atribuido no espaço de tempo definido previamente. Essa solicitação precisa do ID de Chave no URL do pedido para identificar a fechadura para o qual a solicitação foi feita e registada.

4.1.3. Segurança

Como já foi referido, as comunicações deste trabalho acontecem na web por meio de solicitações de HTTP. As solicitações HTTP fazem o transporte de dados, sendo necessário proteger os dados de ataques *malware*.

De modo a proteger os dados e adicionar uma camada de segurança às comunicações do sistema, pode ser usado o *OAuth* 2.0 como protocolo de autorização que vai ajudar o sistema a saber quem tem a autorização para fazer as solicitações necessárias para as comunicações.

O *OAuth* 2.0 é um protocolo padrão da indústria para autorização e comunicação

com o cliente e servidor. (“OAuth 2.0 — OAuth,” n.d.) Este protocolo mantém as comunicações necessárias neste trabalho com um maior nível de segurança indispensável no contexto da Internet das Coisas (IoT).

Quando um utilizador faz login na aplicação de *smartphone*, as suas credenciais são enviadas para a plataforma *cloud* que as valida ou não.

Se as credenciais do utilizador estiverem correctas, a plataforma da *cloud* reconhece que o utilizador efetuou login e, uma vez que a configuração do protocolo *OAuth* 2.0 está na *cloud*, é atribuido um *token* de acesso ao utilizador, conforme mostrado na **figura 14**, que estará presente em todas as solicitações feitas pelo utilizador a partir do momento em que inicia sessão.

Este *Token* de Acesso (ou *token* de sessão referido acima) tem a duração de uma hora em que o utilizador pode fazer quantas solicitações desejar. Após essa hora, o utilizador deve executar nova acção de login na aplicação de *smartphone*.

Este processo faz com que seja desnecessário enviar as credenciais do utilizador para cada acção solicitada e ajuda a identificar o utilizador que faz as solicitações porque cada chave é única.

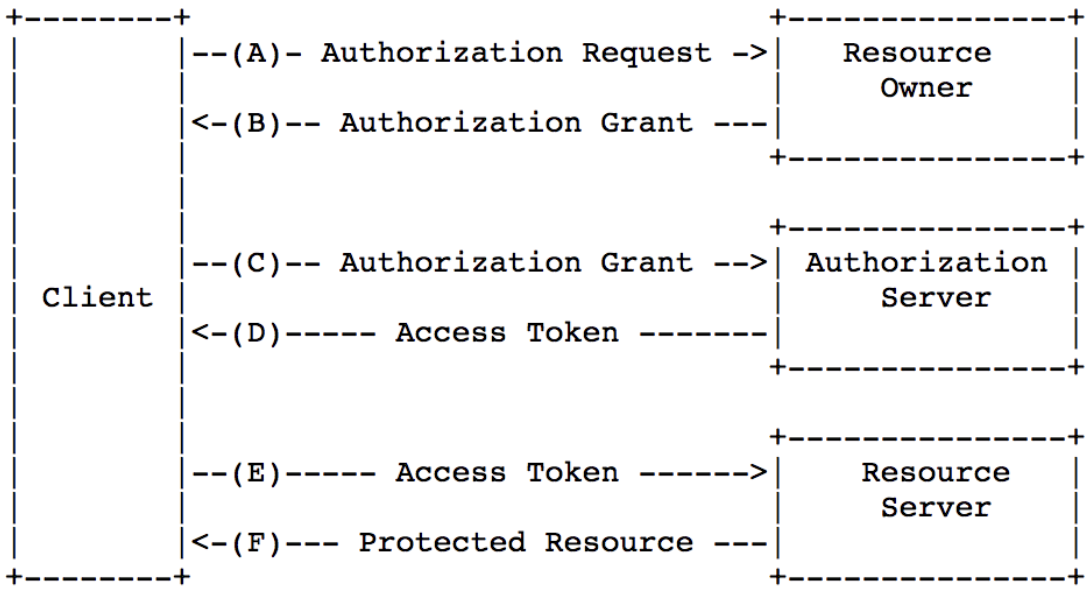

Figura 14: Fluxo do protocolo OAuth 2.0 retirado de (IETF 2012)

4.2. Atribuição de cacifo

Num edifício/departamento podem existir vários locais onde estão localizados os armários com diversos cacifos com um ID associado.

É necessário guardar o local do armário para facilitar a gestão. A informação dos edifícios (morada, nome e contacto, ID do edifício) no qual estão os armários de cacifos também tem de ser guardada.

Um utilizador que seja administrador poderá gerir os cacifos de vários edifícios e pode haver mais do que um administrador a gerir cacifos. No **anexo A** está o desenvolvimento das funções do Administrador tais como Adicionar/Apagar/Editar Edifícios/Departamentos, Armários de Cacifos, Consultar unidades de cacifos, e consultar o registos das acções dos utilizadores.

Os armários de cacifos estão em locais intuitivamente descritos (ex: LGE) e têm um determinado número de cacifos e um identificador único numérico.

Os cacifos têm um identificador numérico e um estado de disponibilidade. Cada cacifo pertence a um único armário. Cada cacifo pode ser usado por um utilizador de cada vez (uso pessoal).

As acções que serão registadas no histórico de actividade são pré-definidas e têm uma hora e data associada.

É possível observar as associações entre entidades na **figura 15**.

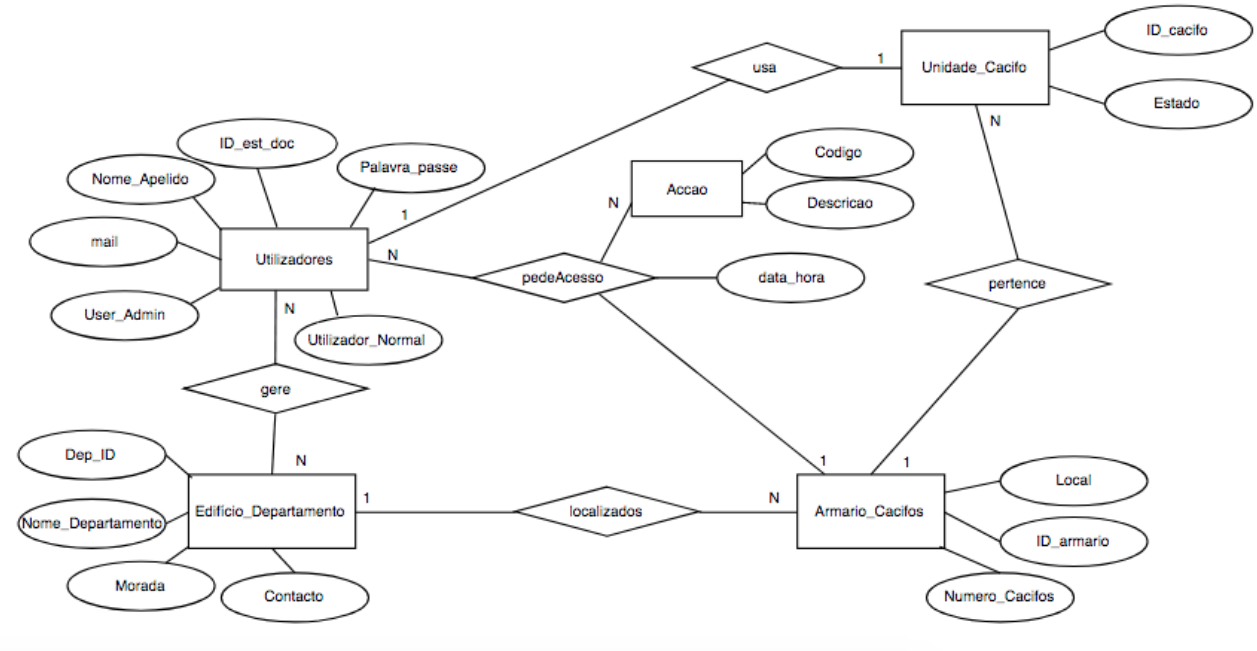

Figura 15 :Modelo Conceptual do Sistema

4.2.1. Modelo Relacional de Dados

Tendo por base o modelo conceptual acima apresentado, foi criado o modelo relacional dos dados e as dependências funcionais tendo em conta os requisitos funcionais do sistema.

Utilizadores(ID_est_doc, mail, Palavra_passe, Nome_Apelido, Utilizador_Normal, User_Admin);

ID_est_doc → mail, Palavra_passe, Nome_Apelido, Utilizador_Normal, User_Admin

Accao(Codigo, Descricao);

Codigo → Descricao

Unidade_Cacifo(ID_Cacifo, estado, *ID_armario*);

ID_Cacifo → estado, ID_armario

Armario_Cacifos(ID_armario, Numero_Cacifos, Local, *Dep_ID*);

ID_Unidade → Numero_Cacifos, Local, Dep_ID

Edificio_Departamento(Dep_ID, Morada, Nome_Departamento, *Contacto*);

```
 Dep_ID → Morada, Nome_Departamento, Contacto
usa(ID_est_doc,ID_Cacifo);
gere(ID_est_doc, Dep_ID);
pedeAcesso(ID_est_doc, Codigo, ID_armario, data_hora);
      ID_est_doc, ID_armario, data_hora →  Codigo
```

Tendo em conta as relações acima apresentadas, foram criadas as tabelas para obter o esquema físico do sistema de gestão desenvolvidas no **anexo B.**

5. Conclusão

Este capítulo apresenta o desenvolvimento e os resultados deste projecto. Uma abordagem de trabalho futuro também é feita para ajudar outros a desenvolver novos projectos de *Internet das Coisas* (IoT) e Fechaduras Inteligentes baseados neste trabalho.

5.1. Conclusões

Este trabalho apresenta um sistema de gestão de fechaduras inteligentes, baseado nas tecnologias Wi-Fi e RFID, que foi desenvolvido com o objectivo de ajudar um administrador do sistema a gerir melhor as actividades dos utilizadores de cacifos presentes em vários locais de uma universidade.

O sistema é fiável e seguro, fornecendo aos utilizadores do sistema um conjunto de recursos úteis que estão de acordo com o que é realmente usado nos produtos de fechaduras inteligentes disponíveis no mercado.

Apesar do facto deste projecto ser focado no histórico de acessos dos utilizadores, abre a possibilidade de criar tipos de notificações com base nos dados adquiridos pelo sistema.

As comunicações mantidas entre a plataforma de *cloud*, os dispositivos de autenticação do sistema e o hardware de fechadura inteligente são executadas através do protocolo HTTP e, embora todas as solicitações HTTP sejam protegidas pelo *OAuth 2.0*, definido como padrão de autorização actualmente, são ainda vulneráveis.

Tal indica que as comunicações do sistema precisam de uma melhoria clara de segurança para proteger os dados que transferem. O sistema gere os pedidos de acesso provenientes da aplicação de *smartphone* e dos cartões universitários RFID, armazena os dados gerados pela actividade e gera chaves novas para cada acesso a cacifo. Todas as

comunicações têm de passar pela *cloud*.

O hardware do sistema desempenha o papel de fechadura inteligente em si. O sistema funciona correctamente ao registar as actividades do utilizador com o sensor de posição da porta.

O uso dos cartões universitários como dispositivo de autenticação do sistema tem a capacidade de integração com outros servidores/*clouds*, como o controlo de acesso a edifícios/departamentos, de modo a criar uma solução de sistema mais inovadora e completa.

Apesar do facto de que o hardware de fechadura inteligente desempenha um papel importante no sistema, é muito simples fazer a sua aplicação num conjunto de cacifos, mas devido a restrições de tempo, nenhum desenvolvimento adicional foi feito no hardware.

Em relação a custos, o preço estimado de hardware de fechaduras inteligentes para um armário de 50 cacifos e sistema de gestão/serviço da plataforma *cloud* de acordo com o analisado, será de aproximadamente 1185€. Este valor estimado é muito inferior ao valor das soluções existentes no mercado.

5.2. Trabalho Futuro

Este trabalho tem muitas maneiras de melhorar e de ser concluído. Para começar, as solicitações do sistema devem tornar-se mais seguras implementando o HTTPS (*Hypertext Transfer Protocol Secure*) com o qual todas as comunicações do sistema são criptografadas. Infelizmente, devido restrições de tempo, o fluxo de comunicação não foi implementado no sistema.

Depois de tornar as comunicações mais seguras entre todos os módulos do sistema, o foco deve estar nos algoritmos de notificação. Há muitas possibilidades para gerar conjuntos de notificações, desenvolvendo novos algoritmos que retornariam saídas diferentes como a notificação de uso por mais de determinado tempo. O administrador do sistema deverá poder selecionar quais tipos de notificações deseja receber ou até mesmo

definir regras para essas notificações. Isso permitiria ao administrador do sistema obter controlo do sistema sobre as suas preferências.

A aplicação de *smartphone* deverá ser desenvolvida com as especificações descritas no projecto. O software mais apropriado para o seu desenvolvimento deverá ser estudado de acordo com os recursos necessários para a implementação deste sistema.

Referências

"Amazon Web Services (AWS) - Cloud Computing Services." URL: https://aws.amazon.com/

Basha, S. Nazeem, S.A.K Jilani, and S Arun. 2016. "An Intelligent Door System Using Raspberry Pi and Amazon Web Services IoT." *International Journal of Engineering Trends and Technology* 33 (2): 84–89. https://doi.org/10.14445/22315381/ijett-v33p217.

Bonaventure, Menezes Allwyn, S Priyadarshini, Sindhu Nayak, and A Ushadevi. 2017. "Smart Key : Secure Door Lock System Using NFC Enabled Smartphone" 6 (2): 67–70. https://doi.org/10.5923/j.ijit.20170602.12.

"Easy IoT." URL: https://iot-playground.com/

Effect, Hall. 1940. "SENSOR vs . HALL EFFECT Reed Sensors vs . Hall Effect Sensors," 37–39. URL: https://standexelectronics.com/resources/technical-library/technical-papers/reed-sensors-vs-hall-effect-sensors/

"Google Cloud Computing, Hosting Services & APIs | Google Cloud Platform." URL: https://cloud.google.com/

"HTTP Methods GET vs POST." URL: https://www.w3schools.com/tags/ref_httpmethods.asp

"IBM Cloud." URL: https://ibm.com/cloud/

IETF. 2012. "RFC6749-The.OAuth.2," 1–76. ISSN: 2070-1721. URL: http://www.rfc-editor.prg/info/rfc6749

Kassem, Abdallah, Sami El Murr, Georges Jamous, Elie Saad, and Marybelle Geagea. 2016. "A Smart Lock System Using Wi-Fi Security." *2016 3rd International Conference on Advances in Computational Tools for Engineering Applications, ACTEA 2016*, 222–25. https://doi.org/10.1109/ACTEA.2016.7560143.

"Magnetic Contact Switch (Door Sensor)." URL: https://www.adafruit.com/product/375

"OAuth 2.0 — OAuth." URL: https://oauth.net/2/

Pandit, Varad, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga, and Sachin Bojewar. 2018. "Intelligent Security Lock." *Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017* 2018-Janua: 713–14. https://doi.org/10.1109/ICOEI.2017.8300795.

"Plataforma de Informática Na Cloud e Serviços Do Microsoft Azure." URL: https://azure.microsoft.com/pt/pt/

Pothuganti, Karunakar, and Anusha Chitneni. 2014. "A Comparative Study of Wireless Protocols :" *IECON Proceedings (Industrial Electronics Conference)*, no. January 2014: 46–51. https://doi.org/10.1109/IECON.2007.4460126

Prada-Delgado, M. A., A. Vázquez-Reyes, and I. Baturone. 2016. "Physical Unclonable Keys for Smart Lock Systems Using Bluetooth Low Energy." *IECON Proceedings (Industrial Electronics Conference)*, 4808–13. https://doi.org/10.1109/IECON.2016.7792955.

Prakash, Y. W., Vishakha Biradar, Shenil Vincent, Minto Martin, and Anita Jadhav. 2018. "Smart Bluetooth Low Energy Security System." *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017* 2018-Janua: 2141–46. https://doi.org/10.1109/WiSPNET.2017.8300139.

Reinisch, W. Kastner, G. Neugschwandtner and W. Granzer. 2007. "Wireless Communication in Home and Building Automation," 2007 Technische Universitat Wien

Roorda, Peter David, Ottawa Ca, Kevan Peter Jones, Kanata Ca, Peter Friesen, Ottawa Ca, Ulllted States Patent, et al. 2007. "REDES SEM FIOS(WIRELESS) E PROTOCOLOS PARA COMUNICAÇÃO DE IEDS DE SISTEMAS DE MEDIÇÃO, PROTEÇÃO, COMANDO, CONTROLE E SUPERVISÃO (MPCCS) EM USINAS E SUBESTAÇÕES DE 500/230KV." *SNPTEE, SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA*, 2007. https://doi.org/10.1590/s1809-98232013000400007.

Sarp, Burak, Netas Company, Kurtkoy, Istanbul, and TURKEY. 2015. "Real Time Smart Door System for Home Security." *International Journal of Scientific Research in Information Systems and Engineering (IJSRISE)* 1 (2).

Sayar, Abhilasha A, and Sunil N Pawar. 2016. “Review of Bank Locker System Using Embedded System.” *International Journal of Advanced Research in Computer and Communication Engineering* 5 (2): 282–85. https://doi.org/10.17148/IJARCCE.2016.5258.

Sousa, Pedro Jose, Rafael Tavares, Paulo Abreu, Manuel Quintas, Ana Reis, and Maria Teresa Restivo. 2016. “Wireless Control and Network Management of Door Locks.” *Exp.at 2015 - 3rd Experiment International Conference: Online Experimentation*, 141–42. https://doi.org/10.1109/EXPAT.2015.7463244.

Sunny, S M Nahian Al. n.d. “NFC Smart Locker System,” 1–4. URL: http://csce.uark.edu/~ahnelson/CSCE5013/reports/SunnyNahian.pdf.

“Token Request - OAuth 2.0 Servers.” URL: https://www.oauth.com/oauth2-servers/device-flow/token-request/

Urien, Pascal. 2014. “A Secure Cloud of Electronic Keys for NFC Locks Securely Controlled by NFC Smartphones.” *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, 1120–21. https://doi.org/10.1109/CCNC.2014.6994415.

Verma, Gyanendra K, and Pawan Tripathi. 2010. “A Digital Security System with Door Lock System Using RFID Technology.” *International Journal of Computer Applications* 5 (11): 6–8. https://doi.org/10.5120/957-1334.

Yunge, Daniel, Philipp Kindt, Michael Balszun, and Samarjit Chakraborty. 2015. “Hybrid Apps: Apps for the Internet of Things.” *Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, H*, 1175–80. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.292.

Anexo A

Funções de um Administrador:

Adicionar/Apagar/Editar Edifícios/Departamentos:

```
-update Edificio_Departamento set
Nome_Departamento='".$_Nome_Departamento."', Morada='".$_Morada."',
Contacto=".$_Contacto." where Dep_ID = ".$_id.";
```

```
-insert into Edificio_Departamento (Nome_Departamento, Morada,Contacto)
values ('".$Nome."','".$Morada."',".$Contacto.");
```

```
-select * from Edificio_Departamento where Dep_ID=".$id.";
```

```
-delete from Edificio_Departamento where Dep_ID=".$id.";
```

Adicionar/Editar/Apagar Armários de Cacifos:

```
-update Armario_Cacifos set Numero_Cacifos=".$_capacity.”,
Local='".$_Local." Dep_ID=".$_id_dep." where ID_armario = ".$id.";
```

```
-insert into lockerUnits (NumberOfCells,IDShop) values
(".$capacity.",".$IDShop.");
```

```
-select * from Armario_Cacifos where ID_armario=".$id.";
```

```
-delete from Armario_Cacifos where ID_armario=".$id.";
```

Consultar unidades de cacifos:

```
-select ID_cacifo, Estado, Edificio_Departamento.Nome as DepNome from
Unidade_Cacifo join Armario_Cacifos join Edificio_Departamento where
Unidade_Cacifo.ID_cacifo = Armario_Cacifos.ID_armario and
Armario_Cacifos.Dep_ID = Edificio_Departamento.Dep_ID;
```

Consultar o registos das acções dos utilizadores:

```
-select * from pedeAcesso;
```

Anexo B

```
CREATE TABLE Utilizadores (
    ID_est_doc INT UNIQUE PRIMARY KEY,
    mail VARCHAR(40) UNIQUE,
    Palavra-passe VARCHAR(30),
    Nome_Apelido VARCHAR(40),
    Utilizador_Normal BOOL,
    User_Admin BOOL
);
CREATE TABLE Accao (
    Codigo INTEGER UNIQUE PRIMARY KEY AUTO_INCREMENT,
    Descricao VARCHAR(140)
);
CREATE TABLE Unidade_Cacifo(
    ID_Cacifo INTEGER UNIQUE PRIMARY KEY AUTO_INCREMENT,
    Estado BOOL,
    ID_armario INTEGER,
    FOREIGN KEY (ID_armario) REFERENCES Armario_Cacifos (ID_armario) ON
DELETE CASCADE
);
CREATE TABLE Armario_Cacifos (
    ID_armario INTEGER UNIQUE PRIMARY KEY AUTO_INCREMENT,
    Numero_Cacifos INTEGER,
    Local VARCHAR(40) UNIQUE,
    Dep_ID INTEGER,
    FOREIGN KEY (Dep_ID) REFERENCES Edificio_Departamento (Dep_ID) ON
DELETE CASCADE
);
CREATE TABLE Edificio_Departamento (
    Dep_ID INTEGER UNIQUE PRIMARY KEY AUTO_INCREMENT,
    Morada VARCHAR(140),
    Nome_Departamento VARCHAR(50),
    Contacto INTEGER UNIQUE
```

```
);
CREATE TABLE usa (
    ID_est_doc INTEGER,
    ID_cacifo INTEGER,
    PRIMARY KEY (ID_est_doc , ID_cacifo),
    FOREIGN KEY (ID_est_doc) REFERENCES Utilizadores (ID_est_doc) ON
DELETE CASCADE,
    FOREIGN KEY (ID_cacifo) REFERENCES Edificio_Departamento (Dep_ID)
ON DELETE CASCADE
);
CREATE TABLE gere (
    ID_est_doc INTEGER,
    Dep_ID INTEGER,
    PRIMARY KEY (ID_est_doc , Dep_ID),
    FOREIGN KEY (ID_est_doc) REFERENCES Utilizadores (ID_est_doc) ON
DELETE CASCADE,
    FOREIGN KEY (Dep_ID) REFERENCES Edificio_Departamento (Dep_ID) ON
DELETE CASCADE
);
CREATE TABLE pedeAcesso (
    ID_est_doc INTEGER,
    Codigo INTEGER,
    ID_armario INTEGER,
    data_hora TSTAMP,
    PRIMARY KEY (ID_est_doc , ID_armario , data_hora),
    FOREIGN KEY (ID_est_doc) REFERENCES Utilizadores (ID_est_doc) ON
DELETE CASCADE,
    FOREIGN KEY (Codigo) REFERENCES Accao (Codigo) ON DELETE CASCADE,
    FOREIGN KEY (ID_armario) REFERENCES Armario_Cacifos (ID_armario) ON
DELETE CASCADE
);
```