CENTRO UNIVERSITÁRIO DE ANÁPOLIS – UniEVANGÉLICA

BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

GLEISON DE JESUS SILVA

TIAGO DOS SANTOS SOARES

AMBIENTE SEGURO UTILIZANDO INTERNET DAS COISAS

ANÁPOLIS

2018-02

GLEISON DE JESUS SILVA

TIAGO DOS SANTOS SOARES

AMBIENTE SEGURO UTILIZANDO INTERNET DAS COISAS

Trabalho de Conclusão de Curso II apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso II do curso de Bacharelado em Engenharia de Computação do Centro Universitário de Anápolis – UniEVANGÉLICA.

Orientador(a): Prof. Me. Alexandre Moraes Tannús

ANÁPOLIS

2018-02

GLEISON DE JESUS SILVA

TIAGO DOS SANTOS SOARES

AMBIENTE SEGURO UTILIZANDO INTERNET DAS COISAS

Trabalho de Conclusão de Curso II apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso II do curso de Bacharelado em Engenharia de Computação do Centro Universitário de Anápolis – UniEVANGÉLICA.

Aprovados pela banca examinadora em [dia] de [mês] de 2018, composta por:

_____

Prof. Me. Alexandre Moraes Tannús.
Orientador

_____

_____

Resumo

Este trabalho de conclusão apresenta um modelo de segurança para garantir um ambiente seguro utilizando os conceitos de Internet das Coisas. Ambiente que nesse trabalho será utilizado o de um automóvel, e ficará claro que poderá ser utilizado em qualquer outro ambiente que necessite de controle, registro e análise de dados, e/ou monitoração. Com uma arquitetura que utiliza os conceitos de Internet das Coisas, o modelo também utiliza *softwares* e *hardwares open source*, como o microcontrolador ESP8266 e o protocolo de comunicação MQTT. O sistema é uma sugestão para o universo tecnológico manter ambientes seguro utilizado o paradigma de *IoT.*

Palavras-chave: Internet das Coisas, modelo de segurança, ambiente, Safecar, automóvel.

Lista de Figuras

Lista de Abreviações

COAP - Constrained Application Protocol

EPC - Eletronic Product Code

GPIO - General Purpose Input/Output

HTTP - Hypertext Transfer Protocol

ID - Identificador

IoT - Internet Of Things

IEEE - Institute of Eletrical and Eletronic Engineers

MAC - Media Access Control

MQTT - Message Queuing Telemetry Transport

M2M - Machine-to-Machine

OBD - ON Board Diagnostic

RAM - Random Access Memory

RFID - Radio-Frequency IDentification

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

WLAN - Wireless Local Area Network

Lista de Tabelas

Sumário

1 Introdução

O mundo tem experimentado uma revolução tecnológica, e um novo paradigma vem conduzindo essa revolução em passos largos, o da Internet das Coisas. Internet das Coisas, do inglês *Internet of Things - IoT*, é um paradigma que integra um mundo de objetos físicos embarcados com sensores e atuadores, conectados por redes sem fio e que se comunicam utilizando a internet, criando uma rede de objetos inteligentes capazes de realizar variados processamentos, capturar variáveis ambientais e reagir a estímulos externos, (ATZORI et al. 2010).

Nesse contexto de inovação e adaptação, pode-se trabalhar em diversos campos de aplicação relacionados a *IoT*. Porém coloca-se em destaque nesse trabalho a necessidade de garantir ambientes seguros, por meio de um modelo de segurança. Um modelo que utiliza microcontrolador, comunicação sem fio, sensores, atuadores, memória e processamento e um software de gestão.

Modelos elevam o nível de abstração do desenvolvimento de sistemas, ajudando no planejamento e entendimento dos mesmos, sendo que a importância do uso de modelos no desenvolvimento de software é um fato comprovado (PRESSMAN, 2001; SELIC, 2003). Sendo assim, o trabalho trata todo o sistema como um modelo de segurança a fim de consolidar a abstração do conjunto hardware, software, protocolo de comunicação e dispositivos *IoT*.

Com o crescimento da *IoT*, cresce também a preocupação com a segurança em geral, pois o volume de transmissão de dados é gigantesco, e fica claro que pode-se utilizar desses dados para diversas aplicações, como controle e/ou monitoração de um ambiente qualquer (CISCO IBSG, 2011).

Todos os dias as pessoas utilizam seus dispositivos móveis em uma rede sem fio, ou seja, em casa, no shopping, no trabalho ou na faculdade, elas estão sempre conectadas, disponibilizando assim diversos dados pessoais e do ambiente em que estão interagindo. Essa conexão constante de objetos e pessoas, possibilita desenvolver aplicações que garantam um ambiente mais seguro. Um ambiente em que seja possível controlar acesso, registrar e analisar dados e monitorar ambiente. Por isso, em poucos anos a sociedade estará

envolvida por cidades inteligentes, saúde conectada, agricultura automatizada, indústria robotizada, enfim diversos campos de aplicação conectados entre si, gerando dados de tudo e de todos, (LACERDA; LIMA – MARQUES, 2015), os quais podem ser facilmente integrados às aplicações que podem garantir um ambiente seguro e controlado.

Em meio a essa revolução, existe a necessidade de controlar e monitorar acesso de pessoas em ambiente não autorizados, acompanhar em tempo real diversas atividades, registrar e analisar dados, dentre várias outras ações que podem impactar na segurança de um ambiente. Como a sociedade de forma automática já está muito conectada, nota-se que, utilizando de forma adequada alguns elementos, é possível monitorar, controlar acesso, registrar dados dentre diversas outras funcionalidades. Sendo assim, existe a necessidade de garantir ambientes seguros utilizando conceitos de *IoT*.

A CISCO (CISCO IBSG, 2011) estima que a quantidade de dispositivos conectados em 2020 será em torno de 50 bilhões para uma população mundial de 7,6 bilhões, chegando a marca de 6,58 dispositivos conectados por pessoa. Esta conectividade entre os mais variados objetos do dia a dia com a web, de eletrodomésticos a equipamentos mais sofisticados é o conceito de *IoT*. Contudo, traz aos profissionais de computação novos desafios.

Com toda essa conectividade é importante que tenha um modelo de segurança que valide e autentique o usuário de forma automatizada. Por exemplo, em um ambiente que necessite de controle de acesso, o usuário poderia ser identificado e autorizado por um sistema através de seu dispositivo móvel conectado na rede sem fio daquele ambiente, com a finalidade de controlar e monitorar o acesso.

Como os dispositivos móveis, sejam eles celulares, relógios, pulseiras, *wearable*, dentre outros se tornaram praticamente uma extensão do corpo humano, permitindo-lhe a capacidade de se conectar, (BAUMAN, 2004), por que não utilizar dessa ferramenta para criar um modelo de segurança? Um modelo que utilize a premissa de que o dispositivo móvel se conecta diariamente nas mesmas redes sem fio, em casa, no trabalho ou na faculdade.

Enfim, para materializar o modelo citado em um ambiente específico, foi escolhido o automóvel, o qual terá o modelo de segurança embarcado em si. Enfrentar o desafio de trabalhar com o modelo de segurança em um ambiente menor e que se movimenta, e ter a facilidade de embarcar o sistema por já existir fonte de alimentação e espaço para instalar os componentes são motivos para escolha de um automóvel como ambiente a ser testado.

Dessa forma, o objetivo geral do trabalho é implementar um modelo de segurança em um determinado ambiente. Utilizando uma arquitetura com os conceitos de *IoT*, a qual realiza a autenticação e a validação do usuário de forma automatizada, por meio do sistema e seu dispositivo móvel e registra dados necessários do ambiente. Para atingir o objetivo esperado existem os seguintes objetivos específicos:

1 – Construir um modelo de segurança utilizando conceitos de *IoT*.
2 – Desenvolver um software de gestão, o Safecar, utilizando todas as fases de um processo de desenvolvimento de software.
3 – Aplicar o modelo de segurança em um automóvel.
4 – Identificar outros possíveis cenários de aplicação do modelo de segurança.

O trabalho está organizado em oito partes, as quais seguem com a fundamentação teórica, o desenvolvimento, que trata a construção do modelo de segurança juntamente com o desenvolvimento do software de gestão. No final um capítulo de possíveis cenários de aplicação e as considerações finais.

2 Fundamentação Teórica

A revolução tecnológica é clara quando se consegue refletir em anos anteriores, como se comunicava, como se utilizava a internet, como se realizava trabalhos, pesquisas, enfim, quando se consegue esse olhar crítico, fica fácil de visualizar esta revolução.

2.1 **Open Source**

Olhando dez anos atrás, seria impossível imaginar a revolução tecnológica que o mundo enfrenta atualmente. Não somente pela capacidade alcançada em diversas áreas, mas também pela acessibilidade deste avanço, ao ponto de acadêmicos fazerem parte dessa revolução, pois existe um universo *open source* que alavanca este crescimento. No desenvolvimento desse trabalho foram utilizadas diversas pesquisas e até utilização de bibliotecas nos programas, utilizando as comunidades *open sources* existentes, referentes a temática do trabalho.

Open source é um termo em inglês que significa software livre, o qual pode ser descrito como o *software* que pode ser utilizado, copiado, estudado e redistribuído, (CAMPOS, 2006). Esses códigos fontes podem ser obtidos através de plataformas na internet e tem sido a forma de avanço de diversos softwares. Por exemplo as distribuições linux, pois os *softwares* são desenvolvidos e atualizados por diversos colaboradores situados no mundo inteiro, normalmente sem custos financeiros.

A característica mais importante do software livre é a liberdade de uso, cópia, modificações e redistribuição (HEXSEL, 2002). Esta liberdade é conferida pelos autores do programa e é efetivada através da distribuição do código fonte dos programas, o que os transforma em bens públicos, disponíveis para utilização por toda a comunidade e da maneira que seja mais conveniente a cada indivíduo. Os benefícios do mundo *open source* são diversos, pois esse universo compartilhado de conhecimentos e experiências tem alavancado o desenvolvimento tecnológico e, assim como *software* livre tem uma parte

extremamente importante nesse desenvolvimento, existe também o *open source hardware* ou *hardware* de código aberto.

2.2 **Open Source Hardware**

Open source hardware são *hardwares* ou placas eletrônicas que tem seu projeto disponibilizado publicamente, cedendo a suas informações com a finalidade de serem utilizadas de forma livre. São fornecidos os diagramas, circuito impresso e dados técnicos em seus *datasheets*, (HARDWARE ABERTO, 2016).

O *hardware* de código aberto traz várias vantagens como concorrência em sua produção, o que acarreta mais qualidade e preços baixos para esses dispositivos e, a vantagem de se adaptar ao modelo de negócios. Pois empresas podem vender kits para a montagem de dispositivos compatíveis com Arduino, por exemplo. (MELLIS, 2009). No desenvolvimento desse trabalho serão utilizados *hardwares* e *softwares* de código aberto, como pode ser conferido na seção metodologia.

Continuando com a breve descrição do avanço tecnológico dos últimos anos, não é possível não destacar a evolução dos *smartphones*. Quando se fala em avanço tecnológico os *smartphones* são um bom exemplo, eles são caracterizados pelo acesso à internet, e também pelo sistema operacional e pelo poder de processamento que os capacitem a executar programas inviáveis em celulares sem tal estrutura, (UCEL, 2009).

2.3 **Smartphone**

Atualmente é visível que na sociedade o *smartphone* com valor agregado da marca ganha certa identidade pessoal, e acaba ocupando lugar de destaque na rotina da maioria das pessoas, pois permite, facilita e amplia a capacidade comunicativa do indivíduo (BACHA, SCHAUN, 2011).

O aparelho celular tornou-se fonte de entretenimento, e até uma forma de extensão da identidade do usuário (BECK et al., 2009). Assim, percebe-se que esses dispositivos alteraram o modelo convencional em que a sociedade se comunicava. Atualmente as pessoas

se conectam através de seus dispositivos móveis e redes sem fio, o que impactou não somente na forma de se comunicar, mas também a forma que o ser humano interage, se relaciona, executa tarefas, enfim, memória, processamento e conectividade na palma da mão alteraram o comportamento da sociedade atual.

Para (LEMOS, 2005) A incorporação de sistemas operacionais que permitiram aos celulares acesso e navegação à Internet banda larga sem fio tem redefinido os processos de interação entre homens e homens e homens e máquinas.

Atualmente todas faixas etárias utilizam *smartphones*, ícones de parte dessa revolução, os quais possibilitam uma comunicação muito diferente como a de dez anos atrás, pois hoje, através dos *smartphones*, a comunicação é realizada muito mais através de aplicações do que em ligações telefônicas. Esses dispositivos móveis, os *smartphones*, estão cada vez mais potentes em termos de processamento e memória. Podendo agora ser utilizados no dia a dia dos usuários para diversas finalidades, desde ligações até controles e monitoramento de atividades em suas residências.

Os *smartphones* estão no dia a dia de todos, sendo conectados em redes sem fios permitindo ao usuário navegar pelo mundo inteiro virtualmente. Como cita (BAUMAN, 2004) a revolução tecnológica, pela qual tem passado o telefone móvel, permite ao usuário um estado de permanente conexão entre indivíduos em movimento.

2.4 **Redes Sem Fio**

Sem dúvidas nenhuma grande parte do sucesso dos dispositivos móveis é a evolução das redes sem fio, que há dez anos atrás não era tão difundida como atualmente. A rede sem fio está em toda parte, na residência, no local de trabalho, nas escolas, nos shoppings, enfim, na cidade onde o usuário estiver com seu *smartphone*, provavelmente haverá uma rede sem fio.

As Redes sem fio ou wireless (WLANs - Wireless Local Area Network) surgiram da mesma forma que muitas outras tecnologias, no meio militar. Havia a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrito ao meio militar e

se tornou acessível a empresas, faculdades e ao usuário doméstico. Nos dias de hoje pode-se pensar em redes wireless como uma alternativa bastante interessante em relação as redes cabeadas. Suas aplicações são muitas e variadas e o fato de ter a mobilidade como principal característica, tem facilitado a sua aceitação, principalmente nas empresas. (FARIAS, 2005).

O uso desta tecnologia engloba desde transceptores de rádio até satélites no espaço. O uso mais comum é em redes de computadores, servindo como meio de acesso à internet, através de locais remotos como um aeroporto, um restaurante ou até mesmo em casa (BUSCH, 2008). Assim como já referenciado no texto, os dispositivos móveis e as redes sem fio são grandes agentes desta revolução tecnológica dos últimos dez anos. Estes agentes transformadores de paradigmas são partes também de uma nova revolução, a da Internet das Coisas, do inglês *Internet of Things – IoT*.

2.5 Internet Das Coisas Ou *Internet Of Things - IoT*

Relata-se que o termo Internet das Coisas ou *IoT* foi utilizado, foi em 1999, quando em uma palestra, Kevin Ashton explicava o potencial de uso das etiquetas de radiofrequência, RFID (Identificação por Rádio Frequência), (ASHTON, 2009).

Pode-se dizer que o RFID é um dos precursores de *IoT*, pois foi uma ferramenta muito importante para construção da Internet das Coisas, visto que é uma tecnologia de identificação automática tal como a de códigos de barra e leitores óticos. O RFID é um código eletrônico de produtos (*Electronic Product Code* - EPC) que define uma arquitetura de identificação, rastreamento e localização de produtos baseada em uma tecnologia de radiofrequência. (BERNADO, 2004).

Ao se utilizar o termo Internet das Coisas, ainda pode existir algumas variações no entendimento e caracterização do que realmente é Internet das Coisas ou *IoT*, na maioria das vezes, apenas pelo conceito de diferentes regiões do mundo. Na Europa e na China o termo Internet das Coisas é bem aceito, nos Estados Unidos as referências mais frequentes são *smart objects, smart grid e cloud computing*, (KRANENBURG et al, 2011). No Brasil, atualmente, tem-se utilizado o termo Internet das Coisas ou *IoT*.

Estima-se que o número de conexões móveis no mundo estará em torno de 50 bilhões no ano de 2020. Estão inclusos nessa estimativa *smartphones*, *tablets*, carros, acessórios de vestuários, eletrodomésticos, dentre outros objetos conectados. (PAIVA, 2015).

Com essa imensa revolução tecnológica, a qual bilhões de dispositivos estarão interagindo com o ambiente, utilizando memória e processamento, softwares e serviços de alguma forma integrados a si, será possível ouvir a batida do coração da terra. Mais uma vez impactando a interação humana com o globo de forma profunda, da mesma maneira que a internet revolucionou a comunicação, (EVANS, 2011).

Como a revolução tecnológica não tem fim, novamente o paradigma comportamental da sociedade está se alterando. A Internet das Coisas trará com diferentes aplicações a capacidade de observar, interagir, controlar, registrar as atividades de qualquer objeto, basta este objeto estar embarcado com sensores e atuadores, processamento e memória e se comunicar através de uma rede sem fio. A sociedade vive um novo paradigma no qual o usuário não controla mais o tempo, duração e local destinado ao uso do computador, agora processamento é em tempo real e distribuído no ambiente, (GREENFIELD, 2006).

O desenvolvimento de aplicações utilizando *IoT* ainda é novidade no Brasil, sendo utilizado normalmente em meio acadêmico e por empresas de tecnologias que tentam sair a frente desse mercado no país, porém muito voltado ainda para automação residencial, o que não pode ser a principal aplicação de *IoT*. Em países como China e Alemanha a Internet das Coisas faz parte do crescimento e desenvolvimento do país, como relatado por um economista norte-americano em uma entrevista concedida à revista Galileu em fevereiro de 2015. Para esse economista, (RIFIKIN, 2015), a Internet das Coisas vai atropelar o capitalismo até a metade do século e os países Alemanha e China serão as grandes potências da nova economia.

A Internet das Coisas desponta como uma evolução da internet e um novo paradigma tecnológico, social, cultural e digital. A Internet das Coisas revolucionará os modelos de negócios e a interação da sociedade com o meio ambiente, por meio de objetos físicos e virtuais, em que esses limites se tornam cada vez mais tênue, (LACERDA; LIMA – MARQUES, 2015).

Hoje o termo *IoT* no Brasil ainda é muito futurista em várias regiões desse país continental, porém quando se percebe a quantidade de equipamentos conectados já

existentes como televisões, vídeos games, câmeras de vigilância, eletrodomésticos e até mesmo pacotes de entregas sendo rastreados online, nota-se que a sociedade já está bastante envolvida com *IoT*.

A internet das coisas ou *IoT* é definida como a rede de objetos físicos que contém tecnologia embutida para se comunicar e sentir ou interagir com o ambiente externo ou com estados internos. Embutindo ou embarcando tecnologia com os dispositivos tecnológicos que existem atualmente, (GARTNER, 2017). Sendo assim, é possível criar várias aplicações em todas as áreas utilizando *IoT*, porém como já exposto, o propósito deste trabalho é além de tudo demonstrar as possibilidades de criar sistemas que possam garantir a segurança do usuário, criando ambientes seguros, de modo que um sistema inteligente possa monitorar e interagir com ações corriqueiras dos seres humanos.

Apesar de ainda não existir uma arquitetura padrão, a IEEE (*Institute of Eletrical and Eletronics Engineers*) com seus vários grupos de trabalho relacionados a *IoT*, existe um que está diretamente focado em Internet das Coisas, o IEEE P2413. O seu escopo é definir uma arquitetura estrutural da *IoT*, com seus domínios, abstrações e pontos comuns. Para esse grupo de trabalho a arquitetura se divide em apenas três camadas, a de Aplicações, Rede/Comunicação de Dados e Sensoriamento, como pode ser verificado na Figura 1 (FACCIONI, 2016).

Figura 1 - Arquitetura da IoT conforme IEEE P2413

Fonte: FACCIONI, 2016

2.6 Protocolo de Comunicação para *IoT*

Focando na camada de aplicação, a qual utiliza protocolos de serviço específico de comunicação de dados, nota-se que o protocolo de aplicação mais utilizado para prover serviços web é o HTTP do inglês *Hypertext Transfer Protocol*, (TORRES, 2001), porém possui muita complexidade computacional e consumo de energia elevado para os dispositivos *IoT*.

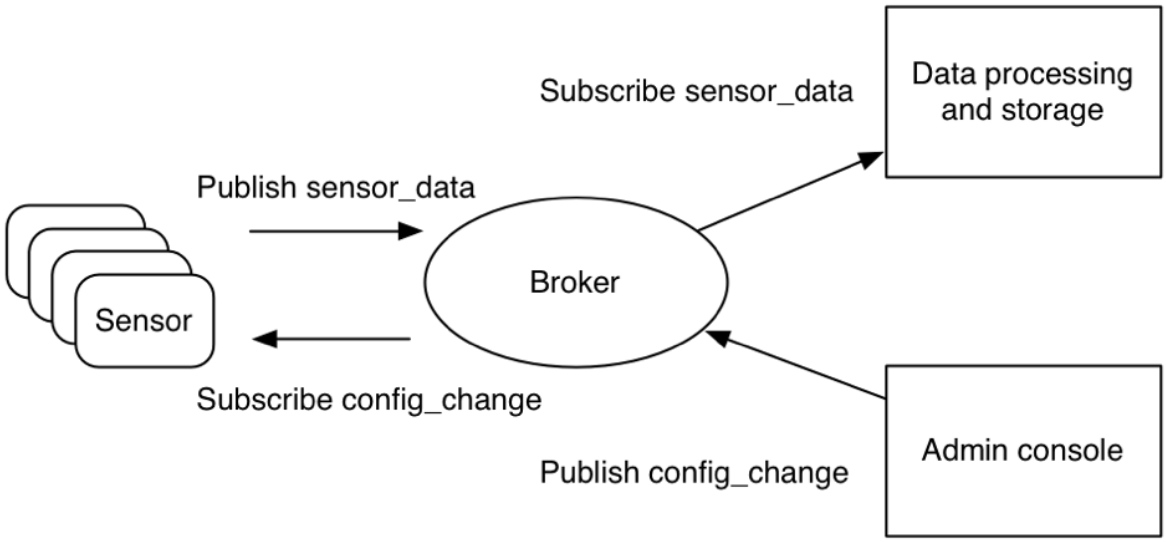
Sendo assim, segue a análise de dois protocolos da camada de aplicação, aparentemente mais utilizados até o momento no mundo da Internet das Coisas. Os dois apresentam características de baixo consumo, possuem mensagens pequenas, gerenciador de mensagens e pequeno *overhead*, ideal para utilização em sistemas embarcados, (STANSBERRY, 2015). O primeiro protocolo é o *Message Queuing Telemetry Transport* - MQTT, criado em 1999 pela IBM, vem ganhando espaço com o advento da Internet das Coisas. O segundo, *Constrained Application Protocol* - CoAP, foi criado em 2014 e foi desenvolvido especificamente para o mundo *IoT*.

2.6.1 Protocolo MQTT

Criado em 1999 pela IBM, MQTT (MQ *Telemetry Transport*), é um protocolo aberto de mensagens projetado para comunicações *machine-to-machine* - M2M, na qual deve lidar com alta latência, instabilidade na comunicação e baixa largura de banda, (IBM; Eurotech, 2010).

O protocolo segue o modelo cliente/servidor. Os dispositivos, microcontroladores e sensores são os clientes que se conectam a um servidor (*broker*) utilizando TCP (*Transmission Control Protocol*). As mensagens a serem transmitidas são publicadas para um endereço (tópico), que se assemelha a um endereço de pastas de um sistema operacional, por exemplo, safecar/telemetria/temperatura. Os clientes podem se subscrever para vários tópicos, tornando-se assim, capazes de receber as mensagens que outros clientes publicam nesse tópico, (JAFFEY, 2014). A Figura 2 mostra o funcionamento descrito do protocolo MQTT.

Figura 2 - Protocolo MQTT



Fonte: IBM, 2018.

2.6.2 Protocolo CoAP

O segundo protocolo de comunicação é o protocolo CoAP que contrasta com o MQTT, o CoAP roda em cima do UDP (*User Datagram Protocol*), também com arquitetura cliente/servidor. Seu foco está na interoperabilidade com a web, (BERGMANN, 2010).

Este protocolo em parte, é similar ao HTTP, porém, como os dispositivos de *IoT* normalmente operam com banda e energia limitadas, os pacotes do CoAP são muito menores. Bitmaps de strings até inteiros são usados extensivamente para economizar espaço. Os pacotes são passados *in place*, ou seja, no espaço de memória de um pacote anterior. Assim, há uma economia de RAM (*Random Access Memory*) nos dispositivos, (SHELBY, 2014).

A comunicação entre o cliente e servidor é feito a partir do sistema GET, PUT, POST e DELETE. Explicando um pouco sobre cada um deles:

- GET: pega o valor da informação desejada.

- PUT: O recurso especificado é modificado com a informação enviada. Caso o recurso não exista, é criado um novo já com a nova informação.

- POST: A informação enviada é processada. A função que processa a informação é dependente do servidor selecionado. Normalmente, resulta em um recurso sendo criado ou atualizado.

- DELETE: O recurso selecionado é deletado.

A troca de mensagens entre o cliente e servidor é feito na base do pedido/resposta (*request/response*). Clientes realizam pedidos ao servidor; servidores respondem de volta uma resposta, se necessário.

Com relação a qualidade de serviço, as mensagens podem ser marcadas com "confirmáveis" ou "não-confirmáveis". Mensagens confirmáveis devem ser respondidas pelo remetente com um pacote, enquanto que mensagens não-confirmáveis seguem o estilo "disparar e esquecer", (SHELBY, 2014).

O mundo ainda está experimentando essa revolução que é a Internet das Coisas, e com isso ainda existem algumas padronizações a serem definidas, como a do protocolo de comunicação. Dentre os diversos protocolos existentes que podem ser utilizados em *IoT*, esse trabalho definiu o protocolo MQTT, o qual tem sido largamente utilizado por diversas empresas seja para *IoT* ou apenas como um protocolo de comunicação. O Facebook tem utilizado o MQTT como protocolo de comunicação de seu sistema de *instant messaging*, (Zhang, 2011), e dentro do contexto de *IoT*, a Amazon adotou MQTT, HTTP e *Websockts* como protocolos padrões em sua plataforma *IoT*, (AMAZON, 2016). Segundo (SKERRETT, 2015), diretor marketing da fundação Eclipse, o MQTT se tornou o padrão a ser suportado por qualquer servidor sério de solução para *IoT*.

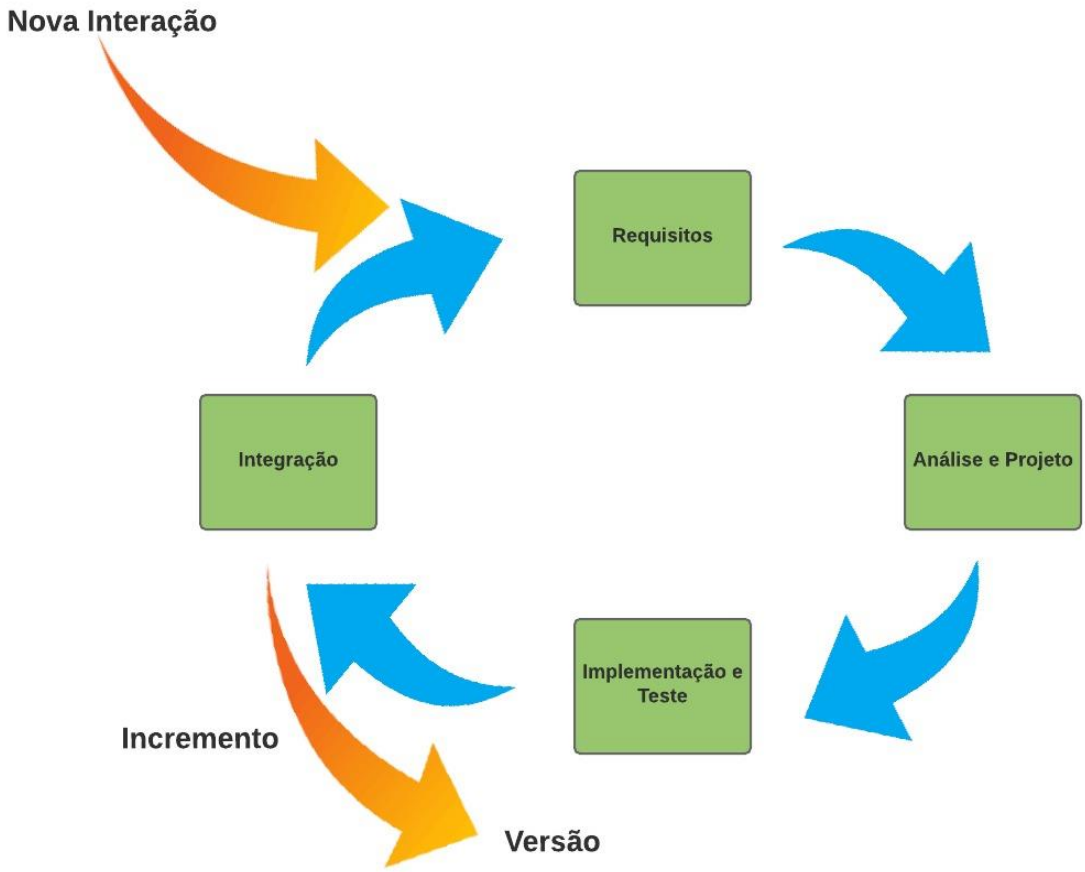
2.7 Desenvolvimento de Software

O desenvolvimento de software não é simplesmente a codificação. Existem métodos, técnicas, normas e ferramentas que auxiliam na construção de um software. Ainda que ele não seja um produto físico ele é desenvolvido com o processo criativo humano, análise, projeto, construção e teste, (PRESSMAN, 2001). É nesse processo criação ou desenvolvimento de software que se apoia a engenharia de software, ela garante que um software seja desenvolvido com qualidade e segurança, utilizando todas as fases de um processo de desenvolvimento. Dessa forma o Safecar, tantos os softwares embarcados

quanto os softwares de gestão, são desenvolvidos utilizando métodos, técnicas e ferramentas da engenharia de software. Para isso segue o detalhe do processo escolhido e a ferramenta de gestão de desenvolvimento utilizados no desenvolvimento.

O ciclo de vida iterativo e incremental aparece para solucionar problemas encontrados na utilização do modelo clássico ou cascata. No ciclo de vida interativo e incremental suas funcionalidades são implementadas contendo todas as fases do processo, análise, projeto, codificação e testes. A figura 3, modelo do processo de desenvolvimento, demonstra o ciclo de vida de cada interação realizada.

Figura 3 - Modelo de Processo Iterativo e Incremental



Fonte: Elaboração do Autor, 2018

O modelo iterativo e incremental é uma derivação do modelo cascata, porém a cada interação o sistema é incrementado, ou seja, a cada interação existe todas fases do processo de desenvolvimento e agregado a uma parte do sistema, (SOMMERVILLE, 2007).

Encontrado um processo, passo a passo, de como desenvolver *softwares*, a preocupação é voltada para como e quando realizar as atividades de desenvolvimento. Para isso existem diversas ferramentas de gestão e planejamento no desenvolvimento de software, e uma delas é a ferramenta Scrum.

A metodologia Scrum não determina o processo de desenvolvimento do *software*, portanto Scrum não é modelo de desenvolvimento. Ele se concentra em descrever como os membros da equipe devem trabalhar para produzir um sistema flexível, num ambiente de mudanças constantes. A idéia central do Scrum é que o desenvolvimento do software envolve diversas variáveis e elas possuem grande probabilidade de mudar durante a execução do projeto (por exemplo: requisitos, prazos, recursos, tecnologias etc.), (FILHO, 2008).

No Scrum, os projetos são divididos em ciclos, normalmente de 04 semanas, chamados de Sprints. A Sprint representa um conjunto de atividades devem ser executadas. As funcionalidades a serem implementadas em um projeto são mantidas em uma lista que é conhecida como Product Backlog. No início de cada Sprint, faz-se um Sprint Planning Meeting, ou seja, uma reunião de planejamento na qual o Product Owner prioriza os itens do Product Backlog e a equipe seleciona as atividades que ela será capaz de implementar durante o Sprint que se inicia. As tarefas alocadas em um Sprint são transferidas do Product Backlog para o Sprint Backlog. Os principais papeis no Scrum são:

- A equipe: São as pessoas que trabalham no desenvolvimento do software.

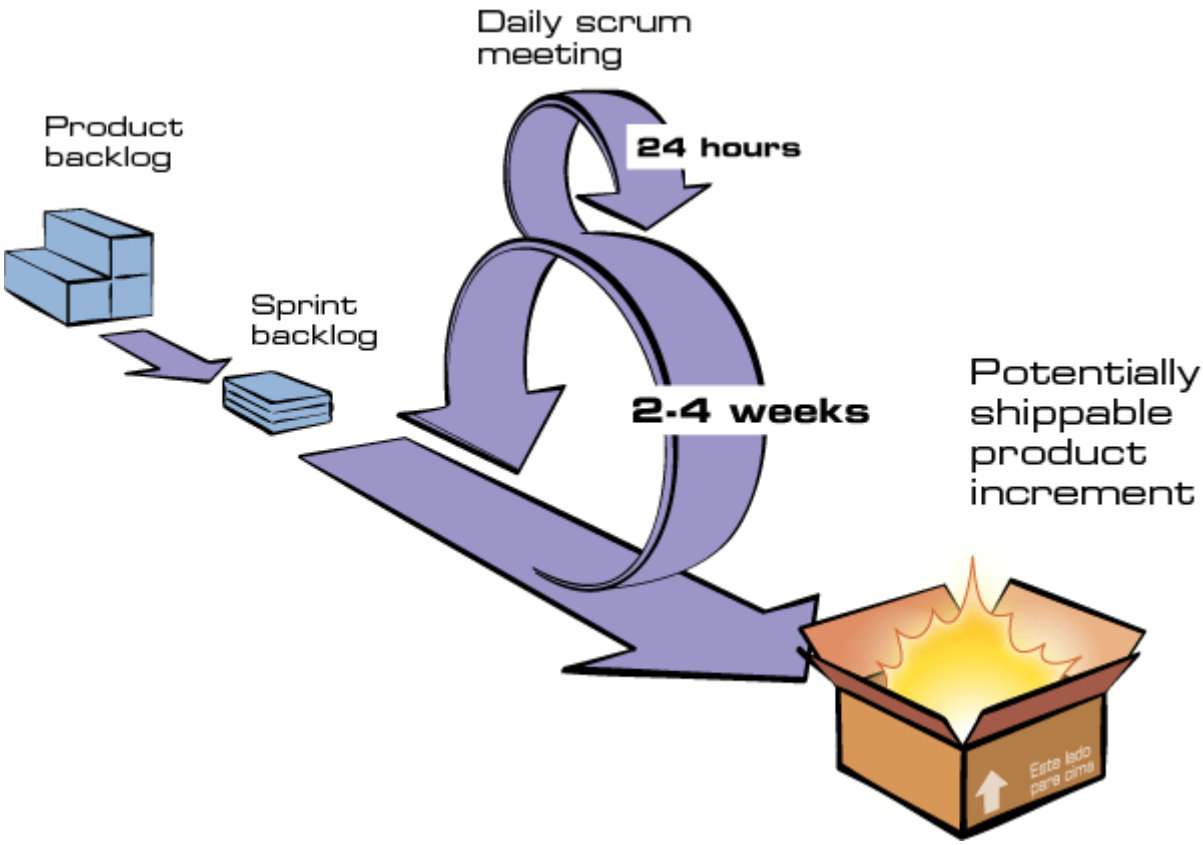
- Product Owner: Representa o cliente, ou a visão do negócio no projeto.

- Scrum Master - Representa o líder da equipe, porém entende-se que a equipe é auto gerenciada.

O processo do Scrum, conforme pode ser visto na Figura 4, inicia-se pelo Product Backlog, onde contém todas as funcionalidades definidas com o cliente ou usuário, melhorias e correções de defeitos a serem desenvolvidas no projeto (OLIVEIRA e LIMA, 2011). Com base nessa lista, é planejada a Sprint que será executada. Sprints são iterações durante as quais são implementados conjuntos de itens do Product Backlog (lista de funcionalidades desejadas), podendo variar a sua duração, de 02 (duas) a 04 (quatro) semanas. No início da Sprint, o Product Owner, o Scrum Master e o time participam da

reunião de planejamento, que é composta por duas partes. Na primeira parte participam o Product Owner, o Scrum Master e o time com a finalidade de selecionar as tarefas (Backlog do Produto selecionado) que farão parte do Backlog da Sprint conforme priorização do Product Owner. Na segunda parte, participam o Scrum Master e o time para subdividir as tarefas com o intuito de melhor entendê-las para facilitar a implementação de cada uma delas (OLIVEIRA e LIMA, 2011).

Figura 4 - Processo do Scrum



Fonte: desenvolvimento ágil, 2018.

3 Metodologia

A capacidade de criar sistemas que interajam com sensores, atuadores, redes sem fio e *smartphones* é o que alimenta esse trabalho de desenvolvimento. Pois o desafio é desenvolver um sistema juntamente com um modelo de segurança que garanta a segurança em um automóvel, utilizando o paradigma de Internet das Coisas, a fim de fornecer ao usuário monitoramento, acesso controlado e controle de algumas funções de seu veículo, garantindo tranquilidade e segurança em seu dia a dia.

Para este trabalho foi realizado vários estudos de revisão bibliográfica tanto sobre os hardwares que compõem o sistema, quanto as tecnologias utilizadas. Essas revisões tiveram como campo de estudo livros, revistas, artigos científicos, vídeos, comunidades de desenvolvedores, trabalhos publicados e demais materiais distribuídos na internet. Com isso, foi possível adquirir os hardwares necessário e desenvolver a parte física do modelo.

Para uma melhor fundamentação do tema proposto, além dos estudos de revisões bibliográficas foi desenvolvido vários softwares para o funcionamento do modelo segurança, sendo eles o safecar.ino, que está embarcado no ESP8266, o safecar.py que está embarcado no Raspberry e o safecar modo web que é o software de gestão relatado no modelo. Para o desenvolvimento dos softwares foi utilizado todas etapas de um processo de desenvolvimento de software interativo e incremental, o qual utilizou o Scrum como ferramenta de metodologia de desenvolvimento. Todas os artefatos produzidos e postados nesse trabalho, foram desenvolvidos nas 03 disciplinas de Práticas de Fábrica de Software do Curso de Engenharia de Computação da Unievangélica.

O Safecar é um sistema embarcado e que integra o modelo de segurança, o qual utiliza conceitos de *IoT* para criar uma camada de segurança em determinado automóvel permitindo acesso controlado e monitoramento do veículo. O sistema utiliza hardwares e softwares livres (*open source* e *open source hardware*), protocolo de comunicação MQTT e uma linguagem com paradigma multifuncional. Sua funcionalidade principal será autenticar o usuário de forma automática, através de seu dispositivo móvel, somente assim então, permitindo realizar outras etapas necessárias para ligar e conduzir o seu veículo.

Para o levantamento de possíveis cenários de aplicação, foram utilizados casos de usos reais, de sistemas seguros que já estão em funcionamento em seus respectivos ambientes.

4 Desenvolvimento

O projeto é um desenvolvimento de um modelo de segurança que proporcione um ambiente seguro no veículo que for implantado. Utilizando os softwares safecar.ino, software embarcado no controlador ESP8266, e safecar.py, software embarcado no Raspberry, o sistema será capaz de validar e autenticar seu usuário de forma automática. O Safecar (conjunto de softwares, o safecar.ino, safecar.py e o sistema web safecar) utilizou o processo de desenvolvimento interativo e incremental, o qual permite realizar pequenas entregas que vão incrementando todo o sistema. Com esse processo é possível utilizar a ferramenta de metodologia de desenvolvimento Scrum, a qual garante planejamento, execução e controle das atividades realizadas.

Por se tratar de um processo cíclico e com interações pequenas, no desenvolvimento do Safecar, esse processo, permitiu desenvolver o software pouco a pouco, garantindo o aprendizado e correções das versões anteriormente terminadas.

O modelo conta também com uma aplicação web, o qual é chamado no modelo de software de gestão, para realizar diversas funcionalidades de apoio ao administrador do sistema e ao usuário. No sistema foi desenvolvido um modo administrador, com a finalidade de manter veículos, manter equipamentos e manter usuários. É necessário também um modo usuário, com a finalidade de disponibilizar os dados da telemetria e manter perfil. O módulo web do sistema foi desenvolvido utilizando a ferramenta Spring em seu *back end* e a ferramenta Angular no seu *front end*. O *back end* requisita os dados diretamente do banco de dados que é mantido pelo Safecar.py e realiza sua integração com o *front end*.

Após realização do estudo sobre o conceito de Internet das Coisas e suas principais características, a fim de levantar requisitos para o funcionamento do sistema, foi realizado, dentro das fases de análise e projeto, a modelagem do sistema. Essa modelagem define algumas necessidades do modelo de segurança, como por exemplo, quais hardwares, softwares e protocolo de comunicação utilizar. Na tabela 1 estão detalhados todos os hardwares que o sistema está utilizando. Esses hardwares são encontrados facilmente no mercado para aquisição. Na tabela 2 estão detalhados os softwares e frameworks utilizados no desenvolvimento do modelo de segurança. Alguns destes softwares estão instalados no

raspberry, o qual está embarcado no veículo, outros estão instalados nas máquinas de desenvolvimento.

Tabela 1 - Lista de Hardwares utilizados

Hardware	Versão
Raspberry	3
APM - ArduPilot Mega Controlador	2.8
Moldem movistar	E173s-6
Nodmcu (ESP 8266)	v3
Shild relé	
Escanner automotivo obd2	elm327

Fonte: Elaboração do Autor, 2018.

Como um dos principais documentos da fase de análise a visão do produto é para proprietários de automóveis que necessitam conduzir, monitorar, interagir com o seu veículo de forma segura e automatizada.

O SafeCar é um modelo de segurança para automóveis tendo como objetivo a interação com o dispositivo móvel de seu usuário a fim de validar a sua autenticidade. Permitindo ao mesmo definir quem poderá acessar, controlar, monitorar e utilizar seu automóvel, lhe proporcionando conforto e segurança.

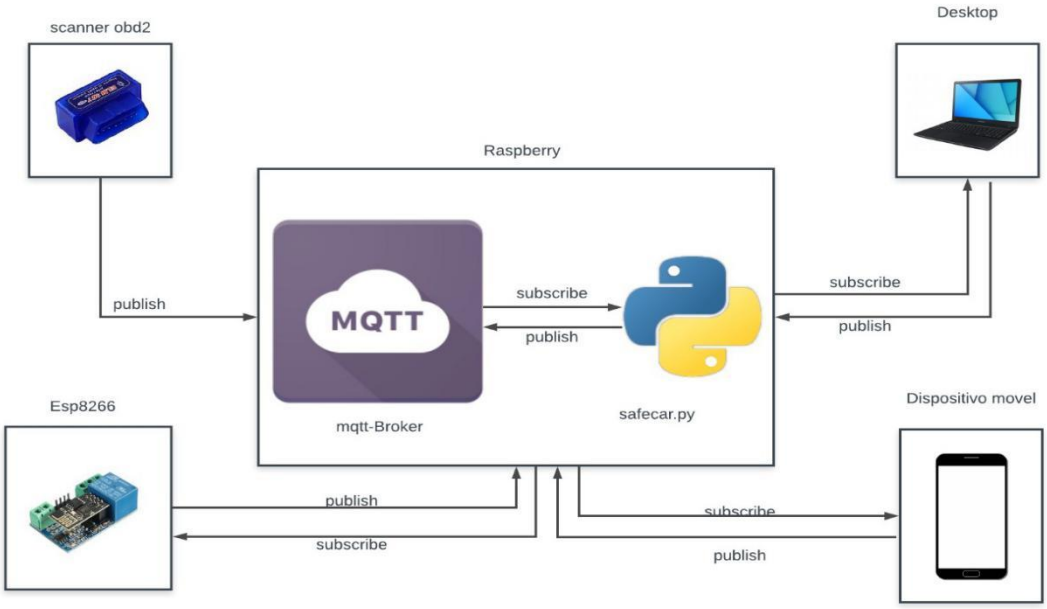
Tabela 2 - Lista de Softwares utilizados

Softwares	Versão
Visual Studio Code	1.23.1
Intellij idea	IU-171.4694.23
Mosquitto	1.5.2003
LinuxMint	18.3 Sylvia
Ubuntu	Bionic
Debian	Stretch
Java	1.8.0_181
Node	v8.11.1
Angular cli	6.1.2005
Python	2.7
Tomcat	8
Apache Jmeter	5.0
Postman	6.44
Git	2.7.4
Gitkraken	4.0

Fonte: Elaboração do Autor, 2018

A Figura 5, é a modelagem da arquitetura do modelo de segurança, e representa em uma visão geral o funcionamento do modelo de segurança. O modelo utiliza o Raspberry como memória e processamento, o ESP8266 como microcontrolador, o qual realiza a interface com sensores e atuadores, além de disponibilizar a rede sem fio interna no veículo e o protocolo de comunicação MQTT, o qual gerência as mensagens de envio e recepção do sistema.

Figura 5 - Arquitetura do Modelo de Segurança



Fonte: Elaboração do Autor, 2018.

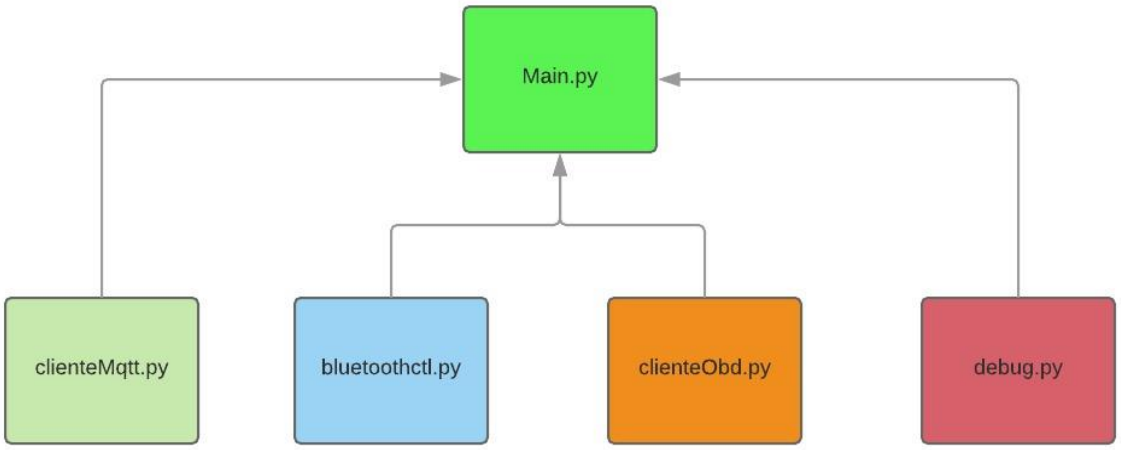
O microcontrolador ESP8266 é o responsável por interagir com a bomba de combustível do automóvel, através de um relé que permite ou não a passagem de energia. O microcontrolador é responsável também por fornecer a rede interna no automóvel, rede a qual o usuário se conecta de forma automática. A fim de realizar a sua função dentro do modelo de segurança, foi necessário desenvolver um firmware para embarcar no ESP8266, o Safecar.ino.

As funcionalidades do Safecar.ino são disponibilizar uma rede sem fio, fornecer o identificador (ID) do dispositivo conectado, permitir acionamento do relé que está instalado em um de seus GPIO's e ser um cliente MQTT. Para implementação dessas funcionalidades, foi utilizada a IDE do arduino.

O Raspberry tem a função de um computador dentro do modelo de segurança, provendo o modelo com memória e processamento. Este computador está utilizando a distribuição do linux Debian, como sistema operacional, o Mosquito MQTT como Broker do protocolo de comunicação e o Postgresql como banco de dados do sistema. Além dos softwares já descritos foi necessário no sistema o desenvolvimento do Safecar.py, o qual é o responsável por verificar se o usuário conectado está autorizado a utilizar o veículo, receber

os registros da telemetria do veículo pelo dispositivo *On Board Diagnostic* ODB, receber os dados do controlador APM - ArduPilot Mega, manter os registros no banco de dados, comunicar com o MQTT e disponibilizar os dados para o *Front End* do sistema, ou seja, ele é o *Back End* do sistema embarcado. O Safecar.py foi implementado utilizando a linguagem de programação Python, o que torna o desenvolvimento mais dinâmico e ágil, pois existe uma sólida comunidade de desenvolvedores na internet e uma gama de bibliotecas que facilitam a implementação do sistema. A figura 6, Modelagem do Safecar.py é um diagrama de blocos que representa a comunicação entre as classes do Safecar.py.

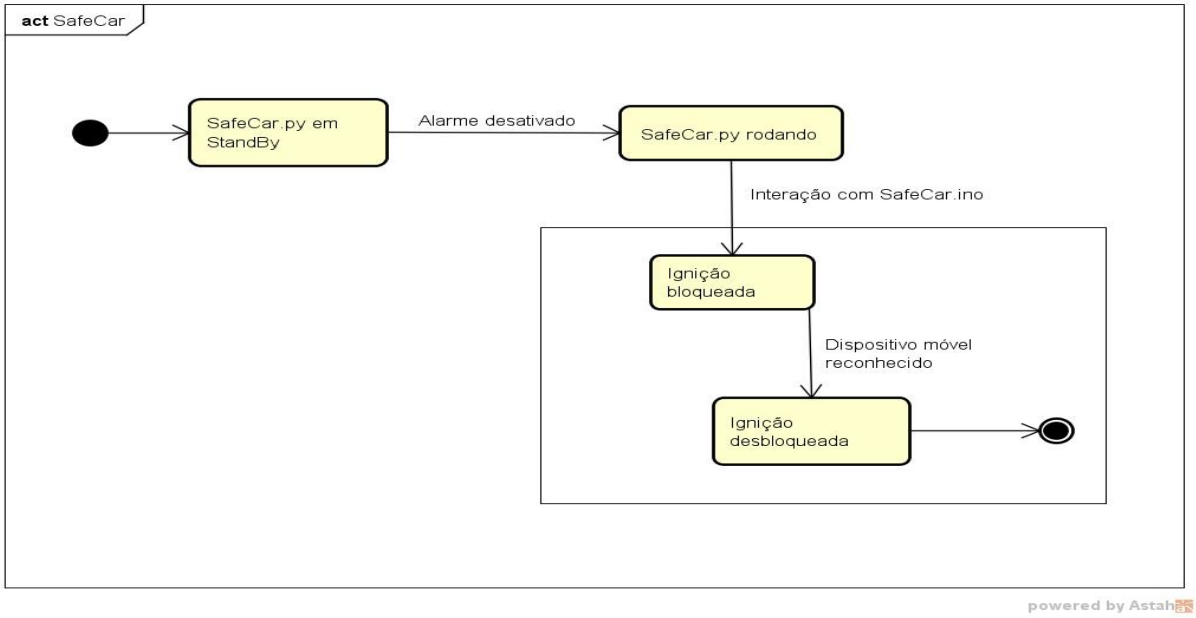
Figura 6 - Modelagem do Safecar.py



Fonte: Elaboração do Autor, 2018

No diagrama de Máquina de Estados, Figura 7, é possível visualizar o modelo de segurança em funcionamento, o qual permite o usuário ligar o seu automóvel somente se o seu dispositivo móvel for reconhecido pelo sistema, automatizando a autenticação e validação, pois espera-se que o dispositivo móvel, autorizado pelo sistema, se conecte de forma automática.

Figura 7 - Diagrama de Máquina de Estados



Fonte: Elaboração do Autor, 2018.

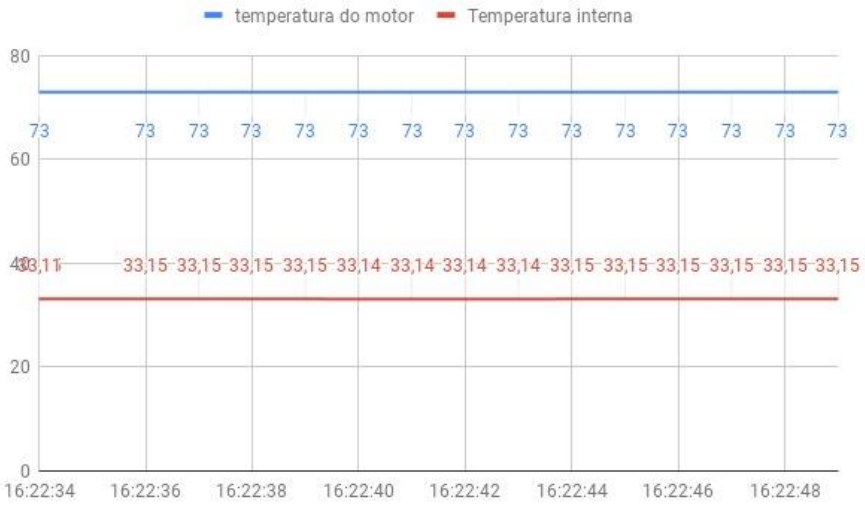
Com a finalidade de tornar-se um sistema mais próximo do usuário, foi desenvolvido um software de gestão, o qual é chamado de safecar web. É um sistema web que permite a interação do usuário através da funcionalidade visualizar telemetria. Por meio dessa funcionalidade o usuário visualiza gráficos referentes a telemetria do seu veículo, conforme figura 8 e figura 9. A figura 8 representa em forma de gráfico a posição do acelerador e a rotação por minuto do veículo em dado instante. A figura 9 é a representação da temperatura do motor e a temperatura interna do carro. Esses dados representados pelos gráficos são recebidos pelo dispositivo Escanner automotivo obd2 que realiza a transmissão de dados via bluetooth para o raspberry. Por meio do safecar.py esses dados disponibilizados no front end, como pode ser visto na figura 10.

No Safecar modo web que o administrador mantém veículos, usuários e dispositivos móveis do sistema. Na figura 11 é possível visualizar um automóvel cadastrado. No sistema web é possível cadastrar o MAC (*Media Access Control*) que está autorizado para cada veículo, conforme demonstrado na figura 12. Sendo o MAC a identificação única de cada dispositivo móvel, é utilizando ele que é realizada a identificação do usuário no processo de automatizado de autenticação.

Figura 8 - Gráfico RPM e Posição do Acelerador do Veículo

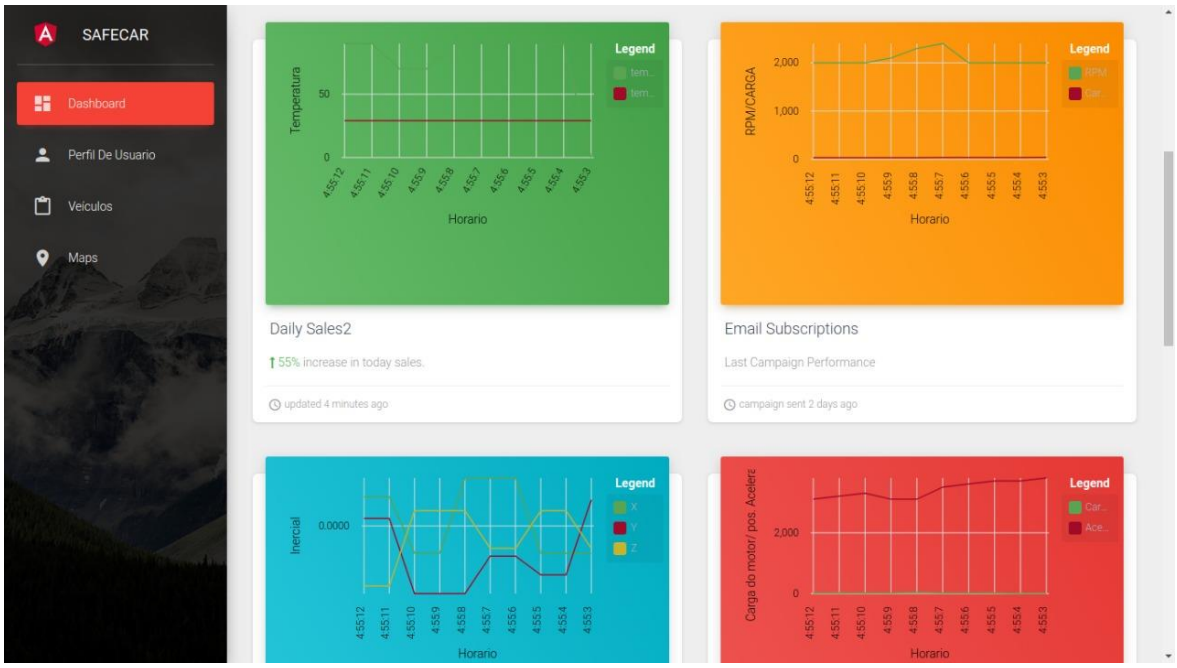
Fonte: Elaboração do Autor, 2018.

Figura 9 - Gráfico de temperaturas do motor e interna do Veículo



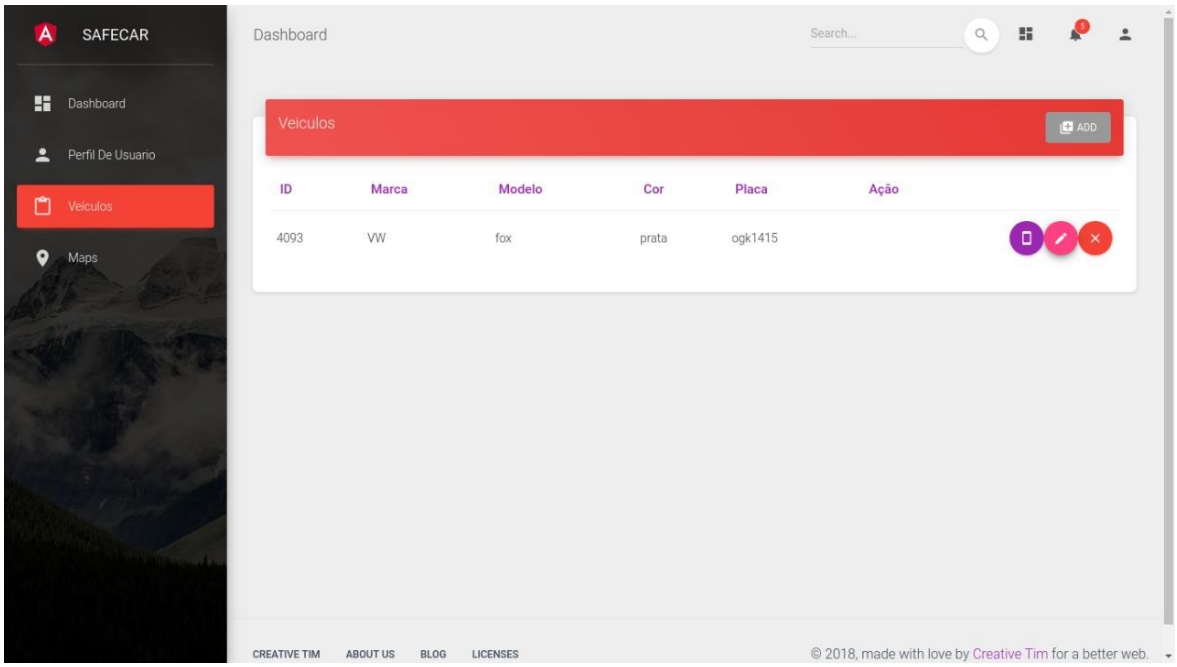
Fonte: Elaboração do Autor, 2018.

Figura 10 - Página de Telemetria do Veículo.



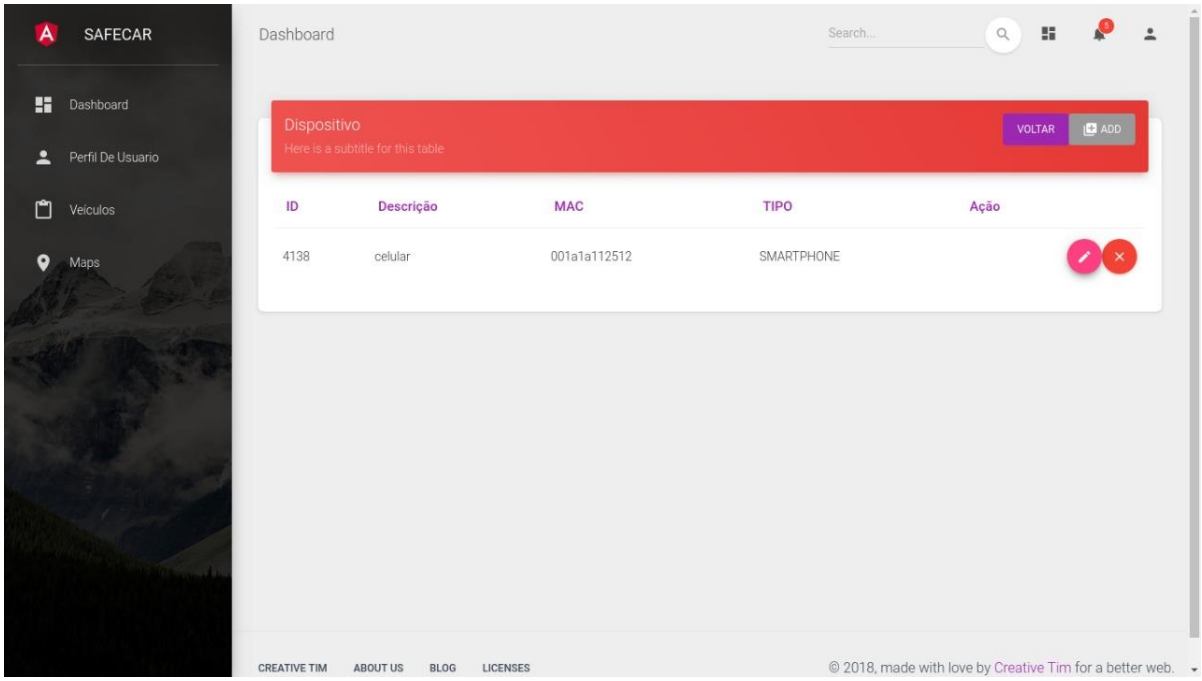
Fonte: Elaboração do Autor, 2018

Figura 11 - Página de Identificação do Veículo.



Fonte: Elaboração do Autor, 2018

Figura 12 - Página de Identificação do Dispositivo Móvel.



Fonte: Elaboração do Autor, 2018

A fase de implantação do modelo de segurança é representada pelo término do trabalho, pois os artefatos e códigos expostos foram construídos para o desenvolvimento deste trabalho de conclusão, ou seja, o modelo de segurança não foi aplicado a um cliente específico e sua implantação foi somente para realizar testes nos veículos dos autores deste trabalho.

5 Possíveis Cenários de Aplicação

Espera-se demonstrar por meio do funcionamento do Safecar que o modelo de segurança é capaz de garantir um ambiente seguro, utilizando o paradigma de *IoT*. Entende-se que em qualquer outro ambiente que possa ser integrado as mesmas ferramentas utilizadas, como memória e processamento, protocolo de comunicação e sensores, também poderá ter um sistema que garanta segurança de forma automatizada. Para isso será realizado um levantamento de diversificados cenários reais os quais podem ter seu ambiente monitorado e controlado utilizando Internet das Coisas.

5.1 Controle de Acesso na Faculdade

Na Unievangélica o controle de entrada é através da tecnologia RFID, a qual utiliza um cartão no terminal da entrada e a cancela se levanta. É observado diariamente alunos sem o cartão de acesso, o que torna necessário um funcionário no local somente para disponibilizar o acesso a instituição para quem esqueceu seu cartão de entrada. Enfim, utilizando o modelo de segurança, o aluno poderia realizar sua entrada na faculdade, por meio da conexão de algum dispositivo móvel com a rede da faculdade, quando isso acontece a cancela permite acesso por determinados segundos, todos registros necessários a sua entrada são registrados no software de gestão e o aluno entraria no ambiente de forma automática. Nessa situação, se utilizar o celular como dispositivo móvel provavelmente o funcionário não seria necessário e poderia estar executando outra tarefa em seu posto de serviço.

5.2 Automatizar entrada em eventos

O modelo de segurança poderia funcionar facilmente na entrada de eventos como shows, teatros, jogos de futebol, dentre tantos outros. Em Porto Alegre-RS, para entrar no estádio Arena do Grêmio é utilizado uma tecnologia de controle e identificação de torcedores que utiliza catracas com identificação biométrica e câmeras de gravação de vídeo, sendo que o processo de registro no sistema é lento e nada intuitivo. Com o modelo de segurança, o

ingresso já poderia ser um dispositivo móvel que faça a conexão na rede, por exemplo uma pulseira, a qual seria utilizada tanto para realizar a entrada do torcedor, quanto para monitorar cada torcedor durante o jogo, pois entende-se que o usuário permanecerá conectada no setor autorizado a sua permanência.

5.3 Acesso seguro em Hotéis ou Condomínios

A empresa Atlas Schindler tem um Sistema de Acesso Seguro - SAS, o qual é um sistema de controle de acesso que utiliza um cartão tipo RFID, para identificar o passageiro do elevador e liberar o acesso somente ao andar autorizado. Isso significa que que somente pessoas previamente cadastradas no sistema SAS, podem circular pelos andares do condomínio. Utilizando o modelo de segurança proposto no trabalho, o sistema SAS poderá ser substituído facilmente, pois no lugar do elevador com tecnologia RFID, o hotel ou condomínio poderá utilizar o modelo que tem como funcionalidade básica identificar e autorizar de forma automática determinado usuário, por meio de algum dispositivo móvel de sua posse conectado a rede sem fio.

6 Considerações Finais

Nesse trabalho foi apresentado um modelo que proporciona segurança em um ambiente utilizando Internet das Coisas. Utilizando o modelo, o qual é composto por memória e processamento, protocolo de comunicação, comunicação sem fio, sensores e atuadores e um software de gestão ficou claro que é possível extrair vários dados do ambiente e dos usuários, o que torna possível registrar, monitorar e controlar a interação do usuário com o ambiente em questão.

Uma das bases da Industria 4.0, a Internet das Coisas trará impacto sobre a produtividade, a redução de custos, o controle sobre o processo produtivo, a customização da produção, dentre outras áreas no Brasil. A estimativa anual de redução de custos industriais no Brasil, a partir da migração da indústria para o conceito 4.0, será de, no mínimo 73 bilhões por ano, (ABDI, 2018). Logicamente que os desafios tecnológicos ainda são muitos no Brasil, porém o trabalho deixa claro que tecnologias abertas e livres são uma boa saída para um país sub desenvolvido avançar na área tecnológica.

Referências Bibliográficas

ABDI, Agência Brasileira de Desenvolvimento Industrial, 2018.

AMAZON Web Services 2016. AWS *IoT*.

ASHTON, Kevin. That 'Internet of Things' . Publicando no RFID Journal, 2009.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: A survey, 2010. Computer Networks 54 (2010), p. 2787–2805.

BACHA, Maria de Lourdes; SCHAUN, Angela. Celular: o gadget da inclusão digital no Brasil. Anais da CONFIBERCOM. São Paulo: Confederación Iberoamericana de Asociaciones Científicas y Académicas de la Comunicación, Julho de 2011.

BAUMAN, Z. Amor líquido: sobre a fragilidade dos laços humanos. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2004.

BECK, Ceres Grehs; MOTA, Flavio Perazzo Barbosa; DO VALE, Solange Cristina; LEITE, Jose Carlos de Lacerda; PEREIRA, Rita de Cassia de Faria. Meu Celular e Eu: mensurando a extensão do Self. Anais do XXXIII Encontro da ANPAD. São Paulo, ANPAD, 2009.

BERGMANN, Olaf. Libcoap: C-implementation of CoAP, 2010.

BERNADO, Cláudio Gonçalves. A tecnologia RFID e os benefícios da etiqueta inteligente para os negócios. Revista Eletrônica Unibero de iniciação Científica, São Paulo, 2004.

CAMPOS, Augusto. O que é Software Livre. BR-Linux, 2006.

CISCO IBSG, abril de 2011, Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf.

EVANS, Dave; A Internet das Coisas – Como a próxima evolução da internet está mudando tudo, 2011.

FACCIONI, Filho Mauro, Internet das Coisas, Unisul Virtual, 2016.

FARIAS, Paulo César Bento, Rede Wireless, 2005.

FILHO, D. L. B.: Experiências com desenvolvimento ágil. Instituto de Matemática e Estatística da Universidade de São Paulo (Dissertação de Mestrado). 2008.

HARDWARE ABERTO, Definição de Hardware de Código Aberto - OSHW 1.0, 2016.

HEXSEL, Roberto A. Propostas de Ações do Governo para Incentivar o Uso de Software Livre. Relatório Técnico do Departamento de Informática da UFPR. Curitiba, Paraná, 2003.

INTERNATIONAL BUSINESS MACHINES; EUROTECH; MQTT specification version 3.1, 2010.

JAFFEY, Toby. MQTT and COAP, *IoT* protocols. 2014.

KRANENGBURG, R.; ANZELMO, E.; BASSI A., CAPRIO, D.; DODSON, S.; RATTO, M. The Internet of Things. 1st Berlin Symposium on the Internet and Society, 2011.

LARCEDA, F., & LIMA-MARQUES, M. (2015). Da necessidade de princípios de arquitetura da informação para a internet das coisas. Perspectivas em Ciência da Informação.

Oliveira, E. e Lima, R. (2011) Estado da Arte Sobre o Uso do Scrum em Ambientes de Desenvolvimento Distribuído de Software. Revista de Sistemas e Computação, Salvador.

PAIVA.Fernando. Internet das Coisas vai produzir "tsunami" de sinalização nas redes móveis, 2015.

PRESSMAN, R.S. Engenharia de Software. 5.ed. McGraw-Hill, 2001.

RIFIKIN, . Como a Internet das Coisas vai atropelar o capitalismo, 2015.

SELIC, B. The pragmatics of model-driven development. IEEE Software, 2003.

SHELBY, Zach. CoAP: The web of things protocol, 2014.

SOMMERVILLE. Software Engineering. Eighth Edi ed. [S.l.]: Addison Wesley, 2007.

SKERRETT, I. 2015. Case Study MQTT: Why Open Source and Open Standards Drive Adoption.

STANSBERRY, J., MQTT and COAP: Underlying protocols for the *IoT*. Electronic Design, 2015.

TORRES, Gabriel. Redes de Computadores Curso Completo - 2001, Axcel Books do Brasil Editora Ltda.

UCEL. Mapa dinâmico de telefonia celular. Mercado de *smartfones*. UWE, Flick. Introdução à pesquisa qualitativa. Porto Alegre: Artmed, 2009.