

## Sistema para análise do perfil de condutores de veículos segurados através de técnicas de IoT

Bruno Oliveira Casotti<sup>1</sup>  
Davi Guaracho Nascimento<sup>2</sup>  
Rafael Paludetti Pereira<sup>3</sup>  
Fábio Henrique Cabrini<sup>4</sup>

### Resumo:

Este artigo apresenta o desenvolvimento de um aplicativo para plataforma Android e a estrutura de *back-end* que tem como objetivo maior tornar-se uma solução para que as seguradoras de automóveis possam monitorar e analisar a forma como seus segurados conduzem seus veículos, a fim de avaliar se as condições pré-estabelecidas em contrato estão sendo cumpridas. Trata-se de um sistema baseado nos conceitos de Internet das Coisas (IoT - *Internet of Things*) que realiza a coleta dos dados a partir de um dispositivo OBD (*On-board Diagnostic*), um conector que acoplado ao barramento do veículo possibilita o acesso aos dados da ECU (*Electronic Control Unit*). Os dados são transmitidos por uma conexão Bluetooth para o *smartphone* que agrega as informações de geolocalização e as envia através da rede 3G/4G para a plataforma FIWARE localizada na nuvem.

**Palavras-Chave:** OBD. Internet das Coisas. Android. FIWARE.

### Abstract:

This article presents the development of an app prototype for Android platform proposing a solution for insurers to monitor how their insureds are driving their vehicles in order to ensure that they are complying with the pre-established terms and conditions in the contract. It is a system based on the Internet of Things (IoT) concepts that performs the data collection from an OBD (*On-board Diagnostic*) device, a connector that coupled to the vehicle's bus allows access to the vehicle's ECU (*Electronic Control Unit*) data. The data is collected through a Bluetooth connection by the smartphone, which will send them using the 3G/4G network along with the current location obtained by the GPS (*Global Position System*) to a MongoDB database hosted on the FIWARE platform.

**Keywords:** OBD. Internet of Things. Android. FIWARE.

---

<sup>1</sup> Tecnólogo em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologia Termomecânica - São Bernardo do Campo.

<sup>2</sup> Tecnólogo em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologia Termomecânica - São Bernardo do Campo.

<sup>3</sup> Tecnólogo em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologia Termomecânica - São Bernardo do Campo.

<sup>4</sup> Professor Mestre na Faculdade de Tecnologia Termomecânica - São Bernardo do Campo.

### Introdução

Por anos as seguradoras geram contratos baseados na confiança mútua, onde seguradora e segurado celebram um acordo por meio de informações disponibilizadas por um questionário de aderência. Segundo a Superintendência de Seguros Privados (SUSEP, 2017), é através do Questionário de Avaliação de Risco que a seguradora define o perfil do segurado para avaliar o risco que irá assumir. Dentre as questões estão: a idade do condutor, tempo de habilitação, região de circulação do veículo, e se possui garagem ou estacionamento fechado. Baseada neste questionário, a seguradora determina os planos disponíveis para o segurado, os valores dos mesmos e estipula as cláusulas do contrato.

Estas informações coletadas pelas seguradoras podem ser imprecisas, uma vez que o segurado pode omitir informações que sejam relevantes para a avaliação criando assim um perfil impreciso do segurado e impactando negativamente na manutenção dos serviços prestados pela seguradora.

### Internet das coisas

Um conjunto de conceitos que vem revolucionando o cenário das telecomunicações, a Internet das Coisas, ou do inglês *Internet of Things* (IoT) é o conceito básico da conexão de objetos (coisas) à Internet, incluindo televisores, celulares, veículos automotivos, etiquetas RFID (*Radio-Frequency IDentification*), sensores, entre outros dispositivos capazes de manter comunicação com a Internet. Essa comunicação permite a interação entre essas diversas coisas e possibilita que elas trabalhem juntas, atuando na coleta de dados. (ATZORI, IERA e MORABITO, 2010, p. 1).

De acordo com (JAYAVARDHANA, RAJKUMAR, et al., 2013, p. 1) a IoT aborda uma série de paradigmas que fugiram ao tradicional *desktop*, onde todos os dispositivos são conectados à Internet de forma imperceptível aos usuários, gerando uma quantidade grande de dados, que serão processados e apresentados de forma eficiente e de fácil interpretação. Um estudo realizado pela NIC (*National Intelligence Council*) prevê que, a partir de 2025, os objetos rotineiros, como por exemplo, documentos de papel ou embalagens de comida estarão conectadas a Internet por meio dos conceitos de IoT e que isso impactará diretamente na forma como é realizado o monitoramento, a localização e o controle dos dispositivos. (NATIONAL INTELLIGENCE COUNCIL, 2008, p. V)

### Computação em nuvem

Segundo (PEDROSA e NOGUEIRA, 2011, p. 1) a Computação em Nuvem é considerada

um modelo de computação que permite aos seus usuários acessar serviços e softwares de qualquer lugar e de qualquer dispositivo, sendo ele móvel ou não, necessitando apenas de acesso à Internet. O termo nuvem transparece a ideia de algo inacessível fisicamente, ou seja, uma infraestrutura que o usuário apenas acessa e a utiliza, porém não a possui fisicamente.

Ainda segundo (MELL e GRANCE, 2011), a computação em nuvem trata-se de um modelo que possibilita o acesso a uma rede compartilhada, disponibilizando recursos de computação maleáveis, escaláveis e de fácil provisionamento e baixa complexidade de implementação.

Computação em nuvem é uma tendência recente de tecnologia que tem por objetivo proporcionar serviços de tecnologia da Informação sob demanda com pagamento baseado no uso. Computação em nuvem pretende ser global e prover serviços para todos, desde o usuário final que hospeda seus documentos pessoais na Internet até empresas que terceirizam toda a parte de TI para outras empresas. Nenhuma abordagem para a utilização real foi tão global e completa: não apenas recursos de computação e armazenamento são entregues sob demanda, mas toda a pilha de computação pode ser aproveitada na nuvem. (RUSHEL, ZANOTTO e MOTA, 2010, p. 1-2)

O principal objetivo é prover disponibilidade e escalabilidade dos dados, diminuir drasticamente os custos com infraestrutura, flexibilizar e facilitar o acesso aos serviços disponibilizados para seus usuários. (RUSHEL, ZANOTTO e MOTA, 2010, p. 3)

### FIWARE

O FIWARE é uma plataforma desenvolvida pela FI-PPP (*Future Internet Public-Private Partnership*), uma parceria entre a união europeia e a iniciativa privada. Com o intuito de “Construir um ecossistema aberto e sustentável, público, livre de *royalties* e padronizado” (FIWARE, 2016), seu objetivo é facilitar o desenvolvimento de aplicativos por meio da disponibilização de API's (*Application Programming Interface*).

O FIWARE tem o apoio de uma comunidade independente, seus membros empregam esforços para tornar a sua missão real. Essa comunidade é constituída por empresas do setor de tecnologia, organizações e indivíduos que contribuem de alguma forma para o crescimento da plataforma sendo esse trabalho organizado pela FIWARE Foundation (2017).

Sua arquitetura é baseada no OpenStack, que segundo SILVA (2015), é uma plataforma de Computação em nuvem aberta para nuvens privadas, públicas e híbridas e altamente escalável. De acordo com a FIWARE Foundation, a plataforma é aberta e dispõe de serviços e ferramentas altamente compatíveis com aplicações para IoT e que permitem o aproveitamento máximo da sua capacidade de processamento e escalabilidade.

Através da configuração de serviços (módulos), chamados GE (*Generic Enablers*), o

FIWARE possibilita a aplicação de serviços para IoT e armazenamento de dados. Por meio de um GE chamado Orion Context Broker, é possível fazer a comunicação com a plataforma e manipular as entidades de contexto da aplicação por meio de uma API; e utilizando um conector de fontes de dados chamado Cygnus, pode ser realizado o armazenamento histórico dos dados em repositório de terceiros, como um MongoDB.

Todos os GEs e recursos da plataforma estão documentados e podem ser acessados pelo web site da FIWARE Foundation (2017).

### ODB

OBD, acrônimo derivado do inglês “*On Board Diagnostic*”, é um sistema padrão para autodiagnóstico de veículos automotivos, sancionado como obrigatório para todos os veículos no ano de 1996 nos Estados Unidos e Europa, e no Brasil em 2010. O conceito do OBD surgiu na Califórnia em meados dos anos 50 com o objetivo de controlar a emissão de poluentes causados pelos automóveis, mas as primeiras disposições foram estabelecidas apenas 11 anos depois, em 1988, onde o CARB (Conselho de Recursos do Ar da Califórnia), com o auxílio da SAE (*Society of Automotive Engineers*), exigiu que todos os carros vendidos na Califórnia saíssem de fábrica com o sistema OBDI ou como também era conhecido, “sistemas pré-OBDII”; sistema esse que era capaz de detectar defeitos nos elementos e sistemas de controle de emissões.

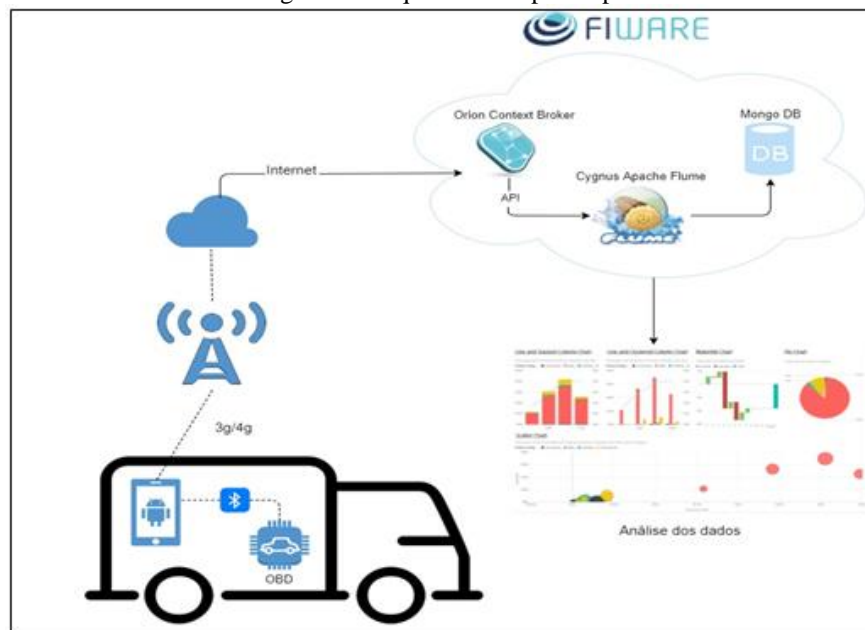
Em 1990 um novo conjunto de especificações foi desenvolvido pelo CARB, pois concluiu-se que o padrão OBDI não era totalmente eficiente na determinação do elemento que provocara o defeito. Assim surgiu a norma OBDII, que é utilizada até os dias de hoje nos sistemas de autodiagnóstico de veículos automotivos.

### Desenvolvimento

O protótipo apresentado neste artigo foi desenvolvido para a plataforma Android utilizando um banco de dados MongoDB, os GE's Orion Context Broker e Cygnus da plataforma FIWARE e um dispositivo OBD. A figura 2 apresenta a arquitetura completa do sistema.

No momento que o aplicativo se conecta, via Bluetooth, ao dispositivo OBD, as informações do computador de bordo do veículo e a geolocalização coletada pelo sensor de GPS do *smartphone* começam a ser transmitidas através das redes móveis 3G e 4G para o Orion Context Broker na plataforma FIWARE, via mensagens REST. Este por sua vez encaminha os dados para o conector Cygnus que os armazena em um banco de dados MongoDB.

Figura 2 - Arquitetura do protótipo



Foi instanciada uma máquina virtual na plataforma FIWARE com o sistema operacional CentOS versão 6.7, o qual hospeda os serviços do Orion, Cygnus e MongoDB. A máquina foi configurada com 4GBytes de memória RAM, 2 (duas) CPUs e 40GBytes de espaço em disco.

Para a comunicação com a API do Orion Context Broker, foi necessário realizar algumas configurações de segurança de liberação de portas no *firewall* que integra a plataforma. Isto é facilmente realizado através do painel de controle do OpenStack. As portas liberadas foram:

- Porta 22: utilizada para acesso ao servidor via SSH;
- Porta 1026: utilizada pelo serviço do Orion Context Broker;
- Porta 5050: notificações do serviço do Cygnus;
- Porta 27017: porta padrão do MongoDB.

### Configuração do Cygnus

Após a etapa anteriormente descrita, foi realizada a configuração do agente Cygnus. O Cygnus possui alguns arquivos que devem ser editados para que o mesmo possa funcionar corretamente. Os mesmos já estão pré-configurados dentro da pasta “/usr/cygnus/conf”.

A configuração do agente é dividida entre dois arquivos:

- `cygnus_instance_<id>.conf`: este arquivo possui parâmetros não utilizados pelo Flume, como o arquivo de log específico para esta instância, a porta de administração, etc;
- `agent_<id>.conf`: contém parâmetros usados pelo Flume, como as configurações dos canais de armazenamento, *sinks*, etc;

O Cygnus pode ter mais de uma instância e a variável ID descrita nos nomes dos arquivos representa a instância a ser configurada para execução.

### Manipulando entidades do Orion

A comunicação com o Orion Context Broker é feita mediante mensagens REST utilizando JSON. Cada JSON representa uma entidade por meio de seus atributos. Neste projeto foi utilizada a versão 2 (v2) da API do Orion, que comparada a primeira versão (v1), possui rotas e estrutura do JSON diferentes.

Para que as entidades enviadas ao servidor fossem armazenadas no MongoDB por intermédio do Cygnus, foi necessário cadastrar a *subscription* da entidade. A *subscription* é uma espécie de assinatura da entidade para o agente Cygnus. Desta forma, quando acontece uma alteração nos valores atuais da entidade no Orion, uma notificação é enviada de forma assíncrona para o Cygnus que registra o momento da notificação com um *timestamp* que será armazenado juntamente com os dados no MongoDB.

A assinatura é criada enviando um JSON para o endereço “http://<ip-address>:1026/v2/subscriptions” por meio do método POST, conforme a estrutura apresentada na figura 3.

Figura 3 - Mensagem para criar a assinatura

```
{
  "description": "Entitie for TCC Smart Car Monitor",
  "subject": {
    "entities": [
      {
        "type": "Vehicle",
        "isPattern": "false",
        "id": "fordKa"
      }
    ],
    "condition": {
      "attrs": [
        "velocidade",
        "combustivel",
        "RPM",
        "localizacao"
      ]
    }
  },
  "notification": {
    "http": {
      "url": "http://localhost:5050/notify"
    },
    "attrs": [
      "velocidade",
      "combustivel",
      "RPM",
      "localizacao"
    ],
    "attrsFormat": "legacy"
  },
  "expires": "2140-12-30T14:00:00:00Z",
  "throttling": 5
}
```

Foi preciso cadastrar a entidade no Orion Context Broker com seus atributos para que esta pudesse ser atualizada a cada nova notificação, sendo eles: geolocalização (latitude e longitude), velocidade, nível de combustível, RPM (Rotações Por Minuto) e seus valores iniciais. No cenário deste trabalho, cada carro foi representado por um ID diferente e todos eram do tipo “Vehicle”, conforme a figura 4.

Figura 4 - JSON de cadastro da entidade

```
{
  "id": "fordKa",
  "type": "Vehicle",
  "velocidade": {
    "type": "integer",
    "value": "50"
  },
  "combustivel": {
    "type": "float",
    "value": "70"
  },
  "RPM": {
    "type": "integer",
    "value": "2960"
  },
  "localizacao": {
    "type": "point",
    "value": [ -23.3245, -41.4644 ]
  }
}
```

Para fazer o cadastro das entidades, foi enviado o JSON para o endereço “http://<ip-address>:1026/v2/entities” via método POST. O aplicativo atualiza os valores da entidade por meio de requisição PATCH para o endereço “http://<ip-address>:1026/v2/entities/<id-entidade>/attrs”. A cada atualização, uma notificação é enviada para o Cygnus registrar a alteração no MongoDB. A figura 5 apresenta a estrutura do JSON de atualização da entidade.

Figura 5 - JSON de atualização de entidade

```
{
  "velocidade": {
    "type": "integer",
    "value": "50"
  },
  "combustivel": {
    "type": "float",
    "value": "70"
  },
  "RPM": {
    "type": "integer",
    "value": "2960"
  },
  "localizacao": {
    "type": "point",
    "value": [ -23.3245, -41.4644 ]
  }
}
```

## Interface do aplicativo

O protótipo deste projeto tem a funcionalidade de capturar os dados do veículo por meio da interface OBD e enviá-los em formato JSON para a plataforma FIWARE. Para que o aplicativo funcione corretamente, é necessário que o *smartphone* esteja conectado à Internet, o GPS do aparelho deve estar habilitado e o Bluetooth deve estar pareado com o dispositivo OBD. A figura 7 apresenta a interface do aplicativo em execução.

Figura 7 - Tela do Smart Car Monitor em execução



## Testes em ambiente real

Para verificar o funcionamento do aplicativo em ambiente real, foram realizadas viagens em veículos diferentes e utilizado o software Power BI da Microsoft para criação de gráficos e *dashboards* afim de comprovar o funcionamento do protótipo.

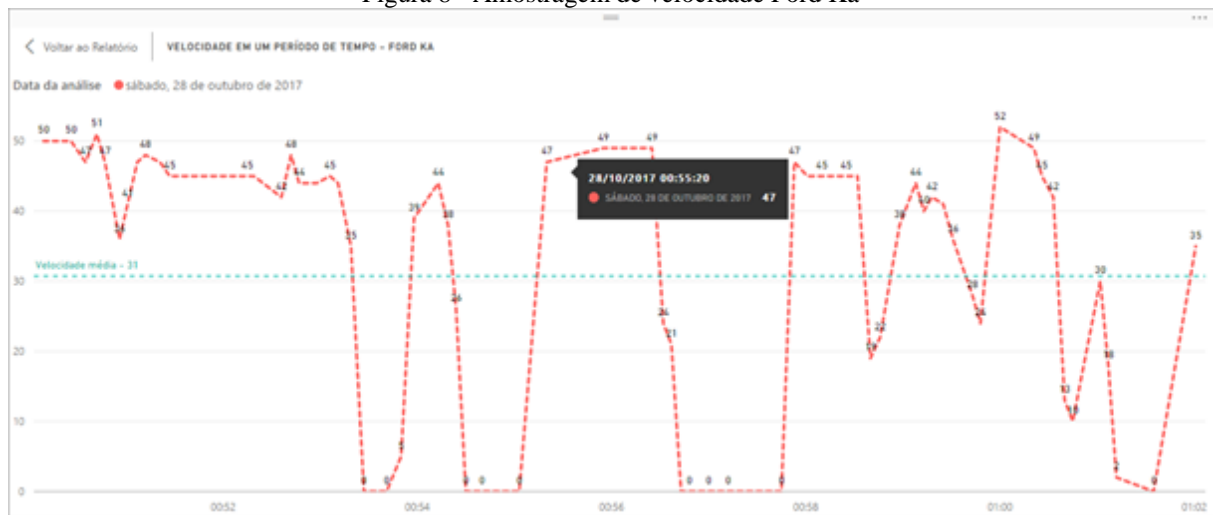
O aplicativo foi testado em dois veículos diferentes, um Ford Ká SE ano modelo 2017 1.0 e um Honda Fit LX ano modelo 2011 1.4, nos dias 27/10/2017 e 08/11/2017, respectivamente. Vale ressaltar que em veículos de modelos mais antigos foram constatadas incompatibilidades nos protocolos utilizados pelo OBD para comunicação com a ECU. Sendo assim, os veículos utilizados para os testes foram os mais compatíveis dentre os disponíveis.

O veículo Ford Ká realizou uma viagem entre as cidades de São Bernardo do Campo e Santo André no período noturno após às 23 horas. O Honda Fit realizou viagens entre as cidades de São Bernardo do Campo, São Caetano do Sul e São Paulo em diversos períodos do dia.



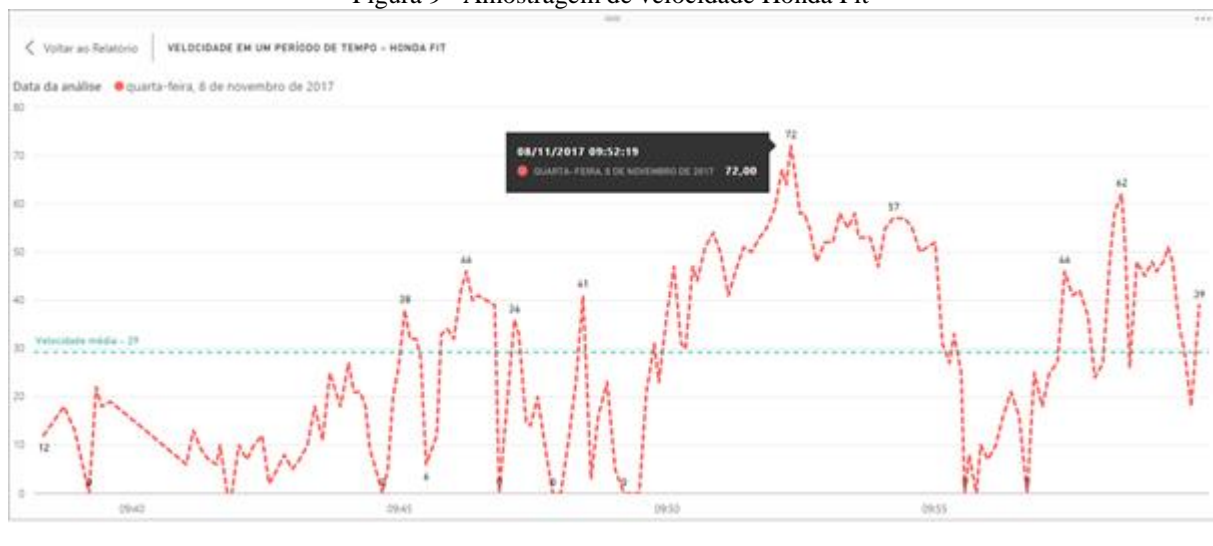
Utilizando os dados de velocidade, data e hora foi possível traçar um gráfico demonstrando a variação da velocidade em função do tempo. A figura 8 apresenta um gráfico com amostragem de 10 minutos com dados da viagem realizada pelo veículo Ford Ká na rodovia Anchieta (SP-150) na altura do Km 16.

Figura 8 - Amostragem de velocidade Ford Ká



A figura 9 apresenta a variação da velocidade em um trecho da viagem realizada pelo Honda Fit na Avenida das Nações, São Paulo.

Figura 9 - Amostragem de velocidade Honda Fit



Utilizando gráficos como apresentado anteriormente, seria possível traçar perfis de condutores avaliando sua maneira de conduzir o veículo, comparando os picos de velocidades

atingidas durante um período de tempo.

Também foi criado um mapa com o trajeto realizado pelo condutor durante a viagem de teste. A figura 10 apresenta o mapa de monitoramento da viagem do veículo Ford Ká, a mesma viagem utilizada para gerar o gráfico da figura 8. O trajeto iniciou-se na rodovia Anchieta Km 16, São Bernardo do Campo, e foi encerrado na rua Tóquio, Santo André, São Paulo.

Figura 10 - Mapa de monitoramento Ford Ká



A figura 11 apresenta o mapa de monitoramento do Honda Fit. O trajeto teve início na avenida das Nações Unidas, São Paulo, e encerrou-se no estacionamento da USP (Universidade de São Paulo).

Figura 11 - Mapa de monitoramento Honda Fit



Este mapa pode ser utilizado para monitoramento do comportamento do condutor e os locais por onde ele percorre, a fim de medir com maior precisão o risco envolvido no contrato do seguro. Podemos visualizar os locais por onde o motorista passou e onde estacionou o veículo, bem como data e hora destes eventos. Desta forma, será possível identificar se as informações declaradas no sinistro, como locais frequentados onde o carro permanece estacionado, são

verídicas.

### Considerações finais

O objetivo principal deste projeto foi o desenvolvimento de um protótipo para coleta e análise de dados provenientes de veículos automotores por meio da interface OBD utilizando os conceitos de IoT, com a finalidade de proporcionar às seguradoras uma visão da forma como os segurados conduzem os veículos, possibilitando a verificação das condições acordadas no contrato de prestação de serviço, o que pode trazer vantagens contratuais para ambos os interessados.

Os GEs do FIWARE (Orion e Cygnus) se mostraram eficientes na função de *back-end* para recepção e armazenamento dos dados enviados pelo aplicativo. O sistema de geolocalização provisionou os dados de latitude e longitude de forma precisa, mostrando-se eficiente em seu propósito, porém apresentou problemas, em locais que as condições climáticas e de alcance do sinal na região eram desfavoráveis.

Os testes realizados não foram capazes de validar o funcionamento da solução quando submetida a uma grande quantidade de veículos, sendo objeto dos trabalhos futuros. Durante os testes foram identificadas algumas incompatibilidades entre os protocolos de comunicação do OBD e da ECU, que serão analisados e corrigidos em trabalho futuro.

Os parâmetros de monitoramento selecionados nessa etapa não foram escolhidos seguindo uma metodologia que possa garantir com precisão a identificação de comportamentos que possam revelar que o motorista apresenta maus hábitos na condução do veículo, sendo necessário um estudo mais aprofundado para tal finalidade. Estes foram selecionados para a demonstração da solução e por serem informações básicas coletadas por sistemas desta natureza.

Um ponto a se destacar é a privacidade do condutor quando submetido a este sistema. O propósito desta solução, como dito anteriormente, é de traçar um perfil mais preciso do condutor para a seguradora poder mensurar o risco envolvido em contrato. Não foi levado em conta o sigilo destes dados, ficando assim a cargo da seguradora decidir como tratar tais informações.

Como próxima etapa para a redução de custos e otimização da solução, será desenvolvido um protótipo baseado na família de microcontroladores Atmel, que será acrescido das shields de GPS, Bluetooth e GSM e poderá ser instalado no veículo utilizando o seu sistema elétrico como fonte de alimentação substituindo o aplicativo desenvolvido para a elaboração deste artigo. O serviço de monitoramento e telemetria do veículo pode ficar em execução mesmo quando o veículo estiver desligado podendo atualizar a geolocalização do veículo sem a interferência do condutor.

Também será necessário realizar um estudo sobre a relevância das informações coletadas para a correta análise do perfil dos condutores através de técnicas de *big data*.

### Referências

ATZORI, L.; IERA, A.; MORABITO, G. **The Internet of Things: A survey**. Elsevier, p. 1, maio 2010.

FIWARE. About US. **FIWARE**, 2016. Disponível em: <<https://www.fiware.org/about-us/>>. Acesso em: 10 nov 2017.

FIWARE Foundation. **FIWARE Foundation**, 2017. Disponível em: <<https://www.fiware.org/foundation/>>. Acesso em: 7 nov. 2017.

JAYAVARDHANA, G. et al. **Internet of Things (IoT): A vision, architectural elements, and future directions**. *Future Generation Computer Systems*, v. 29, n. 7, set. 2013.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing**, set. 2011. 3.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing**. COMPUTER SECURITY RESOURCE CENTER, set. 2011. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-145/final>>. Acesso em: 6 dez. 2017.

NATIONAL INTELLIGENCE COUNCIL. **Disruptive civil technologies**. [S.l.]: [s.n.], abr. 2008.

PEDROSA, P. H. C.; NOGUEIRA, T. **Computação em nuvem**, 2011. 1.

RUSHEL, H.; ZANOTTO, M. S.; MOTA, W. C. D. **Computação em nuvem**, Curitiba, abr. 2010. 1-3.

SUSEP. SUSEP. [www.susep.gov.br](http://www.susep.gov.br), 09 out. 2017. **O que é o questionário de avaliação do risco**. Disponível em: <<http://www.susep.gov.br/setores-susep/cgpro/coseb/duvidas-dos-segurados-sobre-seguro-de-automoveis/o-que-e-questionario-de-avaliacao-do-risco>>. Acessado em 13 de Outubro de 2017.

SILVA, F. Fábio Silva, 2015. **Introdução ao Openstack**. Disponível em: <<https://fabiosilva.com.br/2015/04/12/introducao-ao-openstack/>>. Acesso em: 30 out. 2017.