CENTRO UNIVERSITÁRIO DO PARÁ - CESUPA

ESCOLA DE NEGÓCIOS, TECNOLOGIA E INOVAÇÃO - ARGO

CURSO DE ENGENHARIA DA COMPUTAÇÃO

**JHERSON HARYSON ALMEIDA PEREIRA**

**LUIS ENRIQUE GOMES PORTUGAL**

**RAPHAEL ROSSY PENA**

**Aplicação de Aspectos de Segurança em Comunicação de Redes Veicular**

BELÉM

ANO

JHERSON HARYSON ALMEIDA PEREIRA

LUIS ENRIQUE GOMES PORTUGAL

RAPHAEL ROSSY PENA

**Aplicação de Aspectos de Segurança em Comunicação de Redes Veicular**

Pré-projeto de TC apresentado ao Centro Universitário do Estado do Pará como requisito para obtenção de nota da disciplina de TC1 do curso de Engenharia da Computação na modalidade MONOGRAFIA.

Prof. MSc. Tatiana Araújo



[**1 INTRODUÇÃO 9**](#_heading=h.30j0zll)

[1.1 SITUAÇÃO PROBLEMA 9](#_heading=h.1fob9te)

[1.2 OBJETIVOS DO ESTUDO 9](#_heading=h.3znysh7)

[1.3 JUSTIFICATIVA 9](#_heading=h.2et92p0)

[1.4 METODOLOGIA DA PESQUISA 9](#_heading=h.tyjcwt)

[1.4 ESTRUTURA DO TRABALHO 10](#_heading=h.3dy6vkm)

[**2 REFERENCIAL TEÓRICO 11**](#_heading=h.1t3h5sf)

[2.1 REVISÃO DA LITERATURA (estado da arte) 11](#_heading=h.4d34og8)

[**2.1.1 Subseção 11**](#_heading=h.2s8eyo1)

[2.2 TRABALHOS RELACIONADOS 12](#_heading=h.26in1rg)

[**3 DESENVOLVIMENTO DA PROPOSTA / METODOLOGIA 13**](#_heading=h.lnxbz9)

[**4 CRONOGRAMA 14**](#_heading=h.35nkun2)

[**REFERÊNCIAS 15**](#_heading=h.1ksv4uv)

[**APÊNDICE A 17**](#_heading=h.44sinio)

[**APÊNDICE B 18**](#_heading=h.2jxsxqh)

[**ANEXO A 19**](#_heading=h.z337ya)

**1 INTRODUÇÃO**

O setor industrial que representa a cadeia de suprimentos automobilística possa ser bastante desenvolvido e maduro, onde cada vez mais é requerido produtos mais sofisticados e conectados, principalmente no que se refere a funcionalidades e principalmente com a inclusão de itens da computação embarcada automotiva.

Com o avanço da computação e da era da informação, cada vez mais os veículos automotivos dotam-se e apropiam-se dos mais variados tipos de tecnologia e sistemas, onde estes estão, cada vez mais, ganhando espaço no mercado e se tornando tão importante quanto as partes mecânicas e/ou de motorização do veículo. Dessa forma, esses sistemas controlam eletronicamente diversos aspectos do veículo, desde o sistema de tração e estabilidade, auxilio de partida em rampa, identificação de fadiga do motorista, auxílio de estacionamento dentre muitas outras funcionalidades.

A tendência do avanço da área de Tecnologias de Informação (T.I.) possibilita o desenvolvimento de novas aplicações viáveis nos mais diversos ramos e inclusive no ramo de sistemas embarcados. No setor automotivo, os sistemas embarcados, foram introduzidos, principalmente pela questão financeira; barateando e agilizando o processo de montagem. Outro fator que foi corroborado devido a implantação de sistemas embarcados, estão relacionados principalmente às funções de segurança e conforto, sendo amplamente introduzidas a partir de 2010, como: Keyless; Controle de tração e Estabilidade e Assistente de Partida em Rampa (WATZENIG; ARMENGAUD, 2011).

Atualmente se discute sobre redes veiculares sendo que sua principal característica envolve a comunicação entre veículos em uma escala geográfica ampla, essa tecnologia, também é conhecida como Vehicular AdHoc Netwoks (VANETS). Depois da adoção da computação embarcada automotiva em para fins de segurança e de seu sucesso foi notado a aplicabilidade em outras áreas dentro do veículo. No entanto, a utilização desses sistemas só foram amplamente introduzidos com o barateamento de produção, o que ocorreu devido à medida que o processamento e as comunicações de bordo tiveram redução de custos e se tornaram menos invasivos, dessa forma, se tornando escalável e viável para a produção em massa. É tendência cada vez mais os veículos possuírem um grande número de sensores para o monitoramento de funcionamento do motor, segurança e infotenimento. Algumas das aplicações comumente vistas de sensores em veículos como: a detecção da distância de um objeto; detecção do fechamento das portas; detecção do acoplamento do cinto de segurança; detecção do nível da bomba de combustível; detecção da porcentagem do deslocamento do pedal do acelerador. Dependendo da espécie de metrologia do sensor, a quantidade de informação gerada pode variar de acordo com a frequência da amostragem e a quantidade de dados que eles captam. Dessa forma, um sensor de temperatura pode gerar um byte por segundo assim como o processamento de imagens pode gerar um megabyte no mesmo espaço de tempo (GALHARDI, 2014).

Antigamente era de suma importância para os fabricantes e montadoras o ganho de peso devido a inclusão de novos sensores nos veículos, devido a essa inclusão, necessariamente dependia de fiações aplicadas especificamente para cada sensor adicionado ao veículo, aumentando o peso, e assim, o custo de produção, além de dificultar a manutenção e o rastreio de problemas e mau contatos devido ao grande número de conexões entre as fiações. Além disso outro ponto acarretado pelo antigo modelo de produção é o fato da confiabilidade da informação não poder ser garantida devido ao grande número de interferência. Assim tiveram origem da utilização de CPUs de uso geral dentro dos veículos (LEEN; HEFFERNAN, 2002) e ao seu padrão de comunicação baseado em barramentos (BUS), com fiação compartilhada entre as Unidades de Processamento.

E para padronizar o protocolo de comunicação foi desenvolvido durante a década de 80 a rede CAN (Controller Area Network) (LEEN; HEFFERMAN, 2002).

Nos final da década de 80, surge para solucionar a necessidade de monitoramento das informações dos veículos, o On-Board Diagnostic (OBD). O OBD proporciona um padrão de de interface comunição com o veículo e suas Unidades de Processamento internas, dando acesso a rede veicular e facilitando a obtenção de dados de sensores, atuadores, baterias e CPUs no veículo.

Se tornou possível a introdução do OBD devido ao desenvolvimento acelerado da indústria de microcontroladores e de técnicas de engenharia, proporcionado um cenário bastante atrativo para utilização desses sistemas nas mais variadas áreas.

Inicialmente o OBD era bastante restrito, possuindo as seguintes funcionalidades:

* Monitoramento de sensores.
* Códigos de falhas de sensores.

Durante os anos de 1990 foi desenvolvida uma nova versão do On-Board Diagnostic, chamada OBDII que devido a maior gama de sensores e CPUs nos veículos, proporcionou um cenário mais atrativo para implantação de novas funcionalidades, tais como:

* Monitoramento dos sistemas de gases de escape e componentes que referem mau funcionamento ou de falha, de importantes sistemas e componentes de redução de emissões (catalisador, sensor lambda), injeção eletrônica.
* Armazenamento de falhas e das condições de operação associadas.
* Leitura da memória de falhas através de leitores.

Atualmente Existem diversas aplicações independentes são desenvolvidas com o foco em análise e disponibilização dos dados informados pelas CPUs veiculares com relação ao estado do veículo. Entre as aplicações existentes com as mais variadas funções, sendo algumas delas:

* Análise dos códigos de falha;
* Uso do smartphone como computador de bordo;
* Análise de perfil do motorista;
* Análise das condições de tráfego;
* Diagnóstico preventivo;

O acesso aos dados varia de acordo com as informações disponibilizadas por cada montadora porém a maioria das montadoras atualmente adotam o padrão OBDII (PORTAL G1, 2014). Os principais aplicativos no Brasil que utilizam a interface de comunicação OBDII para obtenção de dados veiculares são:

* Carrorama - 2014
* Engine App (Waze) - 2017
* Torque - 2018

O OBDII além da interface de comunicação, também possibilita, uma série de aplicações desenvolvidas em cima do padrão OBDII, onde softwares e hardwares podem consultar proativamente um serviço de informação de uma unidade, e compartilhar essa informação com a internet ou armazenar em um banco de dados externo ao sistema, bem como possibilitar um banco de dados para análise e diagnóstico de veículos. Dessa forma, o sistema pode obter informações de temperatura do ambiente e compartilhar com servidores e contribuir para a previsão do clima. Outro exemplo seria a utilização dessas informações para contribuir no desenvolvimento de mapas e na precisão do tempo estimado de um determinado percurso (PORTAL G1, 2018).

Cottingham e Davies (2007) descrevem que as aplicações citadas acima, envolvem um alto nível de complexidade de comunicação e sincronização de computação para processar os dados em um grande número de veículos, tornando o extremamente desafiador a implementação desses sistemas. Cottingham e Davies (2007) citam quatro pontos principais:

* Comunicação sem fio com outros veículos e com a Internet.
* Capacidade de se adaptarem a conectividade dinamicamente.
* Recurso computacional disponível executados em tempo real.
* Heterogeneidade da rede (recursos computacionais, de armazenamento, energia e comunicação).

Aplicações devem extrair o máximo dos recursos de maneira que a implementação destas pode ser estimulada pela existência de plataformas de computação de uso geral em veículos, onde os fabricantes e montadoras de veículos, podem desenvolver e compartilhar seus próprios softwares e/ou hardwares, facilitando o desenvolvimento de novas soluções. Uma das aplicabilidades visada pelo mercado automotivo envolve a coleta, o processamento e a distribuição de dados de sensores captados em veículos, visando se tornar uma plataforma em uma rede de sensores sem fio de grande escala.

1.1 SITUAÇÃO PROBLEMA

Atualmente qualquer sistema conectado a rede interna de um veículo por meio da interface OBDII pode obter dados do veículo, compartilhá los em rede e enviar comandos diretamente para CPUs. Essa flexibilidade trás problemas de vulnerabilidade de segurança e sigilo de informações.

Os principais pilares da segurança da informação foram definidos pela Organização Internacional de Normalização (ISO) na norma ISO/IEC 17799, que define a segurança da informação nos seguintes pontos:

* Confidencialidade: Garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada;
* Integridade: A informação é imutável, um dado não pode ser alterado por inconsistência do sistema ou por terceiros
* Disponibilidade: Um sistema deve manter se disponível e operante durante toda a sua execução

Os veículos tendem a ser cada vez mais assistidos por centrais eletrônicas, e com o avanço da Internet das Coisas (IoT) que está ganhando espaço progressivamente; é uma tendência que veículos possuam mais conectividade com a internet. Entretanto, um dos fatores negativos deste avanço tecnológico é a exposição de vulnerabilidades do sistema, possibilitando acesso por pessoal não autorizado a informações do veículo e até mesmo ao envio de comandos remotamente através da rede de internet.

Essas vulnerabilidades se dão por não ter uma camada de segurança explícita entre o usuários e a CPUs, onde a comunicação com o sistema é feita acessando fisicamente o barramento de comunicação proporcionado pela interface OBDII, facilitando o envio de qualquer comando para a Unidade de Processamento do veículo, e desta forma, facilitando o compartilhamento em rede, sem nenhum padrão de segurança estabelecido.

1.2 OBJETIVOS DO ESTUDO

Este trabalho tem como objetivo geral o desenvolvimento de uma modelo de comunicação veicular com inclusão de aspectos de segurança para a perspectiva de mercado automotivo.

E como objetivos específicos:

* Desenvolver um microcontrolador para comunicação com a CPUs do veículo
* Coletar dados veiculares provenientes dos sensores e atuadores
* Desenvolver um sistema de transmissão de dados de dados para a internet
* Desenvolver a camada de segurança que garanta a consistência dos dados durante a transmissão de dados
* Desenvolver a camada de segurança que garanta a consistência dos dados durante o armazenamento
* Armazenar as informações em um banco de dados
* Disponibilizar os dados coletados em uma plataforma

1.3 JUSTIFICATIVA

Com o crescente avanço de tecnologias embarcadas e de internet das coisas aplicadas em soluções automobilísticas é notório que veículos estão se tornando progressivamente mais conectados à rede mundial de computadores. Atualmente existem várias soluções independentes para a análise de informações, gestão e controle de dados dos sensores de veículos através do protocolo OBDII . Essa fácil comunicação proporcionada a nível físico com as CPUs dos veículos e com a conexão das mesmas com a internet expõe vulnerabilidades que podem ser exploradas por hacker e por pessoas mal intencionadas (DE SOUZA: MARCELO, 2015).

1.4 METODOLOGIA DA PESQUISA

Inicialmente, uma pesquisa bibliográfica foi desenvolvida, para identificar as principais interfaces de comunicação com as centrais eletrônicas veiculares. Esses estudos revelaram os principais protocolos de comunicação existente na maioria dos veículos, obrigatoriamente a partir de 2010. Tais protocolos são baseados em rede *CAN Bus*, *LIN Bus*  e possuem interface OBDII como seu padrão. Posteriormente foi desenvolvido uma pesquisa voltada à identificação dos meios e dos protocolos de comunicação externa ao veículo, e como soluções já desenvolvidas consolidadas no mercado o fazem. A partir desse levantamentos analisou-se modelos e arquiteturas de comunicação com ECU (Unidades centrais eletrônicas) embarcadas em veículos automotivos, bem como os sistemas e plataformas de disponibilização de informações destes sistemas embarcados, a fim de analisar os principais problemas e falhas de segurança na comunicação tanto interna (comunicação com o veículo), quanto externa (comunicação com a internet). Dessa forma utilizou-se o utilizou-se o método hipotético-dedutivo, para formular uma melhoria nas arquiteturas de comunicação veiculares, dotando-os de maior confiabilidade e confidencialidade, a fim de garantir maior segurança de informações no sistema automotivo, em suas comunicações em rede tanto interna quanto externa.

Segundo Aguiar (2011), o método hipotético-dedutivo ampliou-se dando uma ampla liberdade à criação de hipóteses sem deixar a exigência do processo de testes, sendo suficiente para confirmar uma hipótese.

1.4 ESTRUTURA DO TRABALHO

Explicar em um parágrafo a estrutura do seu trabalho, por exemplo:

O trabalho consiste em um primeiro capítulo contendo a introdução, onde é apresentado o tema, o problema de pesquisa, a pergunta que norteou o estudo e os objetivos. No segundo capítulo, abordou-se o referencial teórico e as suas categorias – ZZZZZ; XXXX; YYYY – enquanto no terceiro capítulo, apresenta-se o desenvolvimento da proposta/metodologia, que se baseou na execução do programa X para chegar ao resultado Y. Os programas utilizados foram x y z. O quarto capítulo discorreu sobre a análise dos dados, enquanto que o quinto, sobre a discussão dos dados; seguido das considerações finais.

**2 REFERENCIAL TEÓRICO**

Os Sistemas Embarcados foram possibilitados através do avanço dos componentes eletrônicos, sendo bem semelhantes aos computadores modernos, principalmente no que diz respeito à capacidade execução de um conjunto de tarefas de forma mais rápida, porém limitada a um pequeno conjunto de tarefas sendo composto por hardware e software integrado, cuja a funcionalidade é executar um conjunto de tarefas repetidamente (EDWARDS, 2003).

Diferentemente de um PC (*personal computer*), os sistemas embarcados são desenvolvidos para serem extremamente baratos, pequenos e econômicos no quesito de consumo energético, responsáveis por executar com excelência um pequeno conjunto de instruções (SHIBU, 2009).

Atualmente muitos sistemas que possuem alguma parte “inteligentes” possui um microcontrolador. Na indústria automotiva esse cenário não é diferente, principalmente para a diminuição de custo com fiação e aumento da confiabilidade de informação e da comunicação, dessa forma os sistemas embarcados em microcontroladores são embutidos em veículos para otimizar e acelerar a produção, além de baratear os custos de manutenção como em funcionalidades descritas por Watzenig e Armengaud (2011).

Palocz-Andresen (2012) descreve que devido à evolução do sistemas embarcados embutido em veículos e ao grande número de dados sendo obtidos pelos sensores e aos novos protocolos de comunicação que foram desenvolvidos, corroborou para uma dificuldade para a análise de um veículo devido justamente a essa grande diversidade de padrões. Visando solucionar o problema da padronização, foi reconhecida pela legislação do Estados Unidos, a necessidade padronização na interface de comunicação com os veículos. Surge dessa forma a interface de comunicação *On-Board Diagnostic* (OBD) que posteriormente vem a evoluir para o padrão OBDII para acompanhar o avanço acelerado e o crescente aumento do número de protocolos e dispositivos embarcados nos veículos (PALOCZ-ANDRESEN, 2012).

Atualmente existem várias tecnologias focadas em segurança, desde algoritmos de alto a protocolos de comunicação, estes sistemas em sua maioria buscam trazer aspectos de confidencialidade e autenticidade. Tecnologias a nível de aplicação como JWT (*JSON Web Token*) e OAuth2 são muito utilizadas em sistemas para garantir acesso a informação em sistemas. Outra tecnologia bastante disruptiva e em alta no mercado são as *Blockchains* (Cadeia de Blocos), que garantem a imutabilidade de dados utilizando processamento distribuído.

O *JSON Web Token* (JWT) é um padrão da Internet para criar tokens de acesso baseados em *JSON* (*JavaScript Object Notation*). Por exemplo, a solicitação de acesso de um cliente a um serviço específico do servidor é geralmente controlada através de um sistema de *login,*  ao usuário enviar suas credenciais para o servidor, é analisado se o usuário realmente existe e na base de dados, e caso verdade o servidor devolverá ao cliente uma chave secreta de acesso (*token*) que a cada nova requisição ao servidor o usuário deverá enviá-la junto para garantir que o servidor realmente deu acesso aquele cliente, por sua vez, a cada requisição bem sucedida o servidor pode gerar um novo token trabalhando com o conceito de *refresh token,* o servidor receberá esse token e verificará se o usuário é válido e se ainda pode acessar o sistema, caso contrário o servidor pode requerer do usuário um novo *login* a fim de validar a autenticidade do usuário e assegurar a segurança do sistema.

O OAuth é outra forma de garantir o acesso aos recursos de um sistema, sendo um padrão aberto para autorização, comumente utilizado para permitir que os usuários em rede, sem expor suas senhas. O OAuth fornece aos clientes de uma aplicação um "acesso seguro delegado" aos recursos do servidor em nome do proprietário do recurso. Ele especifica um processo para proprietários de recursos para autorizar o acesso de terceiros aos seus recursos de servidor sem compartilhar suas credenciais. Projetado especificamente para trabalhar com o Protocolo de Transferência de Hipertexto (HTTP), o OAuth permite essencialmente tokens de acesso a ser emitidos para clientes de terceiros, mediante autorização do servidor, com a aprovação do proprietário do recurso. O terceiro, em seguida, usa o token de acesso para recursos protegidos hospedados pelo servidor.

O conceito de blockchain foi introduzido primeira vez em 2018 por Satoshi Nakamoto em resposta à crise econômica dos Estados Unidos (DEBABRATA; ALBERT, 2018). Segundo Nakamoto (2008), a blockchain propõe um sistema para transações sem precisar de um terceiro que garanta confiança. Uma aplicação sugerida por Allayannis (2018) permite qualquer rede de usuários rastrear e comercializar virtualmente qualquer coisa de valor.

Acerca do cenário atual discutido por Nakamoto (2008), onde as instituições financeiras servem como as partes confiáveis na hora de processar pagamentos eletrônicos (NAKAMOTO, 2008). Sendo, desta forma, um centralizador de informação cujo as partes devem confiar no intermediador para serem garantidas e certificadas da existência e histórico das transações. A problematização é que um único órgão é responsável por gerir e assegurar todas as informações. Porém segundo o modelo descentralizado ao invés da existência de um terceiro para comprovar e assegurar que uma dada informação ou transação realmente ocorreu, o sistema utiliza todos os “nós” integrantes na rede para compartilhar essa informação, dessa forma, se caso um valor em um único nó seja alterado, como a injeção ilegal de dinheiro em uma conta, todos os demais nós possuem uma prova de que essa informação não é verdadeira, por sua vez não validando a transação e assegurando a autenticidade das transações em todos os nós.

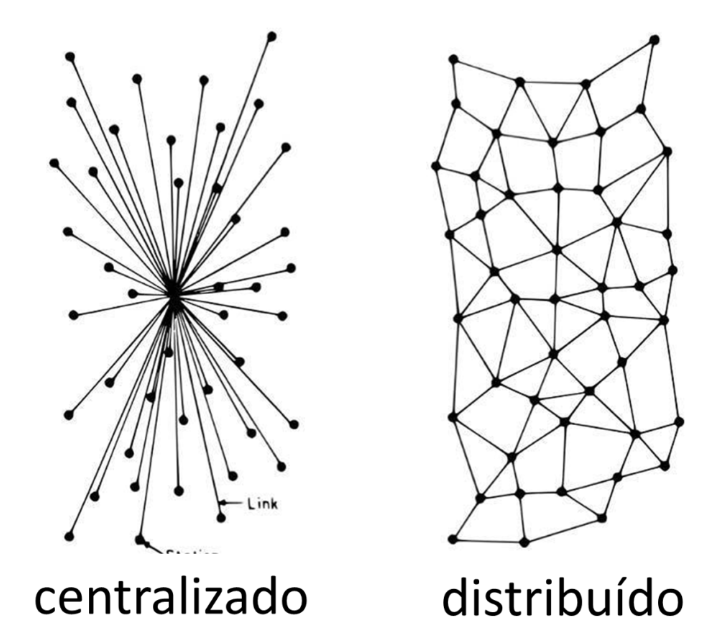


Figura 1 - Arquitetura Centralizada x Descentralizada Fonte: imagem da internet

2.1 REVISÃO DA LITERATURA

A fim de melhorar a extração de informação da interface OBD, Jhou et al. (2013) apresentam um conjunto de sistemas, que por meio de um dispositivo ELM327 conectado na interface, obtém informação veículo e replicando-as para um sistema baseado em experiência em nuvem. o sistema faz a análise das informações recebidas e informa falhas através de alertas para o usuário com informações detalhadas.

Devido o aumento de veículos nas ruas, surge uma também a necessidade de sistemas capazes de auxiliar o motorista durante a direção. De acordo com a empresa McKinsey & Company (2016), a perspectiva para o ano de 2030 é de que 15% dos veículos produzidos sejam totalmente autônomos, com isso a segurança no trânsito será maior.

Montadoras de veículos incentivam seus clientes a utilizarem seus softwares em smartphones para que o cliente mantenha tanto um canal de comunicação com a empresa disponibilizando informações de seu veículo para o cliente assim como também se beneficia utilizando *logs*  de dados da utilização do veículo e do perfil do motorista. Com o avanço da conectividade cada vez mais se torna real a preocupação gerada pela possibilidade do elevado número de aplicações capazes de trocar informações relacionadas ao sistema e ao usuário, aumente a probabilidade ataques cibernéticos no cenário automotivo cenário (YAN, 2015).

O objetivo durante o trabalho de pesquisa no período de dois anos de Yan (2015), foi o de identificar falhas de segurança nas diferentes formas de comunicação de um veículo. Tais falhas como a falta de criptografia em protocolos utilizado por montadoras, permite, que pessoas mal-intencionadas capturem os dados de um usuário e acesse a sua conta. Outra falha notada por Yan (2015) foi identificada durante a comunicação entre a aplicação e o servidor em empresas de locação de veículo, expondo vulnerabilidades do sistema permitindo o acesso por pessoal não autorizado de informações de usuários.

2.2 TRABALHOS RELACIONADOS

O resumo de modelos e trabalhos relacionados que utilizam a comunicação veicular foram indicadas abaixo:

**Quadro 1 ‒ Resumo de Publicações Referentes à comunicação e extração de dados veiculares**

|  |  |
| --- | --- |
| *SafeDrive Online Driving Anomaly Detection From Large-Scale Vehicle Data* | Zhang et al. (2013) propõem um sistema para detectar anomalias no comportamento de motoristas. |
| *An Intelligent Vehicular Telematics Platform for Vehicle Driving Safety Supporting System* | Chen et al. (2015) propõem um sistema com aplicativo capaz de obter informações do veículo e alertar o usuário em caso de falhas, além armazenar os dados em nuvem a fim de propor maior segurança ao motorista. |
| *Captura E Disponibilização Em Nuvem De Logs Automotivos: A*  *Construção De Artefatos De Softwares Para Coleta E*  *Gerenciamento De Anomalias* | Bulgarelli (2018) propõe um sistema para captura e disponibilização em nuvem de logs automotivos gerenciamento de anomalias |
| *Memory Optimized Lifetime Vehicle Data Acquisition Framework* | Athavan e Radhika (2015) propõem uma solução para a redução do tamanho da ocupação em disco dos dados gerados pelo sistema de comunicação veicular. |

Os trabalhos listados acima focam principalmente no modelo de sistemas cujo o objetivo é obter informação do veículo e disponibilizá la para algum tipo de usuário, podendo ser o proprietário do veículo ou a montadora. São poucos linhas de pesquisa nessa área que se preocupam diretamente com a segurança da informação e todo o processo de transmissão e armazenamento de dados de maneira segura.

# 

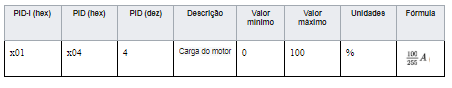
# 3 DESENVOLVIMENTO DA PROPOSTA / METODOLOGIA

Como forma de explorar a necessidade apontada pelo estudo, uma modelo inicial foi proposto. Utilizando-se do método de tentativa e erro chegou-se ao resultado de uma solução composta contendo: Hardware, Servidor, Banco de Dados, Sistema Web e Mobile. Para a composição desta solução, foram consultados sites e manuais de desenvolvimento de aplicações e ferramentas.

3.1 COMUNICAÇÃO

A comunicação com a ECU utiliza o protocolo de comunicação estabelecido pela Bosch para fazer leituras dos sensores dos veículos. O protocolo é baseado padrão OBD-II identificados pelo PID (identificador de processos), conforme definido pela SAE J1979(ISO/IEC 7498-1, 2012). A resposta esperada para cada PID é fornecida, juntamente com informações sobre como converter a resposta em dados significativos. A interface OBD-II aceita requisições obedecendo o protocolo de comunicação enviando os dados em hexadecimal demonstrada na tabela 2 abaixo.

(ABNT)

Tabela 2: Código de comunicação para obter a informação da carga do motor de um veículo Fonte: Os autores (ano)

3.2 OBTENÇÃO DE DADOS

A obtenção de dados foi desenvolvido utilizando a comunicação descrita no tópico 3.1 entre o hardware desenvolvido e a central eletrônica do veículo (ECU). Através dos protocolos de comunicação o dispositivo requisita a ECU para realizar leituras de diversos sensores contidos no veículo. Após a requisição dos dados a ECU retorna ao requisitante os valores obtidos.

3.3 TRANSMISSÃO DE DADOS

Cada computador de bordo do veículo deverá provar aos servidores que estão de fato habilitados a enviar dados utilizando o OAuth como meio de certificação de autenticação por meio de um token de autorização. O mesmo cenário é utilizado para os clientes da aplicação que desejam consumir informação.

Para transmitir e receber dados pela rede os dispositivos deverão primeiro se conectar ao servidor de autorização para receber as credenciais necessárias para ter acesso aos recursos do servidor. O fluxo de informação é demonstrado na figura 2 abaixo.

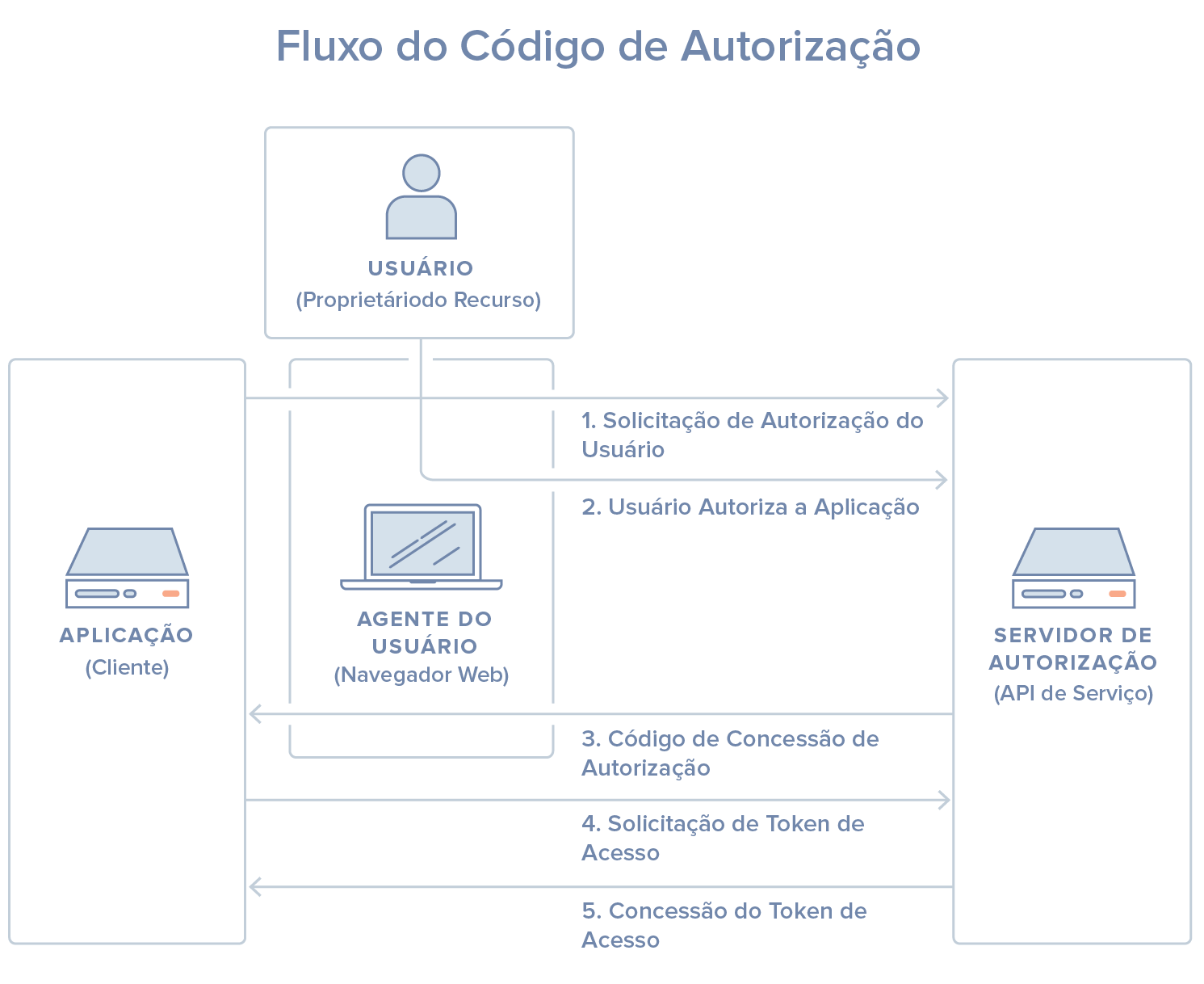


Figura 2 - Fluxo de autenticação utilizada pelo sistema

Fonte: https://www.digitalocean.com/community/tutorials/uma-introducao-ao-oauth-2-pt

Após os usuários e dispositivos receberem as credenciais do servidor de autorização o s serão redirecionados ao servidor de aplicação do sistema.

Para assegurar a segurança durante a transmissão da informação foi implementado a funcionalidade de *refresh token*. O *refresh token* é um método de que sistema cliente consiga requisitar um novo token a cada requisição, ou devido a expiração da validade do mesmo, prevenindo interceptações e a reutilização desse token por terceiros.

3.4 ARMAZENAMENTO DE DADOS

Diante da demanda de dados que trafega do microcontrolador para o banco de dados, foi projetado o uso de um modelo de dados NoSQL com o banco de dados MongoDB, esta última apresenta alta performance, ideal para grande quantidades de dados, uma vez que sua base foi pensada visando o uso em soluções de Big Data, possibilita a expansão no escalonamento horizontal e vertical, seu uso ainda possui tecnologias como replica sets e sharding, o que permite backup e redundância, além de ser uma tecnologia que vem crescendo rapidamente nos últimos anos como mostra a figura 3.

Sua função no projeto é armazenar os dados enviados dos sensores OBDII, persistindo e disponibilizando de forma rápida, segura e eficiente esses dados, junto com o Blockchain assegura que a transação que envia esses dados seja feita com total segurança e com os dados íntegros.

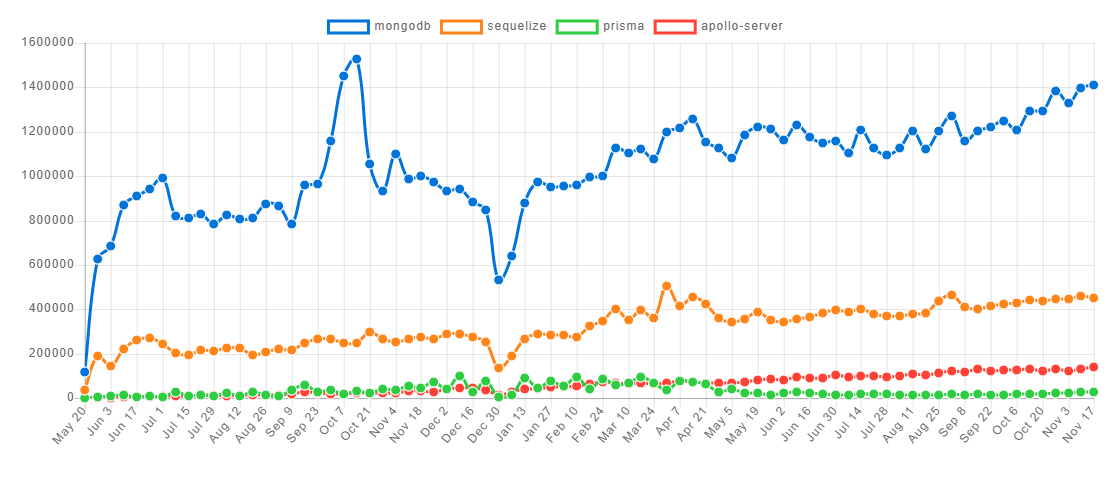


Figura 3 - comparativo dos bancos de dados mongodb, sequelize, prisma e apollo-server nos últimos 2 anos

Fonte: https://www.npmtrends.com/mongodb-vs-sequelize-vs-prisma-vs-apollo-server

3.5 DISPONIBILIZAÇÃO DE INFORMAÇÃO

A disponibilidade dos dados armazenados através de um sistema web foi realizada exclusivamente para as fabricantes dos automóveis ter acesso a painéis digitais de todas as informações repassadas pelo microcontrolador e armazenadas, além de ações de correção e manutenção das funções do automóvel.

A fabricante do automóvel acessa o sistema através de autenticação de login e senha, seguindo o modelo JWT como mostrado na figura 4, sendo os dados trafegados sempre com criptografia de ponta-a-ponta, tanto dos dados de login, tanto quanto os dados e informações do automóvel que alimentam os gráficos e tabelas do sistema.

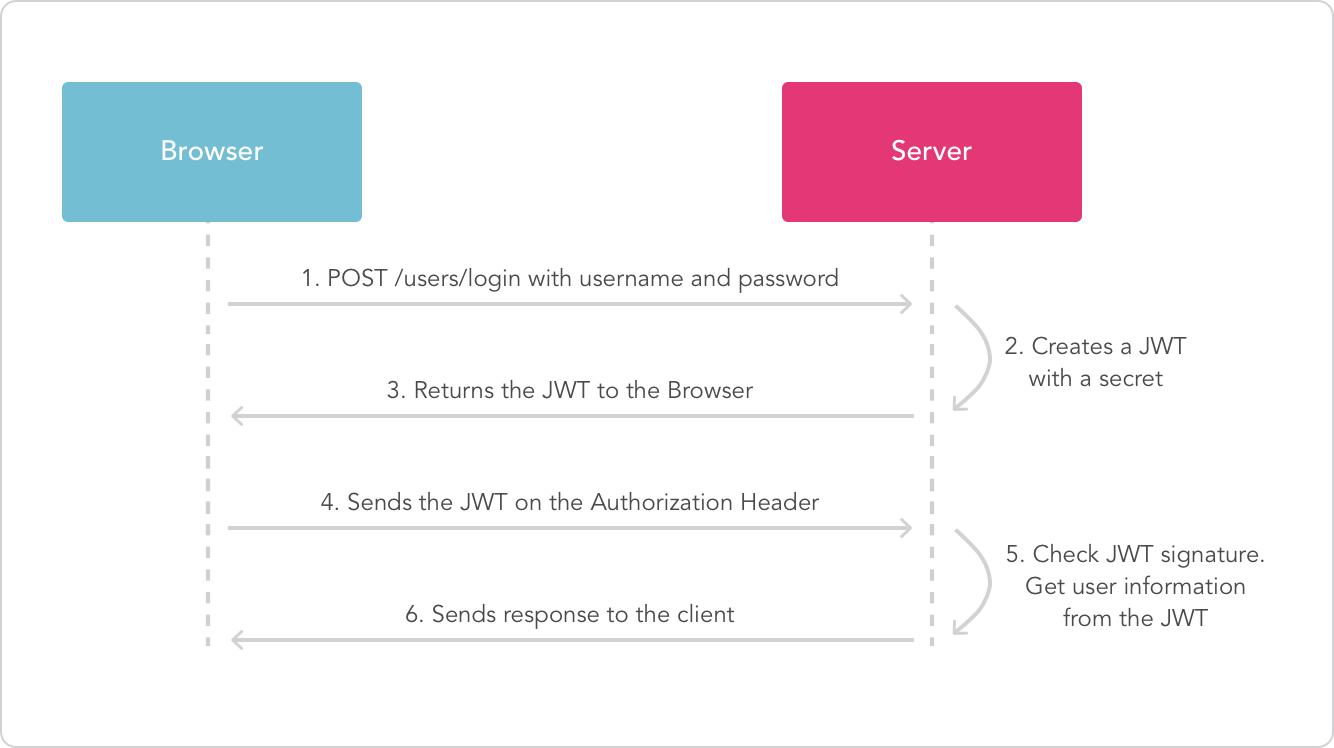


Figura 4 - Diagrama de sequência usando token JWT

Fonte: https://medium.com/tableless/entendendo-tokens-jwt-json-web-token-413c6d1397f6

O JWT é um padrão ([RFC-7519](https://tools.ietf.org/html/rfc7519)) de mercado que define como transmitir e armazenar objetos JSON de forma compacta e segura entre diferentes aplicações. Os dados nele contidos podem ser validados a qualquer momento pois o token é assinado digitalmente (NASCIMENTO, 2018).

Uma vez logado, o usuário tem disponível uma busca dos automóveis fabricados por ela, a busca ocorre principalmente pelo chassi do veículo, tendo porém outras opções de busca como: marca, modelo, ano, cor etc. Feito isso, o usuário da fabricante pode visualizar os dados armazenados através de gráficos e listas, além de ter o controle sobre ações que possa ser executado no veículo.

A disponibilidade dos dados armazenados através de um sistema mobile foi realizada exclusivamente para os usuários/donos dos automóveis ter acesso aos painéis digitais das informações armazenadas somente, sem acesso às funcionalidades de correção e manutenção do automóvel.

Como o objetivo deste projeto é a inclusão de aspectos de segurança para a perspectiva de mercado automotivo, na versão mobile o usuário pode acessar o aplicativo através de login e senha, gerando um token criptografado (figura 5) com as informações dele.

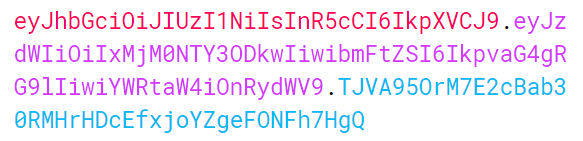
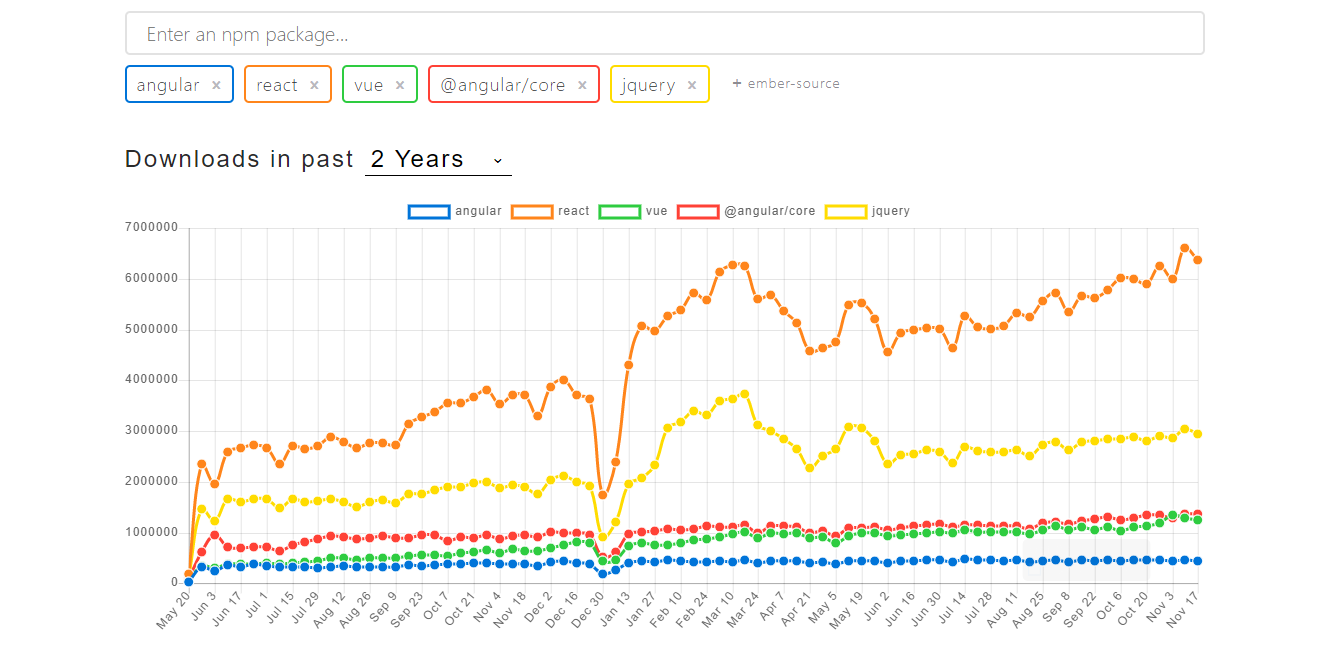


Figura 5 - Token JWT

Fonte: https://medium.com/tableless/entendendo-tokens-jwt-json-web-token-413c6d1397f6

No entanto, para acessar os dados armazenados do seu veículo, o dono é sujeito a validação da conta pela fabricante, através do chassi do automóvel, uma vez validado o dono pode visualizar os gráficos, além de receber notificações sobre possíveis falhas e bugs do veículo, podendo sempre enviar um feedback para a fabricante, que pode corrigir remotamente ou presencialmente com a ajuda de um técnico.

Para desenvolver o modelo proposto no projeto foi utilizado a linguagem de programação Javascript aliado a biblioteca react e react native, tendência de mercado e comprovado por pesquisas sendo a biblioteca mais utilizada quando comparada com suas concorrentes, figura 6.

Figura 6 - comparativo das tecnologias angular, react, vue, @angular/core e jquery nos últimos 2 anos

Fonte: https://www.npmtrends.com/angular-vs-react-vs-vue-vs-@angular/core-vs-jquery

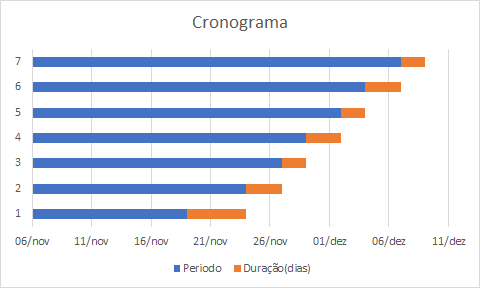
# 

# 

# 

# 

# 4 CRONOGRAMA



**Legenda:**

1 - Desenvolver um microcontrolador para comunicação com a CPUs do veículo;

- Criação de um sistema embarcado;

- Teste do sistema;

- Validação do sistema.

2 - Coletar dados veiculares provenientes dos sensores e atuadores;

- Coleta de dados via OBDII;

- Teste de dados para fins analíticos;

- Validação dos valores coletados.

3 - Desenvolver um sistema de transmissão de dados para a internet;

- Teste de utilização do OAuth;

- Validação de transmissão única de cada carro.

4 - Desenvolver a camada de segurança que garanta a consistência dos dados durante a transmissão de dados;

- Teste de funcionalidade refresh token;

- Validação.

5 - Desenvolver a camada de segurança que garanta a consistência dos dados durante o armazenamento de dados;

- Criação do blockchain;

- Utilização do OBDII para garantir a consistência dos dados.

6 - Armazenar as informações em um banco de dados;

- Teste do modelo de dados NoSQL;

- Validação dos resultados obtidos pelo banco de dados MongoDB.

7 - Disponibilizar os dados coletados em uma plataforma.

- Utilização da linguagem JavaScript;

- Teste do modelo JWT com refresh token;

- Visualização de dados em uma plataforma.

**REFERÊNCIAS**

ABUALI, N. **Advanced Vehicular Sensing of Road Artifacts and Driver Behavior**. IEEE, 2015.

ALLASSI, T. T.; MARTINS, L. E. G. Um Estudo Exploratório sobre Sistemas Operacionais Embarcados. **Revista Técnica Fatec Americana**, v.1. p.78-105, 2014.

ALLAYANNIS, G. Y; FERNSTROM, A. **Bitcoin: Investment or Illusion?**. University of Virginia, Darden Business Publishing. 2018.

BEI, X.; CHEN, N.; ZHANG, S. **On the Complexity of Trial and Error**. ACM, 2013.

ATHAVAN, Aravindhan; RADHIKA, N. **Memory Optimized Lifetime Vehicle Data Acquisition Framework**. IEEE, 2015.

BULGARELLI, G. **Captura E Disponibilização Em Nuvem De Logs Automotivos: A Construção De Artefatos De Softwares Para Coleta E Gerenciamento De Anomalias.** 2018**.** Dissertação (Mestrado em Administração). Centro Estadual De Educação Tecnológica Paula Souza Unidade De Pós-graduação, Extensão E Pesquisa. 2018.

CHEN, L.; LI, H.; CHANG, H.; TANG, J.; LI, K. S. **An Intelligent Vehicular Telematics Platform for Vehicle Driving Safety Supporting System**. IEEE, 2015.

DE SOUZA: MARCELO. Vulnerabilidades em Sistemas Automotivos **.XXIII Simpósio Internacional de Engenharia Automotiva**, At São Paulo, 2015.

DEBABRATA, Gosh; ALBERT, Tan. A Framework for Implementing Blockchain Technologies to Improve Supply Chain Performance. **MIT Global SCALE**. Work Pap.– 2018.

EDWARDS, S. A. Design Languages for Embedded Systems. **Columbia University**, 2003.

FRIEDRICH, A.; TAPPE, M.; GARMS, S.; PALOCZ-ANDRESEN M.; SCHROLL, S. OnBoard-Diagnose (OBD) und On-Board\_Messung (OBM) im Kraftfahrzeug. WLB Wasser, Luft und Boden, 1998.

GALHARDI, A. C. New trends in Automotive Embedded System Design. **SAE International**, 2014.

iMasters. **MongoDB para iniciantes em NoSQL**. Disponivel em: <<https://imasters.com.br/banco-de-dados/mongodb-para-iniciantes-em-nosql>>. Acesso em: 24 ago. 2019.

JHOU, J.; CHEN, S.; TSAY, E.; LAI, M. **The Implementation of OBD-II Vehicle Diagnosis System Integrated with Cloud Computation Technology**. IEEE, 2013.

LEEN, G.; HEFFERNAN, D. Expanding automotive electronic systems. **IEEE**, 2002.

MCKINSEY & COMPANY. **Automotive Revolution – perspective towards 2030**. Advanced Industries, jan. de 2016.

YAN, W. **A two-year Survey on Security Challenges in Automotive Threat Landscape**. IEEE, 2015.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2008.

NASCIMENTO, W. **Entendendo tokens JWT (Json Web Token)**. Medium. Disponível em: <<https://medium.com/tableless/entendendo-tokens-jwt-json-web-token-413c6d1397f6>>

Acesso em: 20 nov. 2019.

PORTAL G1. **Aplicativo ‘traduz’ dados de veículo em tempo real para motoristas**. G1- Sorocaba-Jundiaí, 2014. Disponível em: <http://g1.globo.com/sao-paulo/sorocaba-jundiai/

noticia/2014/10/aplicativo-traduz-dados-de-veiculo-em-tempo-real-para-usuarios.html>

Acesso em: 10 fev. 2018.

SAE J1979. **J1979: E/E Diagnostic Test Modes - SAE International.** Disponivel em: <https://www.sae.org/standards/content/j1979_201202/>. Acesso em: 24 ago. 2019.

SHIBU, K. V. Introduction to Embedded Systems. **Tata McGraw-Hill**, 2009.

WATZENIG, D.; ARMENGAUD, E. Automotive Embedded Systems. **Elektrotechnik & Informationstechnik**, 2011.