



Arquiteturas de Fog Computing para Internet das coisas nas plataformas Fiware e Helix

*Fog Computing Architectures for Internet of
Things based on Fiware and Helix Platforms*

Fillipo Valiante Filho (filippo@usp.br)

Doutorando em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo (Poli-USP) e professor do Centro Universitário Senac e da Faculdade de Tecnologia Termomecânica (FTT).

Fábio Henrique Cabrini (fabio.cabrini@usp.br)

Doutorando em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo (Poli-USP) e professor da Faculdade de Informática e Administração Paulista (Fiap), da Faculdade de Tecnologia de São Caetano do Sul (Fatec) e da Faculdade de Tecnologia Termomecânica (FTT).

Sérgio Takeo Kofuji (kofuji@usp.br)

Doutor em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo (Poli-USP) e professor da Poli-USP.

FTT Journal of Engineering and Business. • SÃO BERNARDO DO CAMPO, SP

DEZ. 2019 • ISSN 2525-8729

Submissão: 2 jul. 2019. Aceitação:

18 Out.2019

Sistema de avaliação: às cegas dupla (*double blind review*).

FACULDADE TECNOLOGIA TERMOMECANICA, p. 34-49

Resumo

Computação em nuvem tem sido usada como um padrão para o desenvolvimento de aplicações de Internet das Coisas (IoT) que se beneficiam de escalabilidade, disponibilidade e custos menores, mas também faz com que as aplicações de IoT dependam da conexão com a Internet e sejam suscetíveis a latências elevadas de comunicação e processamento. Computação em névoa (fog) é apresentada na literatura como a principal solução para esses problemas além de trazer possibilidades adicionais. O FIWARE é uma plataforma europeia para Internet do Futuro e suporta o desenvolvimento de aplicações de IoT oferecendo módulos chamados Generic Enablers para uso em nuvem. O Helix é uma plataforma baseada no FIWARE e em microsserviços para o desenvolvimento de aplicações para ambientes inteligentes. Neste artigo, são propostas e analisadas arquiteturas de fog computing para aplicações de IoT baseadas no FIWARE e Helix que apresentaram uma redução da latência, além da capacidade de possibilitar a comunicação horizontal e vertical através da federação de context brokers.

Palavras-chave: Internet das coisas. FIWARE. Helix. Computação em névoa. Arquitetura de névoa.

Abstract

Cloud computing has been used as a standard for the development of Internet of Things (IoT) applications that benefit from scalability, availability and lower costs but it also makes IoT applications dependent on an Internet connection and susceptible to elevated processing and communication latencies. Fog computing is presented in the literature as the main solution for these problems while bringing additional possibilities. The FIWARE is a European platform for Future Internet and supports the development of IoT applications offering convenient modules named Generic Enablers for use in the cloud. The Helix is a microservice platform for the development of smart environments applications based on FIWARE. In this paper, we propose and analyze fog computing architectures for IoT applications based on FIWARE and Helix that presented latency reduction and enabled horizontal and vertical communication through a federation of context brokers.

Keywords: Internet of Things. FIWARE. Helix. Fog computing. Fog architecture.

Introdução

Muitas implementações da Internet das Coisas (IoT) se valem do modelo de computação em nuvem, aproveitando suas vantagens, tais como escalabilidade, disponibilidade dos serviços e pagamento apenas pelos recursos utilizados. Porém, a adoção da computação em nuvem faz com que o sistema seja totalmente dependente de uma conexão com a Internet, inserindo restrições quanto à latência de comunicação e processamento. A adoção do modelo de fog computing (computação em névoa) é apontada na literatura como uma possível solução para esses desafios, além de promover uma diminuição do tráfego de dados, possibilitar uma maior variedade de aplicações e aumentar a disponibilidade do sistema (AL-FUQAHA, 2015; AAZAM, 2016; MUNIR, 2017; AHMED, 2016; DATTA, 2015 e HU et al, 2016).

A plataforma europeia FIWARE (2016), dedicada à Internet do Futuro, tem sido utilizada para a implementação de diversos projetos de Internet das Coisas, porém, em geral, as redes formadas por dispositivos de IoT são conectadas diretamente a uma nuvem central da plataforma, tendo incorporado o suporte à fog e edge computing muito recentemente. O FIWARE é uma plataforma aberta, fruto de uma parceria público-privada entre a Comissão Europeia e empresas privadas, lançada em 2011 e transformada em fundação em 2016.

Helix (CABRINI et al, 2019) é uma plataforma aberta, brasileira, baseada no FIWARE e certificada como “Powered by FIWARE” pela FIWARE Foundation. Ela é focada no desenvolvimento de aplicações para ambientes inteligentes (smart environments) e baseada em serviços containerizados, integrando e orquestrando os principais módulos da plataforma FIWARE de forma segura, além de possibilitar a operação em condições de alta resiliência. O Helix também prevê uma arquitetura em camadas que visa, através do processo de federação, a operação em ambientes de IoT: edge, fog e cloud.

Observando-se os projetos de IoT desenvolvidos nas plataformas FIWARE e Helix, bem como as vantagens apontadas na literatura para o uso de fog, é possível verificar os benefícios e a importância da proposta de uma arquitetura de fog adequada para o FIWARE e o Helix, o que será feito a partir da exposição da arquitetura para soluções de IoT na plataforma FIWARE, seguida pelas potencialidades do emprego de fog computing para Internet das Coisas relatadas na literatura. Assim sendo, serão propostas arquiteturas de fog computing para IoT na plataforma FIWARE e na plataforma Helix, seguidas das conclusões e trabalhos futuros.

A principal contribuição deste artigo é a proposta de arquiteturas de fog computing para IoT passíveis de implementação nas plataformas FIWARE e Helix.

Arquitetura IoT do FIWARE

O FIWARE é uma plataforma voltada à inovação da Internet, ou à Internet do Futuro. Um dos capítulos técnicos, ou pontos focais, do FIWARE é a habilitação de serviços de Internet das Coisas (IoT) (FIWARE, 2019), além de: hospedagem em nuvem; gerenciamento de dados e contexto; entrega de dados, serviços e aplicações; garantia de segurança; interface para redes e dispositivos e interface avançada para usuários baseada na web (FIWARE, 2019b). Ele é uma plataforma aberta e possui um catálogo de módulos conhecidos como Generic Enablers (GEs) (FIWARE, 2019c). O desenvolvedor seleciona o conjunto de GEs mais adequado para cada aplicação. Para aplicações de IoT o FIWARE utiliza o protocolo OMA NGSI (Open Mobile Alliance - Next Generation Services Interface), que fornece interfaces para gerenciar e trocar informações de contexto entre entidades de contexto, que nesse caso incluiriam os dispositivos de IoT. As informações de contexto podem ser voláteis ou persistentes e descrevem o estado de uma entidade de contexto. Elas podem ser medidas por sensores e combinadas com outras informações de contexto resultantes da interação com humanos ou com sistemas de informação. O uso dos protocolos NGSI permite abstrair a complexidade do gerenciamento de conexões com gateways e dispositivos (FIWARE, 2019).

Os principais GEs do FIWARE ligados à Internet das Coisas são o Orion Context Broker (CEF Context Broker), o IDAS Backend Device Management e o FogFlow.

Orion Context Broker ou CEF Context Broker é um broker baseado em publicação e assinatura fazendo uso dos protocolos NGSI. Frequentemente utilizado com o Cygnus, que atua como um conector para sistemas de armazenamento permanente, como um sistema de banco de dados ou como um cluster Hadoop. O Orion armazena a informação de contexto atualizada de forma que as requisições são atendidas baseadas nessa informação. Ele atua como um mediador entre produtores, como sensores e consumidores de contexto, como aplicações que se utilizam dos dados de sensoriamento. Os consumidores de contexto podem realizar assinaturas para que os dados sejam atualizados de tempos em tempos ou a partir de uma mudança de estado. Trata-se do principal broker disponível na plataforma FIWARE (FIWARE, 2019d). A nomenclatura deste GE mudou recentemente para CEF Context Broker, dentro do projeto europeu “Connecting Europe Facility”.

IDAS Backend Device Management é um GE dedicado ao gerenciamento de dispositivos, viabilizando a conexão de dispositivos ou gateways com os demais GEs, ou aplicações, do FIWARE. Ele traduz protocolos específicos de IoT como o UL2.0, JSON, OMA-LWM2M, SIGFOX e MQTT no protocolo NGSI para a troca de informações de contexto adotado como padrão no FIWARE. Cada um dos módulos responsáveis pela tradução de um protocolo específico é chamado de IoT Agent. Esse GE é dispensável se o dispositivo, ou o IoT gateway, suportar o protocolo NGSI (FIWARE, 2019c);

FogFlow é um GE feito especialmente para serviços de IoT programados sobre edge e cloud computing. Ele também é baseado no padrão NGSI e é constituído principalmente pelos GEs anteriores, IoT Broker e IoT Discovery, descartados ao final de 2018 para viabilizar o gerenciamento de contexto, arquitetados com estruturas adicionais para o gerenciamento de serviços e processamento de dados. O FogFlow também constitui um framework provendo um modelo de programação baseado no NGSI usando dataflow e declarações especiais (declarative hints) para permitir facilidade de programação, interoperabilidade e escalabilidade (CHENG, 2018; FIWARE FOGFLOW, 2019).

As aplicações de IoT na plataforma FIWARE são concebidas para que os GEs mencionados sejam executados em uma nuvem. Não havia anteriormente menção formal sobre a fog computing no FIWARE, mas um relatório publicado por Antonelli et al (2016) destacou a necessidade de se adicionar funcionalidades à borda da rede para atender requisitos como qualidade, latência e tempo de processamento. Nessa época, o FogFlow estava sendo desenvolvido (CHENG, 2018; FIWARE FOGFLOW, 2019), mas só foi incorporado como um GE em 2018.

Além dos GEs específicos de IoT, é comum que aplicações dessa área combinem GEs de análise de dados com armazenamento permanente, a exemplo do GE Cosmos, e visualização de dados e dashboards, a exemplo do GE Wirecloud (FIWARE, 2019c). Por se basear totalmente em padrões abertos, é possível integrar outros softwares aos GEs do FIWARE, ou mesmo desenvolver novos. Uma típica arquitetura de aplicação de IoT no FIWARE, baseada apenas em nuvem, é essencialmente a mesma apresentada para a plataforma Helix na versão Sandbox (CABRINI et al, 2019). Cabe ressaltar ainda que a arquitetura de IoT do FIWARE se adequa ao modelo de referência IoT-A, conforme demonstrado por Krco et al (2014) e Preventis et al (2016).

Fog Computing e suas potencialidades para IoT

Fog computing tem uma variedade de definições na literatura. É definida por Datta et al (2015) como uma extensão dos paradigmas de computação em nuvem em direção às bordas das redes, provendo os mesmos tipos de serviços, porém com as vantagens da proximidade com os consumidores, maior densidade e suporte à mobilidade. O uso de fog em IoT é indicado para reduzir a latência, melhorar a qualidade de serviço (QoS) e possibilitar a análise de dados em tempo real com atuação resultando em uma experiência de usuário superior e a criação de produtos de IoT centrados nos consumidores. A fog também é apontada como um meio de reduzir o uso dos canais de comunicação, prover maior tolerância a falhas, bem como disponibilidade e escalabilidade,

Fog, cloudlets e edge computing são apontados como sinônimos por Al-Fuqaha et al (2015). Os três termos são tomados como pontes entre dispositivos inteligentes e as grandes nuvens de computação e armazenamento, estendendo os serviços destas últimas em direção às primeiras. Além disso, são apontadas como vantagens o menor delay devido à proximidade com a borda da rede, a possibilidade de maior densidade de dispositivos, melhor desempenho para aplicações em tempo real, interoperabilidade com diferentes provedores de nuvem, possibilidade de agregação de dados diminuindo o tráfego para o datacenter em nuvem e suporte à mobilidade, podendo-se mencionar inclusive que as operadoras de telefonia móvel são apontadas como o provedor natural de serviços de fog. Como contrapontos são destacados alguns aspectos, entre eles, os de que em uma fog a confiabilidade e a segurança dos dados analisados nas bordas da rede são problemas em aberto e os recursos de computação, armazenamento e rede são limitados, muito embora possam ser implementados em escala e com menor custo. Smartphones e home gateways são apontados como possibilidades para a implementação de fogs.

Em Aazam e Huh (2016) são mencionadas algumas justificativas para o emprego de fog computing em aplicações de IoT, tais como: dificuldades para a realização eficiente de tarefas com restrições de energia e largura de banda, a necessidade de melhor gerir os recursos na nuvem com a presença de dados multimídia, a necessidade de resposta e processamento rápidos para IoT e a questão do pré-processamento e privacidade dos dados. Os autores apontam a fog como uma nuvem

localizada, de baixa latência e mais contextualizada, viabilizando um modelo de federação de IoTs e a criação de serviços "mais ricos", sendo também uma solução para diminuir a carga de dispositivos limitados. O modelo de fog previsto pelos autores é o de microdatacenters.

Baixa latência e economia de energia também são apontados por Huang et al (2016) juntamente com uma extensão dos serviços de nuvem para dispositivos com restrições de recursos, capacidade para filtrar os dados, incrementos na segurança e qualidade de serviço. Um ponto fraco indicado pelos autores é a questão de lidar com diferentes tipos de dados que impõem diferentes níveis de qualidade de serviço.

O uso de fog computing em aplicações de IoT que requerem processamento em tempo real é trazido como solução por Rauniyar et al (2016), justamente por minimizar delay, jitter e o volume de dados de uma comunicação direta com a nuvem. Também é prevista uma espécie de CEP (Complex Event Processing), na qual os dados processados e selecionados são enviados à nuvem para análise histórica e armazenamento de longo prazo. Os autores pontuam que qualquer dispositivo com conectividade de rede e capacidade de computação e armazenamento pode ser usado para a constituição de uma fog, incluindo dispositivos inteligentes, servidores embarcados e equipamentos de rede.

Munir et al (2017) analisa mais detalhadamente a distinção entre fog e cloud computing, bem como entre fog e edge computing, com a ressalva de que boa parte da literatura trata ambas como sinônimas. Quanto aos dispositivos empregados, são apontados servidores, equipamentos de rede, como roteadores, e de telecomunicações, como estações rádio-base. Fog computing é apresentada como tendo o objetivo de processar os dados próximo à sua fonte, isto é, as extremidades da rede, diminuindo fortemente o volume de dados trafegados entre os dispositivos e a nuvem e viabilizando processamento mais complexo como análise de dados junto à fonte. Análise similar pode ser encontrada no trabalho de Hu et al (2017), enquanto Chiang e Zhang (2016) destacam o uso de fog em aplicações que precisam assegurar serviços ininterruptos mesmo em condições de conectividade intermitente com a nuvem, pois uma implementação de fog confiável continuará a funcionar conforme projetado mesmo sob condições adversas de operação.

Essa distinção entre fog e edge é corroborada pela iniciativa OpenFog Consortium (2018), estabelecida em 2015 pelos membros fundadores ARM, Cisco, Dell, Intel, Microsoft e Universidade de Princeton, com o apoio de outras empresas e instituições, e unidos ao Industrial Internet Consortium (2019) Para o consórcio, edge computing é apresentada como parte da fog computing, frisando que uma arquitetura de edge computing pode ser de certa forma autocontida, com todo o processamento ocorrendo na borda da rede em nós independentes, enquanto em uma fog há um processamento hierárquico e uma arquitetura mais horizontal, onde diferentes nós de fog constituem uma rede com capacidade de comunicação direta entre os nós (peer-to-peer) sem necessitar que os dados sejam enviados à nuvem para isso. Uma fog trabalha de forma mais sinérgica do que independente com a nuvem, sendo esta última uma atribuição da edge computing. Essa definição foi ratificada na norma IEEE 1934-2018 - IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing. A definição adotada no padrão é a de que fog computing é uma arquitetura horizontal em nível de sistema que distribui computação, armazenamento, controle e funções de rede para as proximidades dos usuários ao longo de um continuum da nuvem para as "coisas" (dispositivos) (OPENFOG, 2017). Esse continuum admite múltiplos níveis hierárquicos com comunicação horizontal e vertical entre os diversos nós de fog.

As arquiteturas de fog aqui propostas visam cumprir com as características relatadas e obter as vantagens apresentadas na literatura para o uso de fog computing. Os GEs disponíveis na plataforma

FIWARE permitem a criação de aplicações que se adequam tanto a edge como a fog dentro das diferenças estabelecidas em (OPENFOG, 2017; MUNIR et al, 2017 e HU et al, 2016).

Arquitetura de Fog Computing para IoT na plataforma FIWARE

Ao analisar-se a literatura apresentada sobre *fog computing*, nota-se que ela é caracterizada como um nível intermediário entre as redes de IoT e a nuvem. Para desenvolver uma arquitetura de *fog* na plataforma FIWARE, ou mesmo *edge*, faz-se necessário escolher os GEs apropriados para funcionarem nesse contexto. Há basicamente duas possibilidades: a utilização do GE FogFlow e o emprego de uma federação de GEs Orion *Context Broker*.

No nível da IoT, os dispositivos que suportam o protocolo NGSI podem se comunicar diretamente com os GEs mencionados. Para dispositivos que necessitem de tradução do protocolo de comunicação a ser usado, ou seja, dispositivos de baixa capacidade computacional, faz-se necessário o uso do GE IDAS para a comunicação entre os dispositivos, ou IoT *gateway*, e a *fog*, ou *cloud*, através do(s) IoT Agent(s) correspondente(s). Os IoT Agents permitem a conversão dos protocolos de comunicação empregados nos dispositivos das redes IoT específicas e podem ser implementados tanto na *fog* como no nível da IoT, em um *gateway* por exemplo. Em redes integradas por dispositivos de maior capacidade computacional é possível a comunicação direta desses protocolos com a *fog*.

O nível da *fog* pode ser implementado utilizando-se o GE FogFlow, conforme abordado em Cheng (2018) e FIWARE FogFlow (2019), muito embora o *framework* por eles proposto seja mais adequado à *edge computing*. Dessa forma, o modelo mais adequado de implementação para *fog computing* na plataforma FIWARE torna-se o de uma federação de *context brokers*.

A federação é basicamente um encadeamento hierárquico de GEs Orion *Context Broker* e pode se dar de duas formas conhecidas como *push* e *pull* (FIWARE, 2019e). Na federação do tipo *push*, as notificações de contexto enviadas por uma instância de Orion são processadas e então enviadas para a próxima instância do GE Orion. Já na federação do tipo *pull*, as notificações de contexto são apenas repassadas para a próxima instância do Orion, sem que a primeira instância precise armazenar nenhum dado. O processo de federação é feito através de assinaturas utilizando-se os parâmetros adequados. Uma federação de GEs Orion pode ser criada "horizontalmente" no nível da nuvem ou da *fog*, ou ainda "verticalmente", interligando um ou mais nós de *fog*, cada qual executando sua instância do Orion *Context Broker*, uns com os outros e com a instância central na nuvem. Esse modelo de federação pode ser visto na Figura 1.

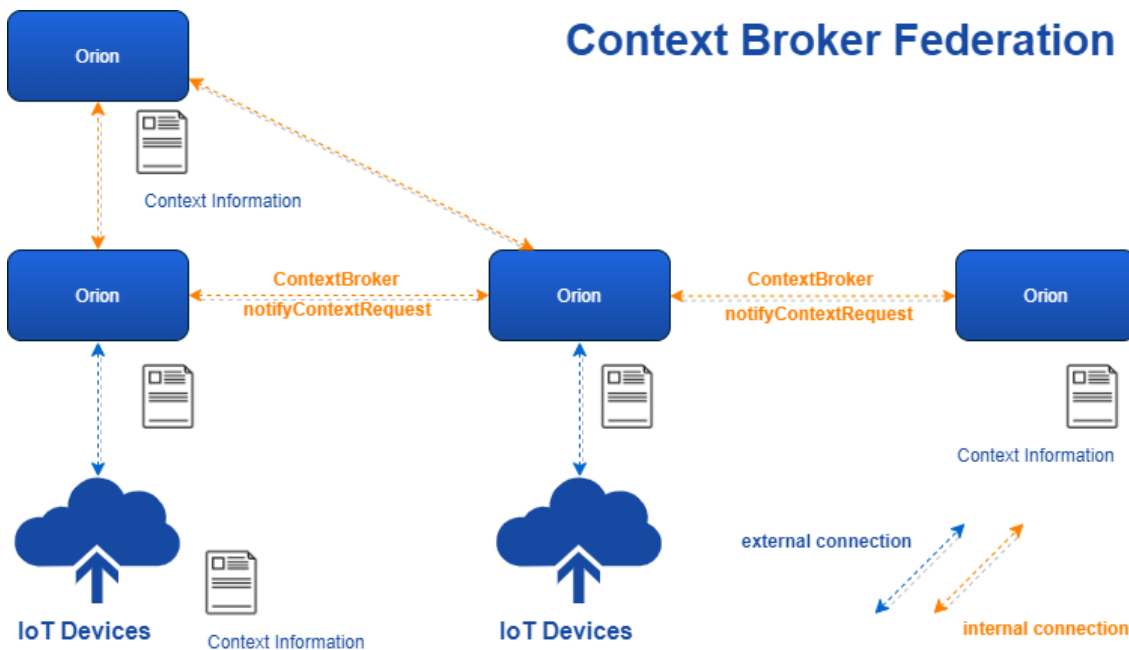


Figura 1: Arquitetura de fog computing proposta para o FIWARE utilizando a federação de Context Brokers.
 Fonte: Elaboração dos autores (2019)

A implementação de diversos nós de *fog* nesse modelo permite a comunicação com a nuvem e através dela, mas eles também podem se comunicar diretamente entre si graças à padronização do protocolo de comunicação baseado na troca de informações de contexto via API (*Application Programming Interface*) utilizando o protocolo NGSI, estabelecendo a comunicação vertical e horizontal entre os diversos nós, permitindo uma *fog* com diversas camadas.

A estrutura de nuvem centralizada abriga como elemento principal um Orion *Context Broker* que atua recebendo e distribuindo os dados enviados da *fog* para os demais componentes da aplicação. Ele pode ser interligado a um banco de dados para armazenamento permanente através do conector Cygnus, frequentemente executado na mesma instância do GE Orion, além de um sistema para visualização de dados como um *dashboard*, por exemplo, constituindo uma aplicação mínima, conforme apresentado na seção II. Geralmente são adicionados outros GEs para a composição da aplicação final como um sistema de Hadoop para *Big Data e Analytics* através do GE Cosmos, ou do GE Knowage para administração de negócios (BI). O GE Kurento promove o processamento de *streaming* de mídia, enquanto o GE Perseo atua como um CEP permitindo realizar uma série de ações a partir de um sistema de regras. Além dos GEs mencionados, podem ser integradas ferramentas externas. Os GEs estão detalhados em FIWARE (2019c).

Quanto à implementação física (*hardware*) dos nós de *fog*, eles se adequam a partir do modelo de “*smart*” IoT gateways até o de *microdatacenters*, mas restritos à arquitetura x86. Os GEs do FIWARE podem ser instalados diretamente no sistema operacional (*bare metal*), compondo um sistema único integrado, ou mesmo com o uso de múltiplas máquinas virtuais ou contêineres Docker localmente ou espalhados em um *datacenter*. É possível escolher a solução mais adequada às demandas de desempenho computacional, comunicação e energia requeridas pela aplicação.

O caminho para se constituir uma federação de GEs Orion *Context Broker* foi adotado na plataforma Helix que, graças à sua arquitetura modular, também pode incorporar o GE FogFlow para facilitar a programação de aplicações baseadas em *fog computing*.

Plataforma Helix e sua arquitetura de Fog Computing

A plataforma Helix (CABRINI *et al*, 2019) integra os principais GEs do FIWARE para a implementação de soluções para ambientes inteligentes com desempenho e segurança otimizados. O Helix possui as versões SandBox e Multi-Layred.

O Helix Sandbox é uma plataforma aberta para prototipação rápida de soluções para ambientes inteligentes que permite o uso dos principais GEs previstos na arquitetura FIWARE de forma segura e integrada. Foi desenvolvido visando fomentar iniciativas de pesquisa e empreendedorismo através do desenvolvimento de aplicações de Internet do Futuro sobre uma plataforma de baixo custo e com características sólidas que possibilitem a implementação e a integração com serviços de terceiros, tendo seu foco em *startups* que precisam validar e apresentar suas soluções a investidores em um curto período de tempo através da elaboração de MVPs (*Minimum Viable Product*) e para empresas e universidades que trabalham no desenvolvimento do PoCs (*Proof of Concepts*) para validar novos produtos e pesquisas. O Helix SandBox é baseado em serviços containerizados na plataforma Docker, de forma a orquestrar e integrar os principais GEs previstos pela FIWARE *Foundation* localmente, na *fog* ou na nuvem. Em setembro de 2018, a plataforma foi avaliada e certificada pela FIWARE Foundation como uma plataforma “*Powered by FIWARE*”.

O Helix SandBox integra de maneira segura os GEs Orion *Context Broker*, Cygnus e IoT Agent, além de utilizar uma base de dados única baseada no MongoDB, que é utilizado pelo Orion *Context Broker* para o armazenamento das informações de contexto e registros dos dados históricos coletados pela plataforma. Também possui o módulo Helix Compose que realiza a orquestração dos GEs e módulos adicionais que compõem a arquitetura. A estrutura pode ser vista na Figura 2, onde é possível notar a integração de dispositivos IoT com maior capacidade computacional diretamente ao *broker*, e a integração de dispositivos de menor capacidade através de IoT Agents para comunicação com os protocolos MQTT e CoAP. Também estão indicadas as portas-padrão utilizadas pelos GEs para comunicação através das conexões externas.

Helix Sandbox Architecture

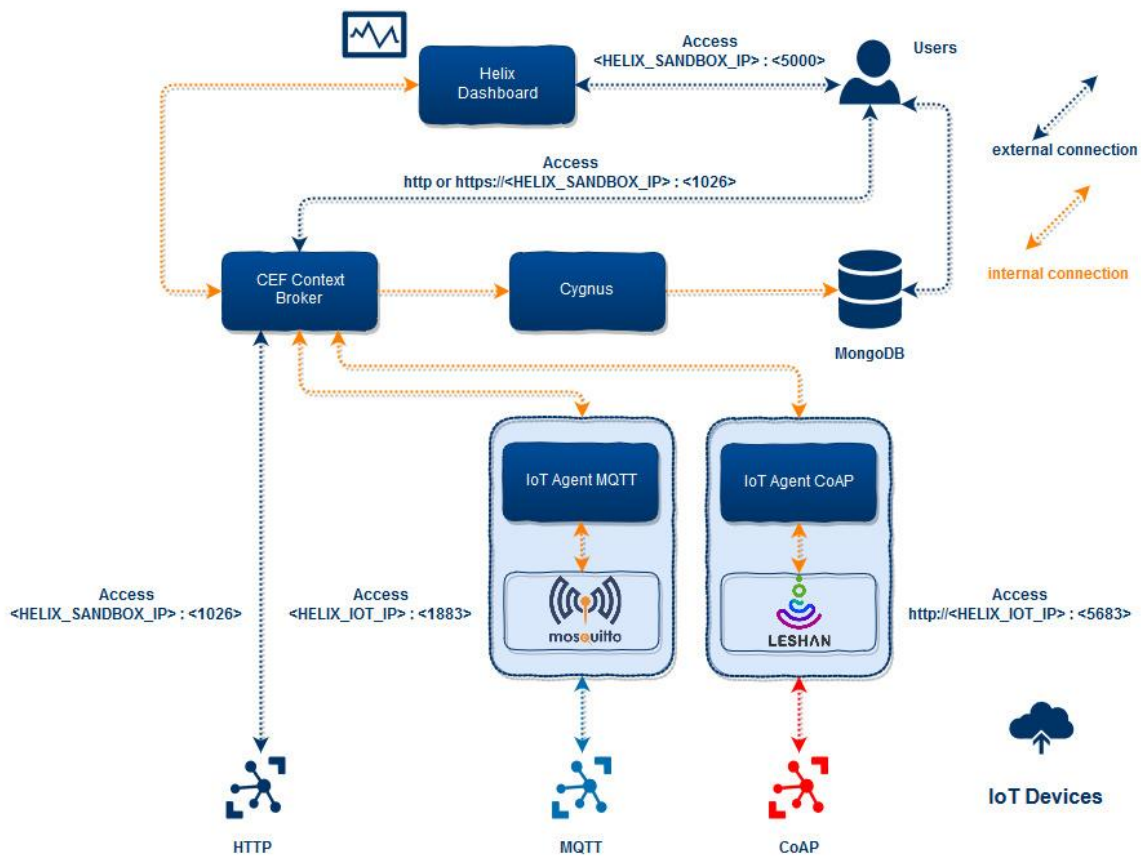


Figura 2: Arquitetura do Helix Sandbox (correspondente à arquitetura básica de aplicação de IoT em cloud no FIWARE).
Fonte: Elaboração dos autores (2019)

A interface web de gerenciamento conta com recursos que possibilitam a integração e a configuração simplificada do Orion, do IoT Agent e dos dispositivos LWM2M seguindo as especificações do padrão da Open Mobile Alliance (2019) OMA LightweightM2M. A plataforma Helix conta com o módulo Helix IoT, que possibilita a conexão com dispositivos não NGSI na abordagem Helix Cloud, Fog e Edge através do uso de arquitetura x86 e ARM. Como exemplo, é possível citar o Helix IoT baseado no MQTT que possibilita a integração com o broker Mosquitto utilizando a abordagem Publisher/Subscriber (Helix IoT MQTT, 2019).

Os GEs presentes no Helix foram selecionados de acordo com critérios de maturidade e funcionalidade oferecidos pela FIWARE Foundation com o objetivo de garantir uma camada de back-end completa para ambientes inteligentes possibilitando a integração de sensores e atuadores, presentes no ambiente, a dashboards que possibilitam a visualização e análise dos dados.

A versão Helix Nebula prevê uma arquitetura em camadas que visa, através do processo de federação, a operação em ambientes de IoT, edge, fog e nuvem para aplicações críticas que exigem alta resiliência e baixa latência. Em acordo com OpenFog (2017), Munir et al (2017) e Hu et al (2016), assumimos edge como a infraestrutura mais próxima aos dispositivos de IoT enquanto fog pode ser implementada em algum lugar entre a nuvem e a borda da rede e suportando comunicação horizontal, isto é, entre distintos nós de fog. Na verdade, ao se trabalhar com o conceito de fog, a edge passa a ser um subconjunto dela (OpenFog, 2017).

Quanto aos requisitos de hardware, a Helix Edge pode ser implementada tanto em um pequeno single board computer como, por exemplo, a Raspberry Pi, comunicando-se com um nó de fog, ou cloud, passando por IoT gateways, servidores ou mesmo um microdatacenter. Já a implementação do Helix nos níveis de Fog e Cloud requerem arquitetura x86 de 64 bits para a execução do Orion Context Broker. É possível escolher a solução mais adequada às demandas de desempenho computacional, comunicação e energia, bem como aos requisitos temporais impostos pela aplicação.

A arquitetura multilayer da plataforma Helix pode ser vista na Figura 3. A nuvem abriga o Helix implementado em alta disponibilidade através da abordagem Swarm ou Kubernetes que inclui o Orion Context Broker e o banco de dados de forma a garantir a capacidade de se adaptar a grandes volumes de informação através de uma estratégia de scale up e down.

O nível da fog é implementado através de uma federação de Helix, aproveitando os recursos de federação do Orion Context Broker, automatizados através do Helix compose previstos na versão Nebula. Os diversos nós de fog podem se comunicar com a nuvem e através dela, mas também podem comunicar-se diretamente entre si. Esse modelo de implementação de fog permite a comunicação com outros GEs do FIWARE, ou módulos externos, como um sistema Hadoop para Big Data e Analytics para a composição de aplicações distribuídas e complexas. Graças à padronização do protocolo de comunicação, baseado na troca de informações de contexto via API utilizando-se do protocolo NGSI, é possível estabelecer a comunicação horizontal.

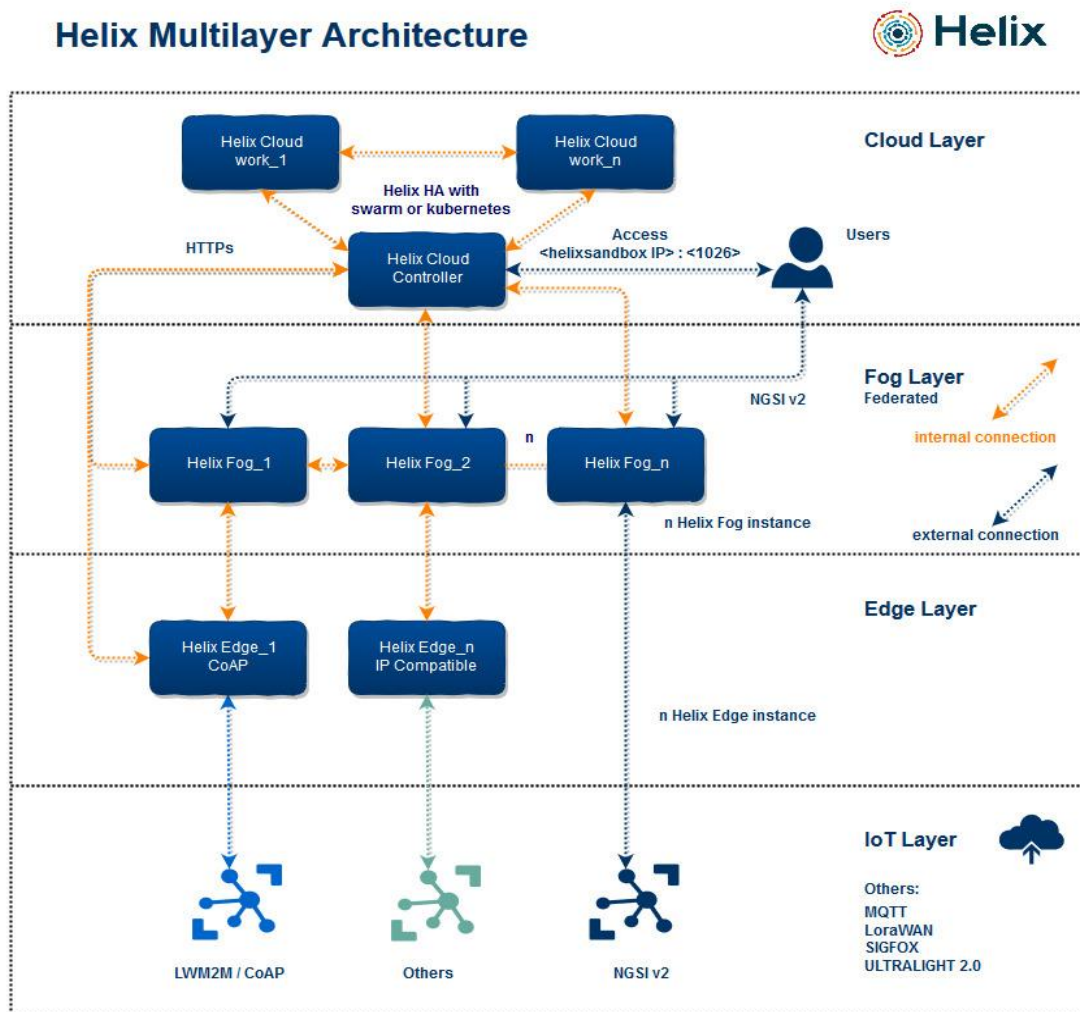


Figura 3: Helix Multilayer Architecture
Fonte: Cabrini et al. (2019)

Na camada Edge, o Helix implementa IoT *Agents*, que permitem a conversão dos protocolos de comunicação empregados nos dispositivos das redes IoT específicas. Nas redes IoT compostas por dispositivos de maior capacidade de processamento, eles podem interagir diretamente com a *fog* ou a *cloud*.

Tanto o Helix SandBox como o Nebula estão em conformidade com o CEF (*Connecting Europe Facility*) devido à sua compatibilidade com o NGSI-LD definido pelo ETSI (*European Network of Telecommunications Standards*), que tem como objetivo a interconexão de sistemas de Internet do Futuro no contexto da União Europeia.

Análise das arquiteturas propostas

Do ponto de vista arquitetural, os modelos propostos para a implementação de fog computing em aplicações de IoT de tempo real na plataforma FIWARE e na plataforma Helix contemplam os principais benefícios e características relatados na literatura existente e apresentados na seção “Fog Computing e suas Potencialidades para IoT”, destacando-se:

- Redução da latência no tráfego de dados na rede e eventual redução do volume de dados trafegado;
- Racionalização dos recursos de nuvem;
- Padronização da comunicação entre a fog e a nuvem com o uso do protocolo NGSI;
- Possibilidade de comunicação horizontal entre os nós de fog;
- Suporte para a maior densidade de dispositivos no nível da IoT;
- Suporte para a maior heterogeneidade de componentes de IoT necessários para aplicações complexas;
- Possibilidade de implementação de fog em dispositivos de baixo custo, desde que adequados à aplicação;
- Aumento da disponibilidade e da resiliência da aplicação no nível da IoT.

O aumento da disponibilidade e da resiliência da aplicação se dá através de uma maior autonomia em relação à nuvem central, garantindo seu funcionamento, mesmo que ocorra a perda de comunicação com a nuvem, uma vez que a fog funciona mais próximo ou mesmo localmente em relação ao ambiente da rede IoT, e também devido à possibilidade de comunicação entre os nós de fog.

A redução da latência foi avaliada por meio de testes utilizando-se a ferramenta Apache Bench a partir de um dispositivo conectado a uma rede Ethernet 1Gbps. Foram feitas 10 baterias de teste com 10 requisições em cada uma nos níveis de edge, fog e cloud. A edge foi implementada na mesma rede local, a fog em um servidor na Amazon AWS na mesma região metropolitana (São Paulo - Brasil) e a nuvem no datacenter do FIWARE na Espanha. A diferença nos Round Trip Times (RTT) variou de 1,0 ms na edge, passando para 8,4 ms na fog, até atingir 608,1 ms na nuvem, conforme pode ser visto na Figura 4.

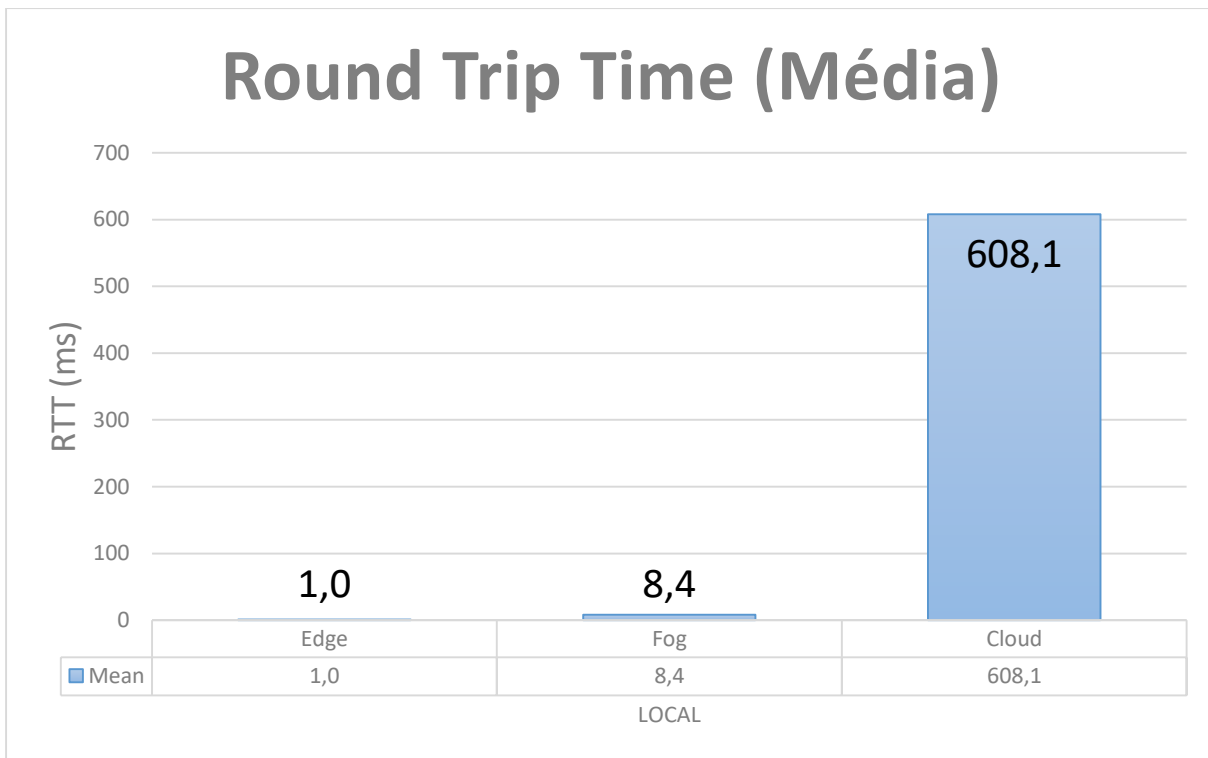


Figura 4: Médias dos Round Trip Time (RTT) medidos localmente na fog e na nuvem.
 Fonte: Elaboração dos autores (2019)

Uma fragilidade do emprego de *fog computing* na plataforma FIWARE é o potencial aumento da complexidade e, eventualmente, do custo de implementação da solução de IoT, fato que deve ser avaliado em especial para soluções mais simples e homogêneas ou de menor porte. O desenvolvimento da plataforma Helix visou mitigar este problema.

Uma dificuldade oferecida é a infraestrutura para a implementação da *fog* que requer, de acordo com a aplicação, de um IoT *gateway* com maior capacidade computacional a um *microdatacenter*. Essas estruturas precisam ser projetadas, implantadas e operadas tanto física como logicamente.

Considerações finais

Este trabalho abordou detalhes das plataformas FIWARE e Helix com foco em soluções para ambientes inteligentes. A arquitetura básica de uma solução de IoT foi apresentada para ambas as plataformas. Em virtude do tempo, da dificuldade de integração dos diferentes GEs do FIWARE e dos recursos computacionais necessários, o Helix Sandbox apresenta-se como uma solução mais conveniente para testes e para o desenvolvimento de PoCs e MVPs devido à sua abordagem lightweight.

Foram relatadas também as vantagens do uso de fog computing como um nível intermediário entre a nuvem e os dispositivos de IoT, além da diferenciação entre os conceitos de fog e edge computing. Também foram apresentadas as possibilidades de implementação de fog e edge computing, através dos recursos de federação, previstos no Orion Context Broker, elemento central da plataforma FIWARE, com destaque para o modelo de federação de context brokers, que permite uma implementação mais adequada de fog, viabilizando a comunicação horizontal entre elas através da abordagem adotada na versão Nebula da Plataforma Helix.

Finalmente foi apresentada a arquitetura de multicamadas da plataforma Helix, que leva o poder de processamento e a capacidade de gerenciamento das informações de contexto às camadas de fog, além de oferecer recursos que potencializam a criação de soluções para ambientes inteligentes que integram recursos presentes na nuvem: fog, edge e IoT. Os potenciais benefícios e dificuldades das arquiteturas propostas foram devidamente analisados.

Na versão Helix Nebula é possível observar uma arquitetura multicamadas que evidencia o uso dos componentes da plataforma Helix operando em modo de alta resiliência nas camadas de edge, fog e nuvem.

A arquitetura multicamadas proposta para a plataforma Helix está em fase de testes para cenários mais complexos, com requisitos de ultrabaixa latência e alta concentração de dispositivos de IoT para suportar aplicações de IoT para ambientes inteligentes críticos, especialmente nos contextos de cidades inteligentes (smart cities), fazendas inteligentes (smart farms), indústria 4.0, grids de energia (smart grids), veículos autônomos e Internet Tátil.

A tese aqui apresentada demonstrou ser uma proposta promissora, e através da avaliação plena dos benefícios e dificuldades da implementação, comprovou que pode oferecer vantagens no futuro para a integração das camadas de edge e fog computing no contexto das aplicações de IoT para ambientes inteligentes. As arquiteturas propostas apresentam adesão à arquitetura de referência do OpenFog Consortium (2017) na norma IEEE 1934-2018 - IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing. Com isso, espera-se oferecer uma diretriz detalhada e confiável para implementar soluções com arquitetura de fog utilizando as plataformas FIWARE e Helix, tendo por base os requisitos de cada aplicação.

Referências

AAZAM, Mohammad; HUH, Eui Nam. *Fog Computing: the Cloud-IoT/IoE Middleware Paradigm*. *IEEE Potentials*, [s. l.], v. 35, n. 3, p. 40–44, 2016.

AHMED, Arif; AHMED, Ejaz. A Survey on Mobile Edge Computing. In: 2016 10TH INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS AND CONTROL (ISCO) 2016, *Anais: IEEE*, 2016. Disponível em: <http://ieeexplore.ieee.org/document/7727082/>.

AL-FUQAHA, Ala et al. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, [s. l.], v. 17, n. 4, p. 2347–2376, 2015. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7123563>

ANTONELLI, Fabio et al. FIWARE Mundus: Map of technology and business challenges for the Future Internet. [s. l.], n. 632912, p. 22, 2016. Disponível em: https://www.fiware.org/wp-content/uploads/tabs-img/tab-mundus-3/FutureInternetChallenges_web.pdf.

CABRINI, F. H. et al. Helix SandBox : An Open Platform to Fast Prototype Smart Environments Applications. *2019 IEEE 1st Sustainable Cities Latin America Conference (SCLA)*, [s. l.], p. 1–6, 2019.

CHENG, Bin et al. FogFlow: Easy Programming of IoT Services Over Cloud and Edges for Smart Cities. *IEEE Internet of Things Journal*, [s. l.], v. 5, n. 2, p. 696–707, 2018.

CHIANG, Mung; ZHANG, Tao. Fog and IoT: An Overview of Research Opportunities. *IEEE Internet of Things Journal*, [s. l.], v. 4662, n. c, p. 1–1, 2016. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7498684>.

DATTA, Soumya Kanti; BONNET, Christian; HAERRI, Jerome. *Fog Computing architecture to enable consumer centric Internet of Things services*. *Proceedings of the International Symposium on Consumer Electronics, ISCE*, [s. l.], v. 2015- August, p. 6–7, 2015.

FIWARE. *Future Internet Core Platform*. Disponível em: <http://www.fiware.org/>. Acesso em: 2016.

_____. *Internet of Things (IoT) Services Enablement Architecture*. Disponível em: [https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Internet_of_Things_\(IoT\)_Services_Enablement_Architecture](https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Internet_of_Things_(IoT)_Services_Enablement_Architecture). Acesso em: 06.2019.

_____. *FIWARE Architecture*. Disponível em: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_Architecture. Acesso em: 06.2019.

_____. *FIWARE Catalogue*. Disponível em: <https://www.fiware.org/developers/catalogue/>. Acesso em: 06.2019.

_____. *Orion Context Broker*. Disponível em: <https://fiware-orion.readthedocs.io/en/master/>. Acesso em: 06.2019.

_____. *Context broker federation*. Disponível em: <http://fiware-orion.readthedocs.io/en/master/user/federation/>. Acesso em: 06.2019.

FIWARE *FogFlow*. FIWARE *FogFlow*. Disponível em: <https://fogflow.readthedocs.io/en/latest/>. Acesso em: 06.2019.

HELIX IoT MQTT. Disponível em: <https://github.com/fabiocabrini/helix-iot-mqtt>. Acesso em: 06.2019.

HU, Pengfei et al. Survey on fog computing : architecture , key technologies , applications and open issues. *Journal of Network and Computer Applications*, [s. l.], v. 98, n. April, p. 27–42, 2017. Disponível em: <http://dx.doi.org/10.1016/j.jnca.2017.09.002>.

HUANG, Lina et al. Software-defined QoS provisioning for fog computing advanced wireless sensor networks. *2016 IEEE Sensors*, [s. l.], p. 1–3, 2016. Disponível em: <http://ieeexplore.ieee.org/document/7808814/>.

Industrial Internet Consortium. Disponível em: <https://www.iiconsortium.org/>. Acesso em: 2019.

KRCO, Srdjan; POKRIC, Boris; CARREZ, Francois. Designing IoT architecture(s): A European perspective. *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, [s. l.], p. 79–84, 2014.

MUNIR, Arslan; KANSAKAR, Prasanna; KHAN, Samee U. IFCloud: Integrated *Fog* Cloud IoT: A novel architectural paradigm for the future Internet of Things. *IEEE Consumer Electronics Magazine*, [s. l.], 2017.

Open Mobile Alliance (OMA). OMA LightWeight M2M (LWM2M) Object and Resource Registry. Disponível em: <http://www.openmobilealliance.org/wp/OMNA/LwM2M/LwM2MRegistry.html>. Acesso em: 06.2019.

OpenFog Consortium. Disponível em: <https://www.openfogconsortium.org/>. Acesso em: 2018.

OpenFog Consortium Architecture Work Group. OpenFog Reference Architecture for Fog Computing. no. February, pp. 1–162, 2017. Disponível em: www.OpenFogConsortium.org. Acesso em: 11 mar. 2019.

PREVENTIS, Alexandros et al. IoT-A and FIWARE: Bridging the barriers between the cloud and IoT systems design and implementation. *CLOSER 2016 - Proceedings of the 6th International Conference on Cloud Computing and Services Science*, [s. l.], v. 2, n. Closer, p. 146–153, 2016.

RAUNIYAR, Ashish et al. Crowdsourcing-based disaster management using fog computing in internet of things paradigm. In: *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2016. p. 490-494.