

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/309312669>

Computação em Névoa: Conceitos, Aplicações e Desafios

Chapter · May 2016

CITATIONS

0

READS

2,975

3 authors:



Antonio Augusto T R Coutinho

Universidade Estadual de Feira de Santana

8 PUBLICATIONS 6 CITATIONS

[SEE PROFILE](#)



Elisângela Oliveira Carneiro

Universidade Estadual de Feira de Santana

5 PUBLICATIONS 7 CITATIONS

[SEE PROFILE](#)



Fabíola Greve

Universidade Federal da Bahia

69 PUBLICATIONS 320 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Blockchain: Theory, Technology and Applications [View project](#)



WebManager [View project](#)

Capítulo

6

Computação em Névoa: Conceitos, Aplicações e Desafios

Antônio Augusto Teixeira Ribeiro Coutinho¹, Elisângela Oliveira Carneiro¹
e Fabíola Gonçalves Pereira Greve²

¹Departamento de Tecnologia (DTEC), Universidade Estadual de Feira de Santana (UEFS)

²Departamento de Ciência da Computação (DCC), Universidade Federal da Bahia (UFBA)

Abstract

Currently, cloud-based solutions have become the predominant approach for the Internet of Things (IoT). However, to meet requirements such as mobility support, location awareness and low latency, current IoT proposals are fomenting a major shift from a centralized model towards a decentralized model. Seen in these terms, Fog Computing is a paradigm that extends Cloud Computing services to the edge of the network on a widely distributed level. This chapter introduces the concepts related to this area highlighting the differences between IoT, Cloud and Fog Computing. Technological aspects about the integration of these paradigms are addressed by examining existing solutions. Future research is discussed focussing on challenges involved in designing fog computing systems.

Resumo

Atualmente, soluções baseadas em Nuvem têm sido uma abordagem predominante para a Internet das Coisas (Internet of Things, IoT). Porém, visando atender requisitos como mobilidade, localidade e baixa latência as propostas correntes sobre IoT estão fomentando uma importante mudança de um modelo centralizado para um modelo descentralizado. Nesse sentido, a Computação em Névoa (Fog Computing) é um paradigma que estende os serviços de Nuvem para a borda da rede numa escala amplamente distribuída. Este capítulo introduz os conceitos relacionados com esta área destacando as diferenças entre IoT, Computação em Nuvem e Névoa. Aspectos tecnológicos sobre a integração destes paradigmas são abordados pelo exame de soluções existentes. Pesquisas futuras são discutidas pela análise de desafios envolvidos no projeto de sistemas em Névoa.

6.1. Introdução

Nos próximos anos, é esperado o surgimento de bilhões de novos objetos com capacidade de coletar, trocar informações e interagir com o ambiente de maneira inteligente. Contudo, a integração desses elementos para beneficiar simultaneamente diferentes setores da sociedade demanda grandes desafios, como parte do que está sendo chamada a Internet das Coisas (*Internet of Things, IoT*) [Atzori et al. 2010] [Gubbi et al. 2013].

Os ambientes IoT são caracterizados por diferentes tipos de conexão entre dispositivos heterogêneos, dispostos de forma local ou amplamente distribuídos, com capacidades de comunicação, processamento e armazenamento limitadas [Sehgal et al. 2012]. Esses componentes físicos embarcados com sensores e atuadores podem ser interconectados com outros recursos físicos ou virtuais [Nitti et al. 2015] para controle, processamento e análise de dados. Sua implementação envolve diferentes questões como confiabilidade, performance, segurança e privacidade [Atzori et al. 2010] [Gubbi et al. 2013].

Propostas sobre a Internet das Coisas vêm agregando diferentes tecnologias para possibilitar a composição de cenários de computação ubíqua e pervasiva baseados em elementos autoconfiguráveis e inteligentes sobre uma infraestrutura de rede dinâmica e global [Botta et al. 2016]. Neste contexto, a Computação em Nuvem (Cloud Computing) [Mell and Grance 2010] se distingue como uma tecnologia madura e confiável, oferecendo capacidades virtualmente ilimitadas de processamento e armazenamento para suplantar as limitações dos dispositivos IoT envolvidos [Moura and Hutchison 2016].

Diferentes soluções centradas em Nuvem para Internet das Coisas são citadas como Nuvem das Coisas (*Cloud of Things*) em [Aazam et al. 2014] e Nuvem IoT (*Cloud IoT*) em [Botta et al. 2016]. Essas plataformas agregam vantagens da Computação em Nuvem [Khalid et al. 2016] para suporte ao crescente volume de dados produzidos pelos dispositivos IoT [ABI Research 2015]. Elas também oferecem o compartilhamento dinâmico de recursos entre aplicações verticais distintas e permitem o gerenciamento de sua infraestrutura em Nuvem IoT através da Internet [Moura and Hutchison 2016].

Porém, a transição para Internet das Coisas não pode ser considerada uma simples aplicação da Computação em Nuvem. Seu estudo envolve um conjunto de novas questões e desafios, requerendo grandes esforços de investigação [Aazam et al. 2014] [Botta et al. 2016] [Díaz et al. 2016]. É necessário otimizar e implantar o conceito de Nuvem para prover conteúdo aos usuários através de uma plataforma IoT densa e geograficamente distribuída. As soluções em Nuvem para Internet das Coisas terão que suportar o modelo *Everything-as-a-Service* (XaaS) [Duan et al. 2015], onde o usuário pode acessar os dados a partir de qualquer dispositivo, em qualquer lugar, a qualquer momento.

Recentemente, a Computação em Névoa (*Fog Computing*) [Bonomi et al. 2012] vem atraindo interesse pelo seu potencial de satisfazer requisitos que não são atendidos por um modelo centralizado em Nuvem [Khalid et al. 2016]. Este paradigma estende os recursos computacionais disponíveis na Nuvem para a borda da rede visando apoio às soluções em IoT. Dessa forma, possibilita a execução de aplicativos em bilhões de objetos conectados para fornecer dados, processamento, armazenamento e serviços aos usuários.

Sua arquitetura introduz o suporte à análise de dados em tempo real, distribuindo o processamento analítico através dos recursos na Névoa [Bonomi et al. 2014]. Esta

abordagem reduz significativamente a quantidade de informações transferidas para a infraestrutura em Nuvem por capturar e processar os dados necessários diretamente em cada dispositivo na borda da rede. Além disso, permite que os dados transmitidos sejam mais significativos e acionáveis pela filtragem de informações em diferentes níveis de sua organização hierárquica [Bonomi et al. 2012] [Bonomi et al. 2014].

Esse movimento seletivo dos recursos computacionais, controle e tomada de decisões para as extremidades da rede é uma área emergente da engenharia de sistemas e ciência da computação. Seu estudo está no centro de vários domínios de aplicação da Internet das Coisas onde pesquisas vem buscando identificar requisitos, experimentar algoritmos e avaliar arquiteturas para esclarecer problemas relativos à sua implementação.

No entanto, prover conectividade e prestação de serviços em larga escala no cenário da Internet das Coisas não é uma tarefa simples [Yi et al. 2015b]. Devido a sua localização e organização, as redes de nevoeiro possuem natureza heterogênea e uma diversidade de conexões envolvidas [Luan et al. 2016]. Diferentes problemas de conectividade, confiabilidade, capacidade e atraso podem influenciar na disponibilidade e qualidade dos serviços oferecidos [Madsen et al. 2013] [Yi et al. 2015b].

A segurança também é um fator chave, uma vez que um número crescente de elementos passam a integrar e atuar diretamente na rede. Isso aumenta a probabilidade de falhas não identificadas, infecções nos sistemas, vulnerabilidades nos canais e riscos de invasão. Neste aspecto, a Computação em Névoa enfrenta novos desafios de segurança e privacidade que vão além daqueles herdados da Computação em Nuvem [Yi et al. 2015c].

Devido a indefinição de padrões para integração das tecnologias relacionadas com a Nuvem IoT, existe atualmente a falta de uma interface unificada e de um modelo de programação que ajude tanto a implementação de novas soluções quanto a portabilidade de aplicativos para a plataforma em Névoa [Yi et al. 2015b]. Embora diferentes iniciativas de padronização tenham surgido nos últimos anos [ETSI ISG MEC 2015] [OpenFog 2016], ainda é preciso um grande esforço para atender às necessidades de seus desenvolvedores.

O objetivo geral deste capítulo é abordar o estado da arte da Computação em Névoa, oferecendo uma visão dos fundamentos, das tecnologias e dos desafios envolvidos na área. Neste sentido, seu conteúdo pretende cobrir os seguintes pontos: *(i)* apresentar aplicações e métodos usados para estender processamento, armazenamento e aplicações em direção a borda da rede visando apoio às soluções em IoT; *(ii)* descrever como as soluções em Névoa podem tirar vantagem da sua proximidade às fontes de dados para atender requisitos como mobilidade, localidade e baixa latência; *(iii)* identificar os desafios associados com a mudança de paradigma promovida pela computação em Névoa.

O restante do capítulo está organizado como segue. Na Seção 6.2 são apresentados conceitos e características da Computação em Névoa e sua integração com outras tecnologias. Na Seção 6.3 é apresentado um estudo sobre aplicações e plataformas de Computação em Névoa, com ênfase em aspectos que definem suas arquiteturas. Na Seção 6.4 são discutidos desafios associados com a mudança promovida por este paradigma e as pesquisas futuras nesta área.

6.2. Fundamentos sobre Computação em Névoa

Neste tópico, é oferecida uma visão geral da Computação em Névoa abordando como as propostas atuais sobre a Internet das Coisas estão fomentando uma importante mudança de paradigma de um modelo centralizado para um modelo descentralizado. Um conjunto de tecnologias emergentes relacionadas são descritas a fim de identificar o seu escopo, requisitos e integração. Serão enfatizadas a maturidade dessas tecnologias, os problemas não resolvidos pela computação em Nuvem e as motivações para a computação em Névoa.

6.2.1. Internet das Coisas

Em 1999, antes de *Kevin Ashton* criar o termo Internet das Coisas enquanto trabalhava no Auto-ID Labs [Auto-ID 2016], seu significado já fazia parte do imaginário de autores de ficção científica em livros, filmes, seriados e desenhos animados. Essa tecnologia é descrita em [Atzori et al. 2010] e [Gubbi et al. 2013] como um mundo repleto de objetos inteligentes e conectados, que participam do cotidiano das pessoas muitas vezes sem serem percebidos. Neste cenário, são capazes de interagir com o ambiente, trocar informações, monitorar processos, coletar estados, analisar dados, obedecer comandos e executar ações de forma coordenada e proativa para atender as finalidades de seus usuários.

Dentre os mais recentes paradigmas da computação, a Internet das Coisas é apontada como uma tecnologia emergente em [Gartner Inc. 2015]. Este documento eletrônico apresenta um relatório gráfico atualizado todos os anos com expectativas na área de Tecnologia da Informação (TI) e Marketing Digital. O *Hype Cycle* [Gartner Inc. 2016] serve como referência mundial para governos e organizações sobre a relevância e amadurecimento das tecnologias, dividido em cinco fases: inovação (*Innovation Trigger*), ápice (*Peak of Inflated Expectations*), desilusão (*Trough of Desillusion*), esclarecimento (*Slope of Enlightenment*) e plenitude (*Plateau of Productivity*).

A fase de inovação é um período inicial onde são estabelecidas provas de conceito e protótipos sobre o paradigma. Na fase de ápice acontece uma diminuição de suas expectativas com o lançamento de seus primeiros produtos ou aplicações. A fase de desilusão envolve adaptações que resultam em novas versões ou mesmo em sua obsolescência prematura. Caso ultrapasse esse período, novas aplicações podem ser descobertas na fase de esclarecimento para atingir seu potencial produtivo na fase de plenitude. A Figura 6.1 mostra que em 2015 a Internet das Coisas atingiu seu ápice de expectativas apoiada pelo surgimento de diferentes aplicações específicas [Vermesan and Friess 2014].

O desenvolvimento de ambientes para IoT é um passo necessário à evolução de tecnologias como Redes Inteligentes de Energia (*Smart Grids*), Sistemas de Transporte Inteligentes (*Intelligent Transportation*) e Cidades Inteligentes (*Smart Cities*). Juntas com a Internet das Coisas, essas soluções fazem parte de uma classe mais genérica de sistemas chamada de Sistemas Ciber-Físicos (*Cyber-Physical Systems*, CPS) [Stojmenovic 2014b].

Esses sistemas são caracterizadas pela colaboração entre elementos computacionais com o intuito de controlar entidades físicas. Em particular, IoT emprega serviços de comunicação convencionais para interligar objetos físicos identificados por endereços baseados na Internet, mas a interconexão de dispositivos através de redes de computadores não é obrigatório em CPS. Além dos objetos físicos, uma arquitetura IoT deve compreender

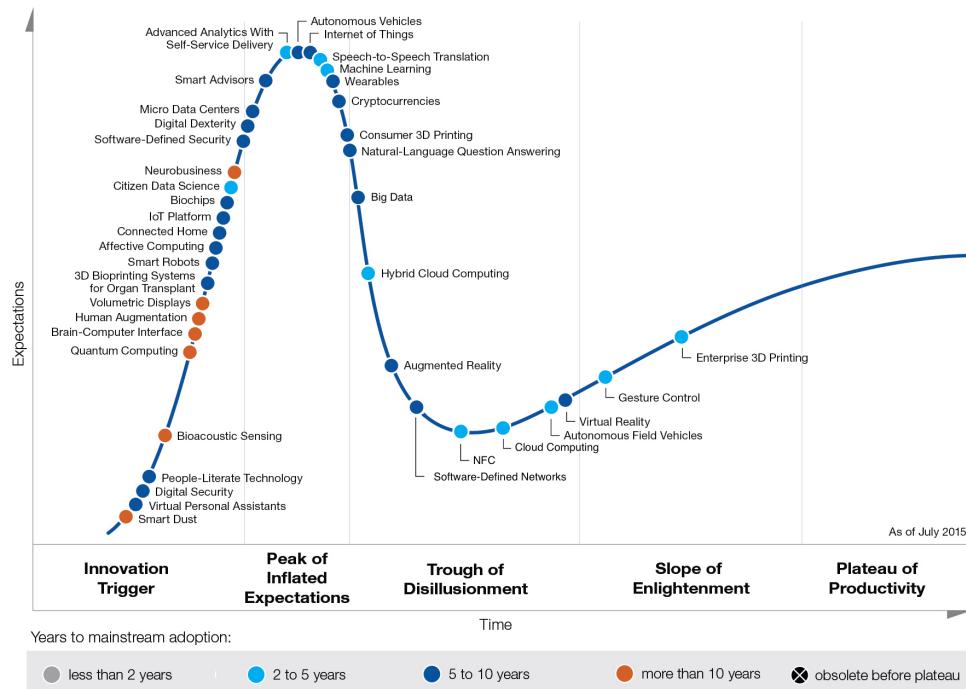


Figura 6.1. O Hype Cycle do Gartner divulgado em Julho de 2015 sobre tecnologias emergentes. Fonte: [Gartner Inc. 2015]

der também outros componentes para permitir uma computação ubíqua integrada.

Em [Gubbi et al. 2013] é apresentada uma taxonomia dos elementos necessários à implementação da Internet das Coisas. Os componentes de hardware considerados atômicos como *Radio-Frequency IDentification* (RFID), *Near Field Communication* (NFC) e *Wireless Sensor and Actuator Networks* (WSAN) são responsáveis pela identificação e conexão entre o mundo de objetos reais e sua representação digital. Uma ou mais camadas de software especial ou *middleware* oferecem uma abstração de funcionalidades para lidar com a heterogeneidade e as capacidades limitadas desses elementos, além de prover o gerenciamento e a composição de serviços para uma ampla variedade de aplicações. A Figura 6.2 mostra os componentes IoT sobre uma Arquitetura Baseada em Serviços (*Service Oriented Architecture*, SOA) organizada em diferentes camadas.

Como identificado em [Atzori et al. 2010], o paradigma da Internet das Coisas pode ser concebido sobre três diferentes visões: orientado a "coisas" (sensores), orientada à Internet (*middleware*) ou orientada à semântica (conhecimento). Embora essa delimitação seja necessária pela natureza interdisciplinar do assunto, as soluções em IoT são efetivas apenas no domínio de interseção desses três pontos de vista. Em [Gubbi et al. 2013] é apresentada uma definição unificadora baseada na interconexão de dispositivos embarcados com sensores e atuadores sobre um quadro operacional comum para permitir o desenvolvimento de aplicações inovadoras. Essa abordagem facilita o compartilhamento de informações entre plataformas através de uma estrutura integrada em Nuvem.

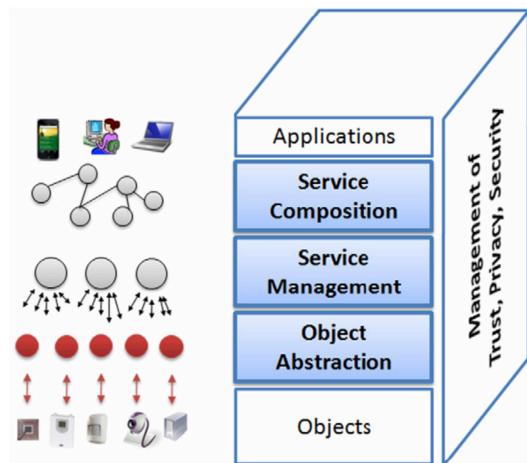


Figura 6.2. Visão geral da arquitetura IoT. Fonte: [Atzori et al. 2010]

6.2.2. Computação em Nuvem

O modelo em Nuvem teve origem na adoção de aplicações que fazem uso de enormes centros de dados com capacidade de suportar serviços Web em larga escala na Internet. Mesmo que a ideia original não seja nova, sua adoção possibilitou o uso eficiente e otimizado dos recursos de hardware e software em ambientes de Tecnologia da Informação (TI). Avanços posteriores em gerenciamento automatizado, técnicas de balanceamento de carga e virtualização permitiram a alocação dinâmica de recursos e o provisionamento elástico de sua infraestrutura aos clientes.

A arquitetura de Nuvem pode ser dividida em quatro camadas [Zhang et al. 2010]: centro de dados (hardware), infraestrutura, plataforma e aplicação. Cada uma delas pode ser vista como um serviço para a camada superior e como um cliente para a camada inferior. Este arquitetura alcançou popularidade pela oferta da infraestrutura da Nuvem em três principais modelos de serviço [Zhang et al. 2010]: Software como Serviço (*Software as a Service*, SaaS), Plataforma como Serviço (*Platform as a Service*, PaaS), Infraestrutura como Serviço (*Infrastructure as a Service*, IaaS).

Essa diversidade de clientes e serviços levou a diferentes modelos de desenvolvimento como descritos em [Zhang et al. 2010]: Nuvem Privada (*Private Cloud*), Nuvem Comunitária (*Community Cloud*), Nuvem Pública (*Public Cloud*) e Nuvem Híbrida (*Hybrid Cloud*). Cada tipo de Nuvem tem suas próprias vantagens e desvantagens, onde a opção por um modelo depende do cenário específico considerando os diferentes aspectos do negócio, os requisitos dos usuários e os ambientes de Nuvem envolvidos.

Seu nível atual de amadurecimento em relação à outras tecnologias pode ser vista através da popularidade em buscadores na Internet. A figura 6.3 mostra a popularidade dos termos *Cloud Computing*, *Big Data* e *Internet of Things* em consultas ao Google nos últimos dez anos [Google Trends 2016]. Os gráficos de popularidade podem ser comparados com o *Hype Cycle* da figura 6.1. Por exemplo, a curva *Cloud Computing* na

figura 6.3 apresenta um contorno similar com a fase de desilusão indicada no *Hype Cycle*, acompanhada por *Big Data* e a Internet das Coisas em seu ápice de expectativas.

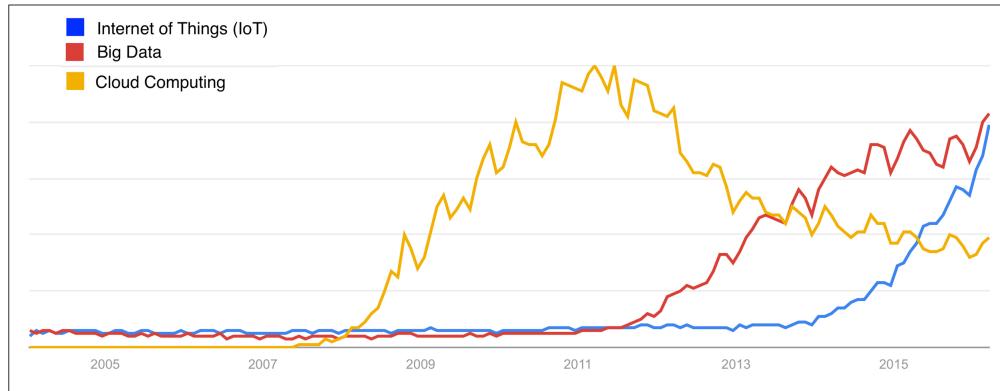


Figura 6.3. Pesquisa do Google sobre a popularidade dos termos *Cloud Computing*, *Big Data* e *Internet of Things*. Fonte: [Google Trends 2016]

Em sua fase de evolução atual, diferentes exemplos dessa tecnologia já se consolidaram através da Internet, onde novos serviços híbridos começam a ser oferecidos por provedores públicos e privados. Embora as empresas mais conservadoras continuem cautelosas quanto à segurança de suas informações, elas migram seus recursos menos críticos para Nuvem buscando usufruir das vantagens técnicas e econômicas desde modelo [Zhang et al. 2015]. Entretanto, a fase de plenitude produtiva desta tecnologia ainda não foi alcançada pela falta de um entendimento completo de suas potencialidades.

Neste sentido, sua agregação com outras tecnologias permitirá que a arquitetura em Nuvem se torne cada vez mais compreendida, difundida e adotada como um importante componente da Internet do Futuro. Em particular, um novo paradigma integrando a Computação em Nuvem com a Internet das Coisas é desafiador e favorável a um grande número de cenários de aplicação, como descrito nos próximos tópicos deste capítulo.

6.2.3. Integração entre Computação em Nuvem e Internet das Coisas

A Computação em Nuvem e a Internet das Coisas são tecnologias que evoluíram de forma independente, baseadas em cenários de aplicação específicos. Embora esses dois paradigmas apresentem definições distintas, pesquisas atuais propõem sua integração com base em aspectos complementares resumidos na Tabela 6.1. Essas soluções são descritas como Nuvem das Coisas (*Cloud of Things*) em [Aazam et al. 2014] e Nuvem IoT (*Cloud IoT*) em [Botta et al. 2016]. Em [Botta et al. 2016], os fatores que motivam essa integração são classificados em três categorias: comunicação, armazenamento e processamento.

- *Motivadores de comunicação:* estão relacionados com o compartilhamento de dados e aplicações através de uma infraestrutura que facilite a conexão entre os elementos e o gerenciamento dos objetos. Neste sentido, as soluções proprietárias em Nuvem oferecem uma forma eficaz para conectar, controlar e gerenciar dispositivos remotos sem restrições de tempo ou localidade através de redes de alta velocidade e aplicativos embutidos em interfaces personalizadas na Internet [Rao et al. 2012].

Tabela 6.1. Comparação de aspectos complementares da Computação em Nuvem e IoT.

Característica / Paradigma	IoT	Nuvem
Modelo de computação	distribuído ou pervasivo	centralizado
Disponibilidade de acesso	local ou limitado	global ou ubíquo
Natureza dos componentes	objetos físicos	recursos virtuais
Capacidade de processamento	limitada	virtualmente ilimitada
Capacidade de armazenamento	limitada ou nenhuma	virtualmente ilimitada
Função da Internet	ponto de convergência	meio de prover serviços
Análise de dados	análise em tempo real	análise de <i>Big Data</i>

- *Motivadores de armazenamento:* buscam compensar as restrições de espaço para arquivos de dados nos dispositivos IoT através de um serviço de memória não volátil em larga escala e sob demanda, baseada na virtualização ilimitada de recursos [Rao et al. 2012]. A Internet das Coisas envolve muitas fontes ou objetos que geram um fluxo de dados com características de volume (quantidade), variedade (tipos de dados) e velocidade (frequência) típicas de *Big Data* [Zikopoulos et al. 2011]. Uma vez depositados na Nuvem, os dados podem ser protegidos do acesso indevido por níveis configuráveis de segurança [Dash et al. 2010] e podem ser manipulados de maneira uniforme [Zaslavsky et al. 2013] ou compartilhados usando uma API (*Application Programming Interface*) bem definida [Fox et al. 2012].
- *Motivadores de processamento:* dizem respeito às limitações computacionais dos dispositivos IoT na execução local de algoritmos complexos considerando suas restrições de energia [Yao et al. 2013]. Em ambientes IoT, os dados coletados são usualmente transmitidos para outros elementos mais poderosos, onde sua agregação e processamento é factível. Transferir essa responsabilidade para uma plataforma de Nuvem permite economizar a energia dos dispositivos IoT acessando serviços externos sob demanda. Além disso, seu processamento virtualmente ilimitado possibilita a realização de análise de dados [Dash et al. 2010] [Rao et al. 2012] e o controle de eventos complexos [Rao et al. 2012].

Outros motivadores em [Botta et al. 2016] são apontados como transversais e têm implicações em todas as categorias. Por exemplo, o modelo em Nuvem vem abordando questões que também precisam ser tratadas em IoT. As soluções existentes para problemas de heterogeneidade, escalabilidade, interoperabilidade, flexibilidade, confiabilidade, eficiência, disponibilidade e segurança são motivadores transversais à integração desses dois paradigmas. Além disso, agregando o fluxo de dados dos objetos em uma infraestrutura unificada torna possível uma rápida configuração e integração de novos elementos. Esse fator incentiva e facilita a implantação dos serviços, proporcionando meios para aumentar receitas e reduzir os riscos envolvidos [Zaslavsky et al. 2013].

Entretanto, a Computação em Nuvem também pode se beneficiar da Internet das Coisas para ampliar seus limites, fornecendo suporte a grande número de situações do mundo real. A arquitetura em Nuvem IoT deve fornecer uma camada intermediária para abstrair a complexidade e prover as funcionalidades necessárias entre os objetos e as aplicações. Uma arquitetura típica é descrita em [Taivalsaari and Mikkonen 2015] onde seus elementos de mais alto nível estão representados na Figura 6.4.

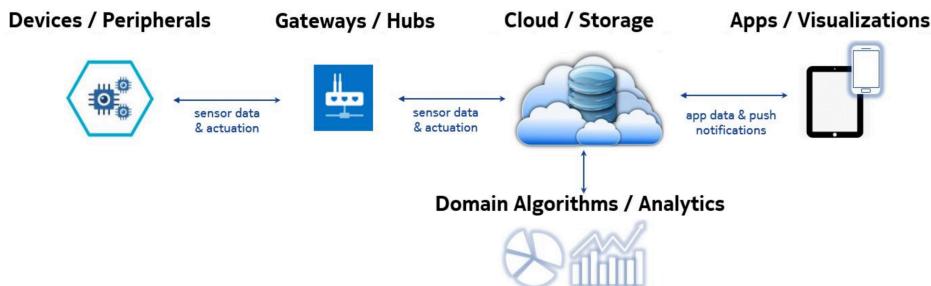


Figura 6.4. Arquitetura Comum em Nuvem IoT. Fonte: [Taivalsaari and Mikkonen 2015]

Nesta arquitetura comum, os objetos ou dispositivos embarcados com sensores e ou atuadores interagem para ativar ações ou submeter dados em resposta aos pedidos de outros componentes de capacidade superior em uma rede de sensores. Os *gateways* ou *hubs* são dispositivos de acionamento, coleta e transferência de dados a partir dos dispositivos periféricos com sensores e atuadores para Nuvem. Usando diferentes protocolos de comunicação (com ou sem fio) permitem uma conexão segura entre diferentes redes físicas e podem apoiar tarefas como armazenamento temporário, *cache* de dados, pré-processamentos, descoberta de serviços, geo-localização e cobrança. Em algumas soluções, os dispositivos embarcados são capazes de receber comandos de atuação ou enviar dados de sensoriamento diretamente para Nuvem sem a necessidade de *gateways* dedicados, ou agir como *gateways* intermediários para outros dispositivos.

Como discutido anteriormente nos motivadores de integração, a Nuvem possui um papel central nesta arquitetura. Uma de suas funções envolve a manutenção do registro com informações ou metadados sobre os objetos gerenciados no sistema. No caso mais simples, o registro pode ser um arquivo em um banco de dados contendo IDs (identificadores) ou URL (*Uniform Resource Locator*) dos dispositivos. Porém, normalmente é um componente abstrato que fornece uma API de programação independentemente da solução de armazenamento subjacente. Assim, os desenvolvedores podem obter e apresentar as informações em diferentes interfaces (móvel, web, etc.) para os usuários.

Outra função importante é a aquisição e armazenamento de dados, onde as soluções podem envolver sistemas escaláveis com replicação massiva e tolerância a falhas. Devido ao crescente aumento no número de dispositivos associados a IoT, as tecnologias em Nuvem podem ser empregadas no armazenamento do enorme volume de dados gerados por esses objetos. Requisitos de latência ou atraso para acesso aos dados históricos ou informações deles extraídas podem variar dependendo da aplicação.

As funções de análise e visualização de informações buscam examinar, relacionar e transformar os dados adquiridos através dos sensores a fim de descobrir e apresentar informações úteis aos usuários ou ao próprio sistema. Devido ao volume, variedade e velocidade de informações geradas pelos dispositivos, diferentes algoritmos de aprendizado de máquina e mineração de dados como redes neurais, algoritmos genéticos ou árvores de decisão podem ser empregados na análise dos dados gerados por esses objetos [Bonomi et al. 2012]. A integração das tecnologias de Nuvem com a análise de *Big Data* vem per-

mitindo um ciclo constante de inovação favorável ao desenvolvimento das plataformas voltadas à IoT [Mineraud et al. 2015].

De forma similar à análise de dados, funções que permitem a programação dos objetos bem como a configuração de ações baseadas em informações históricas ou instantâneas sobre dados de sensores devem ser definidas de forma ampla e segura nesta arquitetura. A Nuvem é um ambiente atrativo para o desenvolvimento de aplicações devido aos seus modelos de programação em alto nível que facilitam o desenvolvimento de serviços em larga escala. A oferta de interfaces integradas e confiáveis para programação remota dos elementos atuadores é fundamental para assegurar uma visão ubíqua em IoT uma vez que sua execução envolve diferentes dispositivos móveis e sensores.

Na medida que novos tipos de informações, recursos, objetos e pessoas são conectadas nesta arquitetura, os usuários espalhados por todo o mundo devem fazer parte rapidamente da Internet de Coisas. A adoção de um modelo em Nuvem para IoT permite a criação de novos paradigmas de serviço inteligentes com base na capacidades de seus componentes para lidar com uma série de cenários futuros. Descritos genericamente em [Duan et al. 2015] como XaaS (*Everything as a Service*), essas propostas incorporam diferentes aspectos de "coisas" como serviço ou *Things as a Service* (TaaS) [Christophe et al. 2011] [Mitton et al. 2012] [Distefano et al. 2012]. Alguns exemplos e suas referências como identificado em [Botta et al. 2016] estão resumidos na Tabela 6.2.

Esta seção abordou as principais motivações que impulsionam a integração do modelo em Nuvem com a Internet das Coisas. Porém, restrições inerentes a sua arquitetura dificultam cenários de aplicação específicos envolvendo um número crescente de objetos em ambientes densamente distribuídos. Para isso, descrevemos na próxima seção como algumas propostas recentes buscam estender os recursos computacionais disponíveis na Nuvem para as extremidades da rede visando apoio às aplicações em IoT. Exemplos de soluções e plataformas serão descritas a seguir na seção 6.3.

6.2.4. Tecnologias Emergentes de Nuvem IoT

Apesar das potenciais vantagens de modelo baseado em Nuvem para Internet das coisas, alguns cenários não são favoráveis a sua aplicação. Os sistemas de Computação em Nuvem são altamente centralizados, onde maioria da computação ocorre em poucos e grandes centros de dados espalhados pelo mundo. Embora esta abordagem ofereça benefícios, ela tem um custo elevado em termos de comunicação e consumo de energia.

Em ambientes IoT onde os dispositivos estão geograficamente próximos uns dos outros, seria ineficiente transmitir todos os dados de sensoriamento para núcleos de processamento distantes e esperar por comandos a partir de um centro remoto para dispositivos atuadores individuais. Nesse cenário, eventuais sobrecargas e atrasos muito peculiares na Internet tornariam as soluções IoT com requisitos de baixa latência impraticáveis. Por exemplo, aplicações para Internet Tátil (*Tactile Internet*) [Simsek et al. 2016] requerem conexões ultra-confiáveis e com latência de 100 ms, 10 ms e 1 ms para realizar respectivamente experiências auditivas, visuais e manuais remotas em tempo real.

As soluções que requerem uma latência muito baixa a nível de aplicação são desafiadoras na Internet. Uma partícula viajando a velocidade da luz (186,3 milhas por

Tabela 6.2. Novos paradigmas de serviço em Nuvem IoT.

XaaS (por extenso)	Referências	Descrição
TaaS (Things as a Service)	[Distefano et al. 2012] [Mitton et al. 2012] [Christophe et al. 2011]	abstração de recursos heterogêneos com semântica similar a dos objetos
SaaS (Sensing as a Service)	[Zaslavsky et al. 2013] [Rao et al. 2012] [Dash et al. 2010]	acesso ubíquo a dados de sensores
SAaaS (Sensing and Actuation as a Service)	[Rao et al. 2012]	implementação da lógica de controle e automação
SEaaS (Sensing Event as a Service)	[Rao et al. 2012] [Dash et al. 2010]	envio de mensagens desencadeadas por eventos em sensores
SenaaS (Sensor as a Service)	[Zaslavsky et al. 2013]	gerenciamento ubíquo de sensores remotos
DBaaS (Database as a Service)	[Zaslavsky et al. 2013]	gerenciamento ubíquo de banco de dados
DaaS (Data as a Service)	[Zaslavsky et al. 2013]	acesso ubíquo a qualquer dado
EaaS (Ethernet as a Service)	[Zaslavsky et al. 2013]	conectividade em nível de camada 2 para dispositivos remotos
IPMaaS (Identity and Policy Management as a Service)	[Zaslavsky et al. 2013]	gerenciamento de políticas de acesso e identidade

milésimo de segundo) levaria aproximadamente 22,5 ms para viajar ida e volta a menor distância de costa a costa (2092 milhas) dos Estados Unidos. Mesmo sem considerar atrasos de *buffering*, filas, ou qualquer tipo de processamento na Nuvem, esse tempo de latência inviabilizaria diferentes tipos de aplicações de tempo real.

Outra questão é o aumento do número dos objetos, que deve gerar uma enorme quantidade de dados produzidos nas extremidades da Internet. Em 2014, o volume de dados gerados por dispositivos IoT ultrapassou 200 exabytes, sendo estimado um total anual de 1,6 zettabytes em 2020 [ABI Research 2015]. Atualmente, apenas uma pequena percentagem dos dados produzidos por esses elementos são enviados e ou armazenados em Nuvem. A maioria é processado ou armazenado localmente e não estão acessíveis para aplicação de técnicas como análise de dados ou *Big Data* [ABI Research 2015].

Agravando este cenário, o custo médio de largura de banda vem diminuindo a uma taxa inferior quando comparado ao custo médio de processamento ou de armazenamento [Nielsen Norman Group 2014]. O aumento do poder computacional torna os dispositivos miniaturizados cada vez mais acessíveis e produtivos enquanto a capacidade de enviar dados a partir da borda da Internet para a Nuvem enfrenta atrasos causados pelo crescimento impulsivo da concorrência aos recursos de comunicação disponíveis.

Essa tendência para concentração dos dados nas bordas da rede é uma realidade contemporânea e estimulada pelo atual crescimento da Internet das Coisas. Diferentes técnicas que minimizem a quantidade de dados enviados para Nuvem através do processamento local em elementos periféricos serão fundamentais na redução dos custos envolvidos e no tempo de resposta das aplicações. Uma vez que nem todos os dados estarão localizados no núcleo da arquitetura de Nuvem IoT, os aplicativos também serão atraídos para borda da rede pelo efeito crescente da gravidade de dados [Fritsch and Walker 2014].

A execução de aplicações nas extremidades da rede passa a ser um interessante estímulo para ampliar as fronteiras do modelo de Nuvem IoT visando aproveitar o poder de processamento, armazenamento e comunicação atual dos diferentes tipos de dispositivos móveis inteligentes que são conduzidos por pessoas em todos os lugares do mundo. Por exemplo, realidade virtual, sensoriamento e navegação são exemplos de aplicações sofisticadas que podem se beneficiar de recursos locais oferecidos aos usuários.

Como as aplicações dos usuários são executadas em redes sem fio ou redes de rádio celular, o conceito de borda de rede envolve os provedores de acesso à Internet (*Internet Service Provider*, ISP). Por exemplo, o código de uma aplicação de realidade aumentada poderia ser dividida em três partes: o aplicativo cliente executado no celular do usuário, os serviços remotos executados a partir do servidor em Nuvem e os serviços locais executados junto (ou em nível acima) da estação base de acesso do usuário.

Quando a execução do código da parte servidor está localizado na borda da rede, a aplicação pode fazer uso de informações em tempo real para tornar mais inteligente a entrega do serviço ao usuário. Por exemplo, informações de congestionamento e largura de banda de acesso concedida através de ISPs podem ser usadas por aplicativos que utilizam a plataforma *Netflix Open Connect* [Netflix 2016] para definir a qualidade do fluxo de vídeo suportado ou seu redirecionamento para o servidor de borda mais próximo ao cliente, como parte de uma solução em Nuvem para entrega de conteúdo sob demanda.

Entretanto, uma infraestrutura em Nuvem plenamente extensível para borda da rede depende da cooperação entre diferentes atores como prestadoras de serviços em Nuvens públicas e privadas, desenvolvedores em Internet das Coisas, provedores de acesso à Internet e diferentes organizações de padronização. Atualmente, a indústria de telecomunicações está passando por uma grande revolução técnica caracterizada pela presença de tecnologias facilitadoras exemplificadas nas propostas abaixo:

- *Redes programáveis* - em [Manzalini and Crespi 2016] é apresentada uma plataforma de telecomunicações que emprega tecnologias de Virtualização das Funções da Rede (*Network Functions Virtualization*, NFV) e Redes Definidas por Software (*Software Defined Network*, SDN) de modo a facilitar a implementação de serviços em Nuvem através da borda da rede. O paradigma SDN separa os planos de controle (inteligência) e comunicação de dados (encaminhamento) em funções distintas, onde os nós da rede seguem o caminho de comunicação obtido pela consulta a um servidor centralizado. Porém, em ambientes com diferentes domínios, esse serviço de controle centralizado pode precisar de uma implementação distribuída.
- *Fatiamento (slicing) de rede* - em [Shimojo et al. 2015], é proposta uma arquitetura em redes móveis para o fornecimento e operação de serviços heterogêneos baseada no fatiamento virtual da infraestrutura de telecomunicações física disponível (canais, redes, hardware, etc.) de forma customizada e configurada para fins específicos ou arrendatários, atendendo diferentes requisitos dos clientes.
- *Interface de rádio 5G* - em [Simsek et al. 2016] esta tecnologia é descrita como um padrão ainda em desenvolvimento que será supostamente flexível para possibilitar uma variedade de novos cenários de uso em redes móveis, incluindo suporte a uma alta largura de banda e baixa latência.

Essas tecnologias podem oferecer suporte as soluções em Nuvem IoT a partir da perspectiva de redes de comunicação, mas sozinhas não são suficientes para abordar todos os problemas relacionados à extensão dessa arquitetura para borda da rede. Outros paradigmas emergentes da integração do modelo em Nuvem com a Internet das Coisas empregam terminologias distintas para representar conceitos semelhantes, onde recursos de computação são localizados próximos dos usuários visando superar limitações como mobilidade, localidade e baixa latência. A popularidade dos termos mais empregados são comparadas na Figura 6.5 e seus significados são descritos logo a seguir.

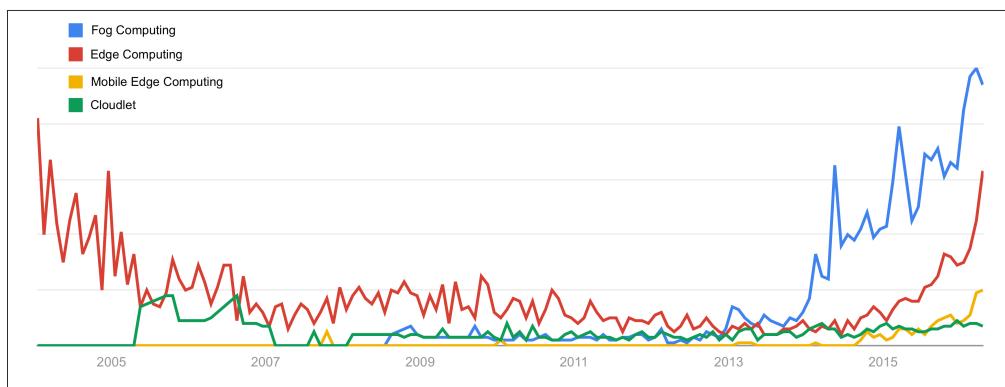


Figura 6.5. Paradigmas emergentes do modelo Nuvem IoT. Fonte: [Google Trends 2016]

- Computação nas Bordas (*Edge Computing*) - no gráfico da Figura 6.5 é o termo mais usado e genérico para designar tecnologias em borda de rede. Entretanto, é usado em propostas que nem sempre envolvem conceitos da Computação em Nuvem ou Internet das Coisas como autenticação de consultas em banco de dados distribuídos e replicação de *caches*. O termo *Edge Cloud Computing*, embora pouco usado, é mais adequado por ressaltar o relacionamento com as tecnologias de Nuvem.
- Mini-nuvens (*Cloudlets*) - pesquisadores da *Carnegie Mellon University* (CMU) [Elijah 2016] apresentaram o conceito em [Satyanarayanan et al. 2009] como uma camada intermediária entre dispositivos móveis e o centro de computação em Nuvem. Este trabalho pioneiro disponibilizou sistemas de código aberto em [Github 2016]. Enquanto [Gao et al. 2015] e [Satyanarayanan et al. 2015] discutem sua utilidade, [Ha and Satyanarayanan 2015] apresenta uma visão técnica detalhada. Como o termo é usado em outras áreas, a curva no gráfico na Figura 6.5 pode mostrar uma popularidade maior do que apenas no domínio de tecnologias de Nuvem.
- Computação Móvel em Nuvem (*Mobile Cloud Computing*, MCC) - é definida em [Dinh et al. 2013] como uma infra-estrutura onde o processamento e o armazenamento de dados são movidos dos dispositivos móveis para as plataformas em Nuvem. Esses dispositivos móveis não precisam possuir uma configuração avançada de hardware visto que as aplicações são executadas remotamente na Nuvem e acessadas através de conexões sem fio. A interação dos usuários com o sistema acontece por meio de interfaces leves ou navegadores *web* instalados nos clientes.

- Computação Móvel nas Bordas (*Mobile Edge Computing*, MEC) - definida pelo *European Telecommunications Standards Institute* (ETSI) através de uma especificação para indústria em [ETSI ISG MEC 2015]. Envolve o desenvolvimento de uma arquitetura e uma série de APIs padronizadas para o suporte da computação em Nuvem através das estações base nas redes móveis de rádio.
- Micro Centro de Dados (*Micro Datacenters*, MDC) - a Microsoft anunciou em [NetworkWorld 2015] seu emprego como uma extensão aos centros de dados Microsoft Azure para tratar dos custos envolvidos com as tecnologia de Nuvem [Greenberg et al. 2008], otimizar o desempenho dos pequenos dispositivos e melhorar a performance das aplicações dirigidas à Internet das Coisas.
- Computação em Névoa (*Fog Computing*) - é considerada como uma extensão não-trivial da computação em Nuvem [Bonomi et al. 2012]. Em [Vaquero and Roder-Merino 2014] é oferecida uma definição abrangente, com ênfase em algumas propriedades importantes como a predominância de acesso sem fio, heterogeneidade, distribuição geográfica, ambiente de execução, etc.

Entretanto, não existe uma nítida distinção entre essas propostas que parecem convergir sobre os seguintes pontos identificados em [Klas 2016]:

- *Mini-centros de processamento de dados* - introduzem uma versão em miniatura de um ambiente de Computação em Nuvem com suporte a virtualização de recursos que podem ser mantidos pelas companhias de telecomunicações e outras empresas consorciadas. Dependendo da proposta acima, esses elementos podem ser referenciados como *micro datacenters*, *cloudlets*, *fog nodes* ou servidores MEC.
- *Distribuição de recursos em larga escala* - promovem a distribuição de pequenas Nuvens em centenas ou milhares de pontos estratégicos de um estado ou país para fornecer recursos computacionais aos clientes. Sua localização dependerá de fatores como economia de energia ou requisitos de latência das aplicações, distribuídas em uma arquitetura com no mínimo três camadas como mostrado na Figura 6.6. Pontos prováveis de instalação são nas estações base, em comutadores de agregação ou nas centrais de suporte de rede das empresas de telecomunicações.
- *Infraestrutura e plataforma como Serviço*: oferecem uma infraestrutura integrada em pequenas Nuvens seguindo os modelos IaaS e PaaS descritos na seção 6.2.2. Nesta plataforma, aplicações podem ser implementadas de maneira bastante ágil usando ambientes de Máquina Virtual (*Virtual Machine*, VM). O modelo de plataforma como serviço favorece a migração de VMs em tempo de execução e sob demanda entre as pequenas Nuvens para tratar questões de mobilidade dos clientes.
- *Serviços Especiais* - oferecem serviços exclusivos em algumas pequenas Nuvens usando informações apenas presentes na rede local ou em suas proximidades. Por exemplo, uma pequena Nuvem pode hospedar um serviço que fornece acesso as estimativas de tráfego na vizinhança. Essas informações podem ser utilizadas pela aplicação em tempo real para ajustar as rotas iniciais transmitidas aos usuários.

Dentre os termos analisados na Figura 6.5 é possível notar que a Computação em Névoa vem crescendo constantemente desde a sua adoção no final de 2012 pela Cisco [Bonomi et al. 2012]. Os tópicos a seguir abordam esse paradigma, que desonta como uma solução integrada para estender os recursos da Computação em Nuvem em direção a borda da rede buscando cumprir requisitos não atendidos por um modelo clássico centralizado.

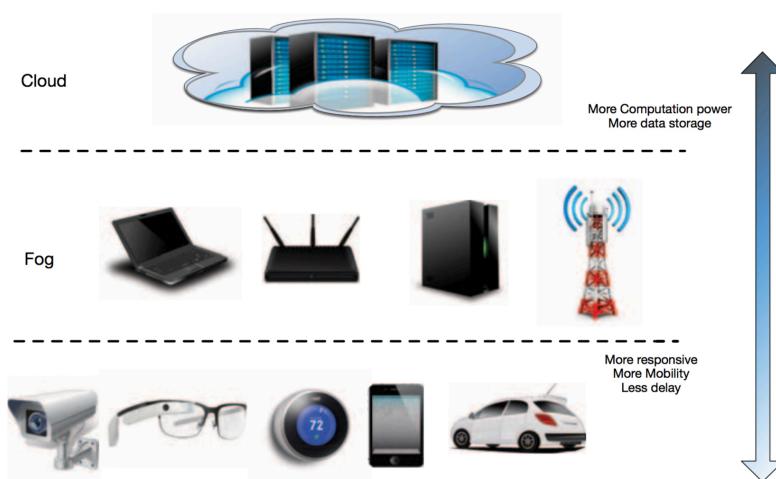


Figura 6.6. Arquitetura em três camadas: dispositivos inteligentes e sensores, Névoa/cloudlets/MEC e a Computação em Nuvem. Fonte: [Yi et al. 2015c]

6.2.5. Caracterização da Computação em Névoa

A computação em Névoa é definida em [Bonomi et al. 2012] como uma plataforma altamente virtualizada que fornece serviços de computação, armazenamento e comunicação entre os dispositivos finais e os centros de dados tradicionais de computação em Nuvem, localizada normalmente, mas não exclusivamente, na borda da rede. Essa definição implica em uma série de características que tornam a Névoa uma extensão não-trivial da Nuvem, como descritas em [Bonomi et al. 2012] a seguir:

- *Reconhecimento de localidade e baixa latência* - a origem da Computação em Névoa pode ser atribuída às propostas anteriores envolvendo pontos de acesso com suporte a serviços sofisticados na borda da rede, incluindo aplicações com requisitos de baixa latência como jogos, *streaming* de vídeo e realidade aumentada.
- *Distribuição geográfica* - em nítido contraste com a computação mais centralizada da Nuvem, os serviços e aplicações orientadas para Névoa demandam implantações amplamente distribuídas. Por exemplo, a Névoa vai desempenhar um papel ativo no fornecimento de *streaming* de alta qualidade para veículos em movimento, através de servidores proxies e pontos de acesso posicionados ao longo das estradas.
- *Suporte a redes de sensores em larga escala* - o monitoramento do ambiente através das redes de sensores, o controle de tráfego entre veículos conectados e as redes de

energia inteligentes (*Smart Grids*) em [Satyanarayanan et al. 2015] são exemplos de sistemas inherentemente distribuídos que exigem o controle e a oferta dos recursos de processamento, armazenamento e comunicação em uma escala Máquina-a-Máquina (*Machine-to-Machine*, M2M) [Stojmenovic 2014b].

- *Grande número de nós* - é uma consequência da ampla distribuição geográfica como evidenciada pelas tecnologias de redes de sensores em geral, e pela aplicação *Smart Grid* em particular. Os serviços são executados pelos nós presentes na Névoa como parte de uma aplicação em Nuvem distribuída. Quando possível, esse objetivo não é simples de alcançar em arquiteturas de hiperescala como a Internet.
- *Suporte a computação móvel* - em muitas aplicações de Névoa é essencial uma comunicação direta com os dispositivos associados para permitir o suporte às diferentes técnicas que podem ser empregadas na computação móvel, como por exemplo o protocolo LISP 1, que desassocia a identidade utilizada por um cliente da sua identidade local, e exige um sistema de diretório distribuído.
- *Interações em tempo real* - as principais aplicações em Névoa envolvem interações em tempo real, em vez do processamento em lote. Como a Névoa está localizada longe dos principais centros de processamento em Nuvem, é necessário a disponibilização e o gerenciamento dos recursos locais necessários para auxiliar o cumprimento dos requisitos de tempo de execução das aplicações.
- *Predominância do acesso sem fio* - para os dispositivos IoT algum tipo de protocolo de comunicação sem fio como RFID, Bluetooth, ZigBee, Wi-Fi ou LTE é a única forma possível de conexão em rede. Os nós presentes na Névoa devem oferecer serviços especiais que só podem ser exigidos no contexto da Internet das Coisas.
- *Heterogeneidade* - as Nuvens são geralmente ambientes fechados, que utilizam componentes de hardware de um mesmo fornecedor ou ambientes e linguagens de programação proprietárias. Pela sua abrangência e escopo, os dispositivos na Névoa podem ser oferecidos por diversos fabricantes, empregar diferentes ambientes e envolver variados desenvolvedores, linguagens e protocolos.
- *Interoperabilidade e federação* - o suporte contínuo e integrado de certos serviços requer a cooperação de diferentes provedores, onde *streaming* é um bom exemplo. Assim, os componentes de Névoa devem ser capazes de interagir de forma orquestrada e os serviços devem ser federados através de diferentes domínios.
- *Análise de dados em tempo real* - interagindo com a Nuvem e perto das fontes de dados, a Névoa está bem localizada para desempenhar um papel significativo na ingestão e processamento de dados em *Big Data* com restrições de tempo real.

A Computação em Névoa envolve a execução de aplicações sobre elementos distribuídos nas camadas entre os dispositivos sensores e a Nuvem. Elementos como *gateways* inteligentes, roteadores e dispositivos de Névoa dedicados podem oferecer recursos de processamento e armazenamento para permitir a extensão dos serviços de Nuvem

até a borda da rede. A Figura 6.7 mostra uma arquitetura de referência para a Computação em Névoa apresentada em [Dastjerdi et al. 2016]. Na parte inferior desta arquitetura encontram-se os objetos inteligentes, redes de sensores e atuadores, bem como dispositivos de borda e os *gateways*. Esta camada inclui aplicativos que podem ser instaladas nos dispositivos finais para ampliar sua funcionalidade. Os dispositivos nesta camada podem usar a camada seguinte para a comunicação com outros dispositivos ou com a Nuvem.

A camada de Rede deve favorecer também a conexão de outros elementos, não necessariamente sensores ou atuadores, conectados através de tecnologias de rede com ou sem fio. Além disso, esta camada pode prover acesso a recursos de rede virtualizados como instâncias de Névoa através de elementos inteligentes, capazes de processar e armazenar temporariamente dados coletados pelos *gateways* sobre dispositivos IoT da camada inferior. Estes dispositivos de Névoa também são responsáveis por filtrar e enviar informações para a Nuvem em uma base periódica de tempo.

Acima da camada de Rede são executados os serviços que oferecem suporte ao processamento de tarefas voltadas a Internet das Coisas para aplicações que precisam do auxílio de recursos virtualmente ilimitados disponíveis na Nuvem. No topo da camada de Nuvem reside o software de gerenciamento de recursos que coordena de forma global a infraestrutura e oferece qualidade de serviço para as aplicações em Névoa. Finalmente, na camada superior estão as aplicações que utilizam a infraestrutura de Computação em Névoa para fornecer soluções inovadoras e inteligentes para os usuários finais.

A camada de Gerenciamento de Recursos Definidos por Software implementa diferentes serviços de *middleware* para otimizar o uso dos recursos de Nuvem e Névoa em benefício das aplicações. O objetivo destes serviços é reduzir a carga de utilização da Nuvem ao mesmo tempo que melhora o desempenho das aplicações, transferindo a execução de tarefas para nós da Névoa e oferecendo níveis aceitáveis de latência. Isto pode ser alcançado pelo trabalho conjunto de diferentes serviços descritos a seguir:

- *Localização de Fluxo e Tarefas* - mantém informação sobre o estado dos recursos disponíveis na Nuvem, Névoa e na rede a partir de consultas ao serviço de Monitoramento visando identificar os melhores candidatos para receber tarefas e para suportar os fluxos de execução. Este componente se comunica com o serviço de Provisionamento de Recursos para indicar o número atual de fluxos e tarefas alocações, o que pode desencadear uma nova rodada de alocações quando a demanda pelos recursos for considerada elevada.
- *Base de Dados de Conhecimento* - armazena informações históricas sobre a demanda de aplicações e recursos, podendo ser fornecidas a outros serviços para auxiliar o processo de tomada de decisão.
- *Previsão de Desempenho* - consulta informações na Base de Conhecimento para estimar o desempenho dos recursos disponíveis. Esta informação é usada pelo serviço de Provisionamento de Recursos para decidir a quantidade de recursos que serão disponibilizados em momentos quando existe um grande número de tarefas e fluxos alocados, ou quando o desempenho não é satisfatório.

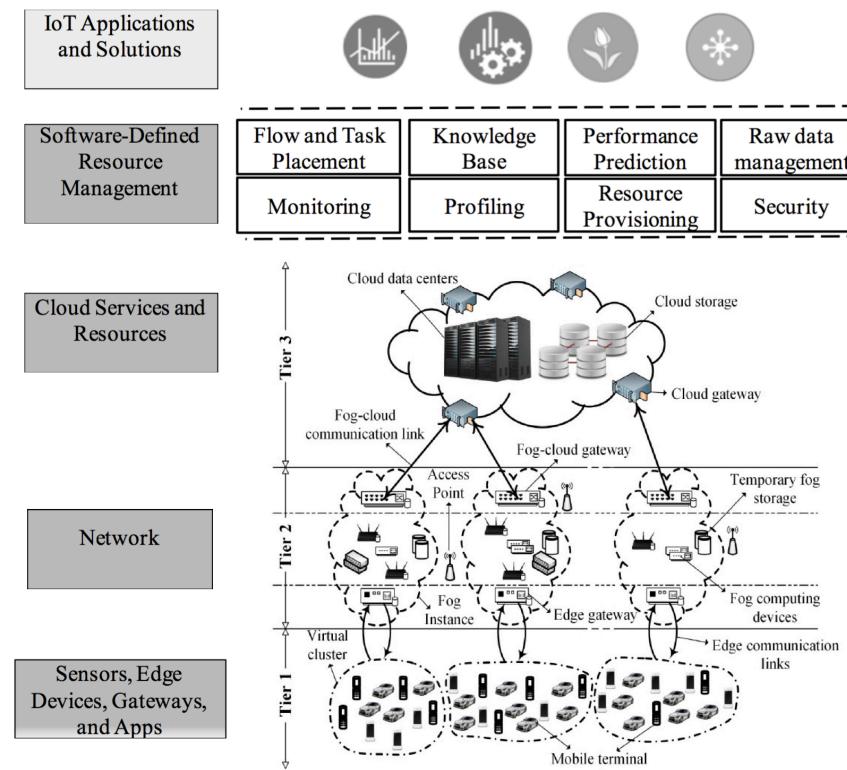


Figura 6.7. Arquitetura de referência para Computação em Névoa. Fonte: [Dastjerdi et al. 2016] e [Sarkar et al. 2015]

- *Gerenciamento de Dados* - oferece visões sobre os dados para outros serviços através do acesso direto às fontes e arquivos históricos. Essas visões podem ser obtidas por meio de consultas simples em SQL ou através de processamento mais complexos envolvendo técnicas de *Big Data* como *MapReduce*. No entanto, o método específico empregado na geração das visões é abstruído para os outros serviços.
- *Monitoramento* - mantém o controle do desempenho e do estado das aplicações, recursos e outros serviços, fornecendo essas informações conforme solicitado.
- *Gerenciador de Perfis* - estabelece perfis de recursos e aplicações baseadas em informações obtidas a partir da Base de Conhecimento e Monitoramento de serviços.
- *Provisionamento de Recursos* - é responsável pela aquisição de recursos na Nuvem, Névoa e na rede para hospedar as aplicações. Esta alocação é dinâmica, uma vez que o número de aplicações hospedadas e seus requisitos mudam ao longo do tempo. A decisão sobre os recursos é feita baseada nos requisitos de latência, nas credenciais gerenciadas pelo Serviço de Segurança, e nas informações fornecidas por outros serviços como Gerenciador de Perfis, Previsão de Desempenho e Monitoramento. Por exemplo, o componente transfere as tarefas com requisitos de baixa

latência para a borda da rede logo que os recursos apropriados ficam disponíveis.

- *Segurança*: fornece serviços de autenticação, autorização e criptografia para acesso e execução de serviços e aplicações, estendido a todos os elementos da Névoa.

É importante destacar que todos os elementos e serviços descritos são apenas de referência. As pilhas de protocolo e aplicações para Névoa podem ser desenvolvidas sem o uso de todos os elementos descritos, ou podem integrar outros componentes e serviços não apresentados na Figura 6.7 como aqueles relacionados na plataforma da Figura 6.11.

6.3. Aplicações e Plataformas de Computação em Névoa

Iniciativas para o emprego de soluções em Névoa devem surgir em diferentes setores de domínio público e privado. Nesta seção, buscaremos oferecer uma visão dessas aplicações em diferentes áreas e examinar suas plataformas sobre um ponto de vista arquitetural, bem como identificar a utilização de técnicas como virtualização, análise de dados, *caching* e segurança em redes na organização e implementação desses sistemas.

6.3.1. Aplicações em Computação em Névoa

As aplicações sobre a Internet das Coisas podem ser tão ou mais variadas quanto os dispositivos nela empregados. Elas possuem em comum a análise de dados em tempo real de "coisas" conectadas, podendo promover ações sobre seus elementos. Cada ação executada pode envolver uma comunicação Máquina-a-Máquina (*Machine-to-Machine*, M2M) [Stojmenovic 2014b] ou uma interação Homem-a-Máquina (*Human Machine Interface*, HMI) [Bonomi et al. 2012]. Exemplos incluem o acender de uma lâmpada, o acionamento de um motor, o fechamento de uma porta, a alteração das configurações de equipamentos, o acionamento dos freios de um carro, o movimento ou foco de uma câmera de vídeo, a abertura de uma válvula em resposta a uma leitura de pressão, etc.

Considerando as características descritas na seção 6.2.5, existe um conjunto de aplicações em Nuvem IoT que podem ser apoiadas pela computação em Névoa. Este tópico será então subdividido em áreas onde o atendimento desses requisitos contribuem para melhorar as propostas e soluções. Serão discutidos principalmente cenários que são fundamentais, motivadores e beneficiários do conceito de Computação em Névoa.

6.3.1.1. Redes de Sensores e Atuadores

Os nós tradicionais em redes de sensores sem fio (*Wireless Sensor Networks*, WSNs), comumente chamados *motes* [Kashi and Sharifi 2013], são projetados para trabalhar com níveis de energia extremamente baixos buscando prolongar a vida da bateria ou até mesmo acumular energia do ambiente quando possível [Rahimi et al. 2003].

A maioria dos WSNs (*Wireless Sensor Nodes*) podem ser distribuídos em amplas áreas geográficas, requerendo baixa largura de banda, baixo consumo de energia, baixo poder de processamento e pouca capacidade de memória. Atuando como fontes de dados unidirecionais para *gateways* estáticos chamados *sinks*, executam tarefas simples de processamento e encaminhamento de dados. O sistema operacional de código

aberto [TinyOS 2016] é um padrão usado nesses tipos de dispositivos, e vem provando sua utilidade em uma variedade de cenários envolvendo coleta de dados em diferentes ambientes (temperatura, umidade, quantidade de precipitação, intensidade de luz, etc.).

Devido às limitações dos WSNs, são propostas diferentes configurações para atender aos requisitos das aplicações [Kashi and Sharifi 2013]: múltiplos *sinks*, *sinks* móveis, múltiplos *sinks* móveis e sensores móveis. No entanto, em aplicações que exigem mais do que apenas funções de detecção e rastreamento é necessário o uso de atuadores exercendo ações físicas como abertura, fechamento, movimento, foco, etc. Os atuadores, recebendo comandos dos *sinks*, podem controlar um sistema ou o próprio processo de medição, ampliando o emprego de *Wireless Sensor and Actuator Networks* (WSANs).

Com o uso de atuadores, o fluxo de informação passa a ser bidirecional: dos sensores para o *sink* e do nó controlador para os atuadores. Essas soluções tornam-se sistemas de ciclo fechado em que os potenciais problemas de estabilidade e comportamentos oscilatórios não podem ser ignorados [Bonomi et al. 2012]. A latência e o *jitter* são questões dominantes em sistemas que requerem uma resposta rápida.

As características da Computação em Névoa como proximidade, consciência de localidade, geo-distribuição e organização hierárquica torna esse tipo de plataforma adequada para suportar restrições de energia em WSNs e WSANs. Além disso, essas são características típicas de computação em Névoa, e não de computação em Nuvem.

6.3.1.2. Análise de Dados

Enquanto os nós de Névoa fornecem uma computação localizada, permitindo assim baixa latência e consciência de contexto, a Nuvem oferece uma computação centralizada e global. A análise de dados é uma das aplicações fundamentais em Computação em Névoa, visto que muitas aplicações requerem tanto a localização da Névoa quanto a globalização da Nuvem, particularmente aquelas que fazem uso de análise de dados em tempo real.

Em [Bonomi et al. 2014] a aplicação da análise de dados em Névoa é iniciada a partir dos *gateways* na borda da rede, que coletam os dados gerados pelos sensores e dispositivos inteligentes. Alguns desses dados dizem respeito às aplicações que exigem processamento em tempo real como, por exemplo, em automação e controle de processos. A primeira camada da Névoa pode ser concebida para facilitar a interação M2M garantindo a coleta, o processamento dos dados e o controle dos dispositivos atuadores. Também pode filtrar os dados que serão processados localmente e enviar as informações resultantes para as camadas mais elevadas.

A segunda e a terceira camadas da Névoa podem permitir uma interação HMI tratando questões de visualização, relatórios, notificação, bem como sistemas e processos M2M. A escala de tempo dessas interações na Névoa podem variar de segundos a minutos para as análises em tempo real, até horas ou dias em análises transacionais. Como resultado, a Névoa tem de suportar vários tipos de armazenamento partindo de um modelo mais transitório na camada inferior até um suporte semi-permanente no nível mais elevado. É observado que quanto maior o nível da Névoa, maior a cobertura geográfica e mais longa a escala de tempo. A cobertura final global é fornecida pela Nuvem, que

é usada como repositório de dados com permanência de meses até anos, sendo tomada como base para análises voltadas à inteligência sobre negócios. Este é o ambiente HMI típico, com visualização dos principais indicadores de desempenho.

Como ilustrado na Figura 6.8, a medida que os dados são analisados na borda da rede e as informações são transferidas para o núcleo da Névoa elas podem ser usadas como retorno para aprimorar os modelos empregados, além de melhorar a tomada de decisão em tempo real. Diferentes métodos de otimização e predição podem ser usados como sistemas adaptativos, aprendizado de máquina, algoritmos genéticos, etc.

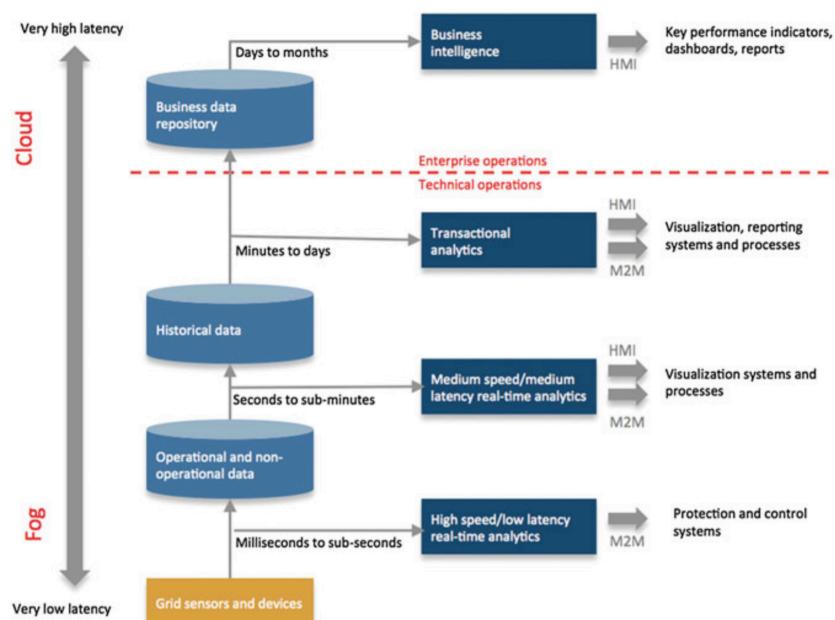


Figura 6.8. Análise de dados em Névoa: muitos usos para os mesmos dados.
Fonte: [Bonomi et al. 2014]

6.3.1.3. Cache de Dados

Em [Peng 2004] *Content Delivery Network* (CDN) é definida como uma rede de armazenamento em *cache* implementada através de servidores na borda da Internet para reduzir o atraso de *download* de conteúdos a partir de locais remotos. Esse tipo de rede é projetada para servir usuários tradicionais, com interesses muito mais amplos e difíceis de prever do que usuários móveis. Atuando em uma área de serviço precisa, cada dispositivo de Névoa possui usuários mais definidos e uma demanda por serviços mais específicos.

Portanto, é fundamental para aplicações em Névoa explorar essas características buscando oferecer de forma plena sua capacidade de armazenamento e computação. De maneira similar, *Information Centric Network* (ICN) [Ahlgren et al. 2012] também define uma infraestrutura de *cache* sem fio que fornece serviços de distribuição de conteúdo para

usuários móveis. Mas de maneira diferente dos servidores *cache* em CDN e ICN, os dispositivos de Névoa são unidades de computação inteligentes.

Com isso, podem ser utilizados não apenas para armazenamento, mas também como uma infraestrutura de computação que interage com usuários e dispositivos móveis para o processamento de dados em tempo real. Os dispositivos de Névoa podem ser interconectados a Nuvem para utilizar um amplo poder de processamento e ferramentas de análise em *Big Data* em outras finalidades como descritas nesta seção.

Em [Bastug et al. 2014] é demonstrado que os padrões de busca por informações de usuários móveis são previsíveis o suficiente para permitir que um sistema de *cache* obtenha essas informações antes que seus usuários as solicitem. Em uma área de serviço predefinida, um dispositivo de Névoa pode prevê o aumento da demanda dos usuários por certas informações e efetuar o armazenamento em *cache* dos dados mais acessados de forma proativa em sua memória local. Além disso, essas informações podem ser distribuídas geograficamente entre outros nós de Névoa com base nos locais específicos próximos ou mais distantes na hierarquia. Tais informações podem ser recuperadas a partir da Nuvem, ou acessadas pelo seu proprietário na borda da rede.

6.3.1.4. Gerenciamento de Dados sobre Saúde

Muitas vezes, a vida dos pacientes dependem de ações em um intervalo de tempo extremamente curto. No apoio a tomada de decisão rápida e eficiente, dispositivos inteligentes vêm ajudando os médicos tanto nas decisões quanto no monitoramento da saúde dos pacientes. O paradigma em Nuvem permanece importante nesta área, onde [Shi et al. 2015] discute as características da computação e dos serviços em Névoa que podem fornecer benefícios em sistemas voltados à saúde.

Para as soluções baseadas em Nuvem esta tem sido uma questão naturalmente sensível, pois os dados sobre a saúde contêm informações valiosas e privadas. Entretanto, a computação em Névoa permite que os pacientes compartilhem e mantenham seus dados particulares de forma local e privada. Esses dados serão armazenados em nós de Névoa pessoais como celulares ou veículos inteligentes. O processamento desses dados (mas não os dados) será transferido de uma maneira autorizada para o dispositivo do paciente quando procurar ajuda de uma clínica médica ou um hospital. A alteração dos dados ocorre diretamente no dispositivo do paciente.

Em [Ahmad et al. 2016] é proposto um cenário sobre dados de saúde onde a computação em Névoa é usada como uma camada intermediária entre os usuários finais e a Nuvem para permitir maior controle e flexibilidade da privacidade dos clientes. Para isso, é introduzido um *Cloud Access Security Broker* (CASB) como componente integral da arquitetura, onde políticas de segurança podem ser aplicadas.

6.3.1.5. Segurança em Névoa

Não apenas na saúde, mas a segurança e integridade dos dados são duas características importantes e exigidas pela maioria das aplicações em IoT. Quanto mais tempo os dados

permanecem em "rota", mais vulneráveis eles se tornam para ataques, mesmo quando criptografados. Por isso, é sempre desejável ter pouco saltos entre clientes e servidores. A computação em Névoa pode oferecer a menor distância possível, proporcionando ainda vantagens da computação em Nuvem.

Mesmo sistemas de Nuvem localizados no interior da Internet podem sofrer ataques de disponibilidade através de métodos de Negação de Serviço (*Denial of Service*, DoS) [Sudha and Viswanathan 2013]. Esses tipos de ataques não precisam ser realizados diretamente sobre os próprios sistemas finais, uma vez que a desconfiguração dos dispositivos intermediários como roteadores podem ser igualmente fatais. Portanto, há muitas oportunidades para atingir sistemas de computação em Nuvem.

Por outro lado, os nós de Névoa são altamente distribuídos perto da borda da rede. Assim, para interferir completamente na disponibilidade destes sistemas é necessário um ataque em massa envolvendo todos os dispositivos que se encontram nas proximidades de um cliente. Isso exige métodos mais sofisticados e o emprego de mais recursos por parte dos atacantes do que em sistemas centralizados. Assim, é possível afirmar que de forma geral os sistemas de Computação em Névoa são menos propensos à ataques de negação de serviço do que os sistemas de computação em Nuvem.

A própria Névoa pode funcionar como um mecanismo de segurança, uma vez que outros mecanismos de proteção de dados existentes como criptografia podem falhar na prevenção de ataques, especialmente aqueles executados por invasores dentro de provedores. Em [Stolfo et al. 2012], é proposta uma abordagem diferente para a proteção de dados na Nuvem usando uma tecnologia ofensiva como armadilha (*decoy*). Nesta solução, o acesso aos dados na Nuvem é monitorado para detectar padrões de acesso anormais. Os acessos identificados como suspeitos são verificados através de perguntas contendo desafios. Caso não sejam respondidas corretamente, um ataque de desinformação é lançado sobre o invasor com o envio de grandes quantidades de informação *decoy*, protegendo os dados reais do usuário contra o acesso abusivo. Essa abordagem pode fornecer níveis sem precedentes de segurança para os dados dos usuários em um ambiente de Névoa.

6.3.1.6. Redes Inteligentes de Energia

Uma das mais avançadas aplicações de campo para Computação em Névoa reside nas Redes Inteligentes de Energia (*Smart Grids*), onde diferentes dispositivos como medidores e microcentrais de energia inteligentes são interconectadas através de uma rede de dados, como ilustrado na Figura 6.9. Neste contexto, aplicativos voltados ao balanceamento de carga de energia podem ser executados na borda da rede permitindo monitorar e controlar o consumo dos usuários ou alternar automaticamente entre energias alternativas de acordo com a demanda dos usuários, disponibilidade dos recursos e o menor preço.

Um algoritmo de gerenciamento de resposta à demanda centralizado em [Fadlullah et al. 2014] é implementado com uma abordagem de Computação em Nuvem, em que cada fornecedor e cliente se comunicam diretamente com a Nuvem. Porém, os algoritmos centralizados causam muito custo de largura de banda e gargalos, sendo inviáveis quando as redes reúnem um grande número de usuários [Jin et al. 2013]. Por outro lado, uma implementação totalmente distribuída onde cada usuário lida com seus próprios recursos e

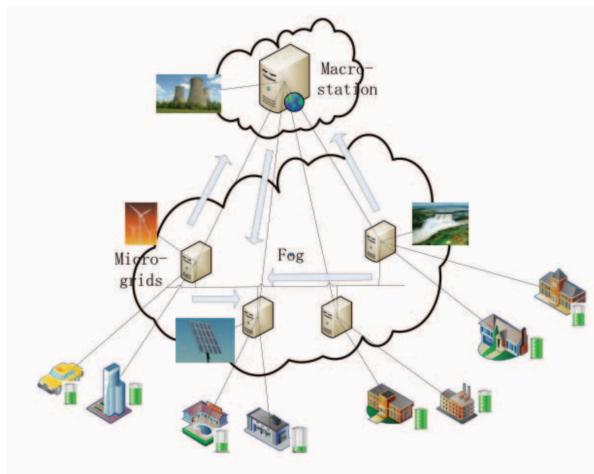


Figura 6.9. Computação em Névoa em Redes Inteligentes de Energia. Fonte: [Stojmenovic 2014a]

controla seu consumo através da consulta frequente do preço dos fornecedores de energia requer uma computação em cada extremidade, além de uma comunicação extensiva pela distância entre fornecedores e clientes.

Em [Wei et al. 2014] é descrita uma solução intermediária através de uma rede inteligente de energia descentralizada e que emprega o paradigma em Névoa para fornecer aplicações essenciais. Recentemente, esta tecnologia foi considerada promissora na integração das redes de energia convencionais com fontes alternativas de energia como parques eólicos, células solares, microturbinas, etc. Nessa arquitetura, componentes chamados *macro-grids* e *micro-grids* possuem funções equivalentes aos dispositivos de Névoa na redução da sobrecarga de comunicação.

Na solução de gerenciamento de resposta à demanda em [Wei et al. 2014], cada um dos *macro-grids* ou *micro-grids* podem atuar como dispositivo de Névoa considerando diferentes camadas. Por exemplo, a primeira camada é formada pela interação com base nas informações locais e nos parâmetros fornecidos entre os consumidores conectados ao mesmo dispositivo de Névoa. A segunda camada é formada pela interação com base nas informações globais fornecidas pelos dispositivos de Névoa conectados ao mesmo servidor de Nuvem. Os clientes se comunicam com os dispositivos de Névoa nas proximidades em vez da Nuvem remota, e os dispositivos de Névoa frequentemente se comunicam com os clientes e, ocasionalmente, com a Nuvem.

Além disso, os dispositivos de Névoa podem ser interconectados, onde as informações parciais disponíveis nesses dispositivos permitem a formação de coalizões eficazes para minimizar as perdas de energia e reduzir o custo de comunicação. As *macro-stations* coordenam a transferência de energia entre os *micro-grids* e entre cada *macro-grid* e *macro-station*. Para reduzir de forma otimizada as perdas totais na rede elétrica, um algoritmo de formação de coalizões gananciosos é proposto em [Wei et al. 2014]. O algoritmo otimiza as perdas de potência totais em toda a rede de energia, incluindo o custo de carregamento e descarregamento nos dispositivos de armazenamento, e as perdas devido

as transferências de energia. O algoritmo cria intercâmbio entre pares de *micro-stations* dando prioridade aos pares com maior redução de perdas por unidade de energia trocada.

Outro exemplo de aplicação do conceito de Névoa está no problema do agendamento *on-line* da demanda por carregamento de energia em uma grande frota de veículos elétricos, onde o objetivo consiste em não sobrecarregar as redes de energia. A solução em [Jin et al. 2013] é baseada na classificação dinâmica de veículos elétricos heterogêneos em múltiplos grupos, onde uma abordagem de janela deslizante é utilizada no agendamento em tempo real da demanda de carga dentro de cada grupo. Neste processo, a informação sobre a carga atual de cada veículo é obtida *on-line* com a ajuda da Névoa.

6.3.1.7. Redes de Veículos Conectados

Em [Bonomi 2011] é descrito um cenário de veículos conectados a semáforos e postes de iluminação inteligentes, equipados com câmeras, sensores e pontos de acesso ilustrado na Figura 6.10. A comunicação de veículo para veículo (*Vehicle-to-Vehicle*, V2V), de veículos para pontos de acesso (*Vehicle-to-Infrastructure*, V2I) e diretamente entre os pontos de acesso enriquecem esse cenário. Os semáforos são capazes detectar as luzes piscando de uma ambulância e alterar automaticamente a sinalização das ruas para permitir a passagem do veículo de forma mais rápida pelo tráfego. Os postes de iluminação interagem localmente com sensores para detectar a presença de pedestres e ciclistas, medindo a distância e a velocidade dos veículos que se aproximam. Os semáforos podem sincronizar uma "onda verde" entre as avenidas e enviar sinais de alerta para evitar acidentes.

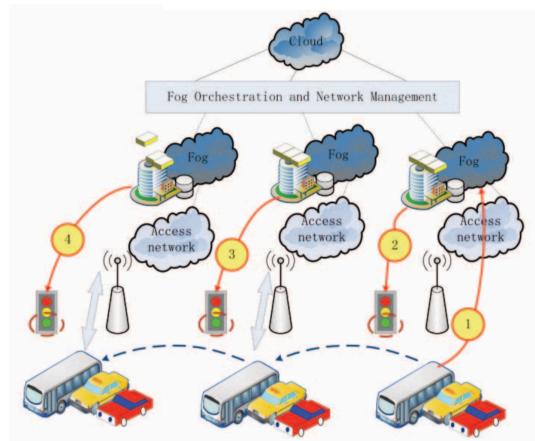


Figura 6.10. Cenário de veículos conectados. Fonte: [Stojmenovic 2014a]

A comunicação de dados em redes veiculares é usualmente realizada de forma descentralizada. Uma pesquisa mais extensa sobre métodos de encaminhamento e problemas em disseminação de dados nas redes veiculares *ad hoc* é apresentada em [Daraghmi et al. 2013]. Entretanto, o conceito de Névoa pode ser aplicado junto com SDN para tratar problemas fundamentais das redes veiculares como a conectividade intermitente, o grande número de colisões e alta taxa de perda de pacotes.

O conceito SDN em redes veiculares foi estudado e elaborado para o problema do *agendamento cooperativo de dados* em um ambiente de comunicação veicular híbrido descrito em [Liu et al. 2015]. No framework para redes veiculares proposto, os semáforos e as unidades inteligentes nas estradas funcionam como dispositivos de Névoa, assumindo a função dos roteadores no plano de dados SDN. O plano controle é implementado para monitorar e manter o estado individual dos veículos, otimizando o roteamento *multi-hop* nas redes V2V e V2I de uma forma logicamente centralizada.

A computação em Névoa pode fornecer um controle eficiente de semáforos em escala muito mais ampla do que as soluções existentes. Em [Zhou et al. 2011] um comando adaptativo de semáforos é empregado para maximizar o tráfego ao longo de pistas de mão única ou de mão dupla. Analisando o trajeto dos veículos, é possível diminuir o número de paradas e reduzir a emissão de gases do efeito estufa no ambiente. Em [Li and Shimamoto 2012] é proposta uma arquitetura em três camadas para calcular em tempo real a velocidade recomendada de veículos a partir da coleta de dados sobre o tráfego rodoviário utilizando: (i) dispositivos ETC (*Electronic Toll Collection*), (ii) antenas de rádio instaladas perto de semáforos e (iii) algoritmos para detecção de informações de tráfego com base em redes de sensores de proximidade [Zhang et al. 2013].

Uma solução baseada no paradigma em Névoa pode acomodar uma variedade de mecanismos para coleta de dados como etiquetas RFID em carros, sensores e câmeras de vídeo em semáforos, etc. As análises localizadas podem derivar informações de densidade de tráfego e fluxos em pontos específicos. Resumos dessas informações de tráfego devem ser encaminhados a partir dos dispositivos de Névoa para a Nuvem, possibilitando assim sua coordenação global. Mas os dispositivos de Névoa são tomadores de decisão e podem coordenar ações locais junto com seus vizinhos. Para suportar o controle centralizado, a disseminação de dados e a mobilidade entre os nós de Névoa é necessário que as informações sobre o estado dos veículos participantes sejam coletadas e migradas de forma eficiente. As informações sobre o estado dos veículos incluem sua localização em tempo real, velocidade, trajeto, capacidade de comunicação, etc.

6.3.1.8. Casas, Edifícios e Cidades Inteligentes

A aplicação da Internet das Coisas e Computação em Nuvem no desenvolvimento do conceito de Casas Inteligentes (*Smart Homes*) [Alam et al. 2012] tem aumentado nos últimos anos. Recentemente, grandes empresas têm oferecido seus primeiros dispositivos inteligentes e *gateways* voltados ao mercado pessoal. Entretanto, a sua adaptação ao cotidiano das casas é apenas o primeiro passo rumo a uma grande disseminação dessas tecnologias em outros ambientes ou cenários similares. Por exemplo, em [Nandyala and Kim 2016] é proposta uma arquitetura para o monitoramento de saúde usando as motivações e as vantagens da Computação em Névoa em casas inteligentes e hospitais.

Uma vez aprimoradas, estas tecnologias podem ser estendidas para ambientes mais amplos e complexos. Em [Stojmenovic 2014a] é descrito um cenário em Edifícios Inteligentes (*Smart Building*) onde o controle descentralizado pode ser facilitado por sensores sem fio implantados para fornecer a temperatura, a umidade, ou os níveis de vários gases na atmosfera do edifício. Além disso, os nós de Névoa podem trocar in-

formações com outros nós (por exemplo, no mesmo piso) para coordenar a combinação de leituras até alcançar medições confiáveis e realizar uma tomada de decisão distribuída para acionar outros dispositivos. Os componentes do sistema podem, então, trabalhar em conjunto para baixar a temperatura, injetar ar fresco, ou abrir janelas. Os condicionadores de ar podem remover a umidade do ar ou aumentar a umidade. Sensores também podem rastrear e reagir a movimentos (por exemplo, ligando e desligando a luz). Os dispositivos de Névoa distribuídos em cada andar podem colaborar em maior nível de atuação. Edifícios conectados podem manter a infraestrutura de seus ambientes externos e internos, para conservar energia, água e outros recursos.

Porém, a implantação de forma ubíqua de vários tipos de sensores em cenários futuristas e ainda mais abrangentes como em Cidades Inteligentes (*Smart Cities*) vai exigir uma complexa arquitetura em Névoa que suporte um grande número de componentes e serviços de infraestrutura para Internet das Coisas. Em verdade, todos as aplicações descritas nessa seção além de muitas outras que não foram citadas ou que ainda serão criadas devem ser integradas, gerenciadas e compartilhadas de forma global, sobre diferentes infraestruturas de comunicação e provedores de Névoa. Por exemplo, [Tang et al. 2015] propõe uma arquitetura em Névoa em larga escala como forma de garantir a segurança de grandes comunidades. Nessa abordagem, a integração de diferentes redes de sensores geograficamente distribuídas e o suporte a análise de grandes volumes de dados é necessária para identificar eventos anômalos e perigosos, oferecendo respostas em tempo real.

6.3.2. Plataformas para Computação em Névoa

As plataformas em Névoa são desenvolvidas aproveitando sua proximidade às fontes de dados para suportar características tais como apoio à mobilidade, reconhecimento de localidade e baixa latência [Bonomi et al. 2012]. Suas arquiteturas devem incluir requisitos presentes nas arquiteturas em Nuvem como escalabilidade, virtualização, orquestração e multi-arrendatário. Na próxima seção, discutiremos os diferentes componentes que podem ser incorporados em sua organização hierárquica para garantir a distribuição dos recursos e serviços. Os demais tópicos desta subseção apresentam exemplos de iniciativas que podem ajudar na implementação das aplicações apresentadas na Seção 6.3.1.

6.3.2.1. Arquiteturas de Plataformas em Névoa

Em [Yi et al. 2015a] é sugerida uma plataforma em Névoa constituída pelos componentes ilustrados na Figura 6.11, onde alguns componentes são semelhantes aos da arquitetura de referência ilustrada na Figura 6.7 e descrita na Seção 6.2.5. Neste ambiente, as funções de Gerenciamento de Rede com bilhões de dispositivos heterogêneos executando diferentes serviços é uma tarefa desafiadora. Esses elementos distribuídos precisam ser configurados e coordenados, onde algumas tecnologias têm evoluído para domar a complexidade envolvida [Vaquero and Rodero-Merino 2014]:

- *Técnicas de Rede Definida por Software (network softwarization)* - como a Névoa pode abranger infraestruturas gerenciadas por diferentes organizações, é necessário que seus serviços sejam executados de forma homogênea ou idealmente automatizada por software. O uso de técnicas de virtualização baseadas em NFV pelas

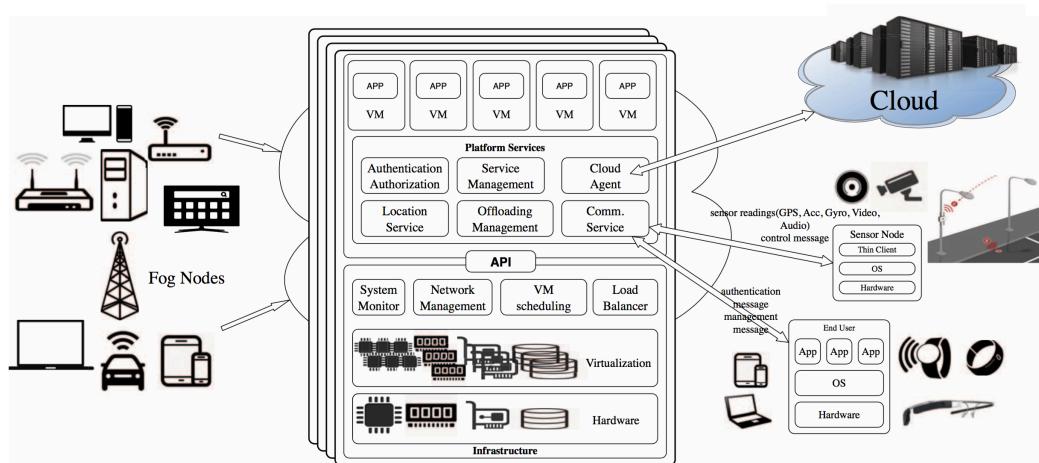


Figura 6.11. Componentes da Plataforma de Computação em Névoa. Fonte: [Yi et al. 2015a]

operadoras podem prover a implantação dinâmica de serviços sob demanda. O emprego de tecnologias baseadas em SDN permite que alguns serviços sejam estabelecidos apenas por software, resultando em operações mais ágeis e baratas do que soluções tradicionais baseadas em hardware. Por exemplo, a Figura 6.12 ilustra como os nós de Névoa podem ser implementados usando máquinas virtuais em uma Nuvem local na borda da rede móvel LTE (*Long Term Evolution*) e como seu tráfego no núcleo EPC (*Evolved Packet Core*) pode ser rigidamente controlado graças à recursos de SDN.

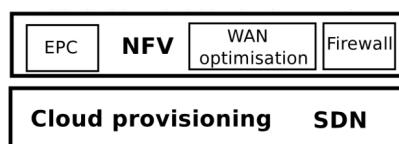


Figura 6.12. Uma Mini-Nuvem na borda da rede móvel implementada com SDN como base para NFV. Fonte: [Vaquero and Rodero-Merino 2014]

- *Técnicas Declarativas e Assintóticas* - voltadas ao gerenciamento em larga-escala, estas soluções permitem a especificação do estado desejado para o sistema de forma declarativa ao invés do uso de comandos de configuração individuais. Entretanto, é assumido que o estado final almejado pode não ser alcançado uma vez que o sistema é passível de modificações durante o processo de configuração. Por exemplo, problemas de conexão podem levar a saída de nós da rede. A Cisco propõe uma nova abordagem para SDN utilizando técnicas de controle declarativo para lidar com a escala e a complexidade do gerenciamento em [OpFlex 2014].
- *Nós de Névoa* - um subconjunto de elementos e dispositivos na Névoa podem se comportar como mini-nuvens, onde duas diferentes implementações são mostradas na ilustração abaixo. Na Figura 6.13 (a), uma arquitetura *Cloudlet* em três camadas:

a camada inferior executa uma plataforma Linux e mantém uma *cache* de dados local da Nuvem, a camada central oferece virtualização usando um conjunto de softwares como [Openstack 2015], e a camada superior executa aplicações de forma isolada em instâncias diferentes de Máquinas Virtuais (VM). Outra abordagem na Figura 6.13 (b) é proposta em [Cisco IOx 2014], onde o software IOS no roteador torna-se parte de uma infra-estrutura SDN para habilitar recursos NFV e serviços de aplicação próximo dos clientes na borda da rede. Embora IOx seja uma plataforma proprietária, acompanha uma distribuição Linux e permite a instalação de outros sistemas operacionais, a execução de *scripts* e a compilação de código.

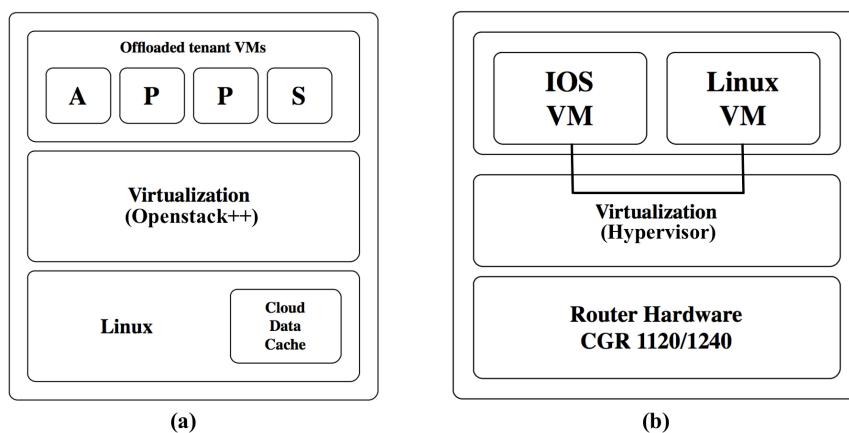


Figura 6.13. Arquitetura *Cloudlet* (a) e IOx (b) para nós de Névoa. Fonte: [Yi et al. 2015a]

- *Abordagens baseadas em Redes Peer-to-Peer (P2P) e de Sensores* - permitem uma cooperação entre os nós a fim de alcançar maior escalabilidade, porém com resultados similares às técnicas de gerenciamento que exigem um único provedor responsável pelo funcionamento da rede e dos serviços. Após anos de desenvolvimento e experimentação, as tecnologias P2P são suficientemente maduras para viabilizar a visão de Névoa explorando o conceito de localidade e eliminando a necessidade de um ponto de gerenciamento central. Recentemente, aplicações controversas como *Popcorn Time* [Idland et al. 2015] baseadas no protocolo *BitTorrent* [Shah and Pâris 2007] têm demonstrado o potencial das redes P2P para fornecer serviços globais em larga escala. Muitas das ideias usadas em Redes de Distribuição de Conteúdo (*Content Distribution Network*, CDN) são aplicáveis também à Névoa através da troca de dados entre pequenas nuvens para reduzir o fluxo desnecessário e indesejado de informações para servidores em centros de dados distantes dos clientes.

O Monitor do Sistema é um elemento padrão em infraestruturas de Nuvem e fornece informações úteis para outros componentes. Por exemplo, pode ser empregado em funções de gerenciamento relacionadas com o descobrimento, a alocação, o provisionamento e a manutenção de um conjunto de recursos de forma distribuída. Particularmente, é usado pelo Balanceamento de Carga para distribuir trabalhos entre múltiplos nós de Névoa de modo a permitir a redundância e aumentar a disponibilidade dos serviços.

O Escalonamento de Máquinas Virtuais é responsável pela distribuição das instâncias de VMs com aplicações e recursos em uma sequência lógica considerando o uso do sistema, as estatísticas de carga de trabalho, as informações de localização e o modelo de mobilidade. Diferentes estratégias de programação são necessárias na tentativa de fornecer uma solução ideal para o escalonamento.

Por meio de uma API bem definida, esse conjunto de componentes descritos acima colaboram no compartilhamento virtualizado da infraestrutura de hardware (dispositivos, canais, nós, servidores, etc.) usando uma Arquitetura Baseada em Serviços (*Service-Oriented Architecture*, SOA). Essa camada fornece as funcionalidades necessárias à implementação dos Serviços de Plataforma através dos seguintes componentes:

- Gerenciamento de Serviços - oferece as principais funções que permitem a descoberta dinâmica, a monitoração e a configuração dos serviços. Esta componente possibilita a implantação remota de novos serviços em tempo de execução a fim de satisfazer as necessidades das aplicações. Um repositório pode ser construído para identificar o catálogo de serviços associados com cada objeto na rede para facilitar a composição de outros serviços mais complexos. Além disso, podem incluir outras funções relacionadas, por exemplo, com a Qualidade de Serviço (QoS) ou com questões semânticas como o gerenciamento de contexto.
- Serviços de Comunicação - devem manter a interoperabilidade entre os níveis da plataforma envolvendo dispositivos inteligentes com sensores e atuadores, nós de Névoa e a Nuvem. Em relação aos dispositivos, deve oferecer suporte a diferentes padrões de apresentação para garantir que os dados sejam propagados pelas aplicações em diferentes tipos de sistemas. Da mesma forma, os Agentes específicos devem garantir a comunicação com diferentes provedores de Nuvem, resguardando as particularidades na operação sobre cada modelo de serviço oferecido.
- Mecanismos de Autenticação e Autorização - localizados próximos dos usuários finais, a computação em Névoa abre uma porta para novos esquemas de autenticação e autorização através do uso de padrões de acesso, padrões de mobilidade e dispositivos de segurança confiáveis. Um trabalho relacionado em [Dsouza et al. 2014] propôs um esquema de controle de acesso de recursos heterogêneos.
- O Gerenciamento de *offloading* - tem impacto geral sobre a plataforma e se encarrega da transferência de tarefas a partir dos dispositivos para a Névoa. Em [Yi et al. 2015b] há uma pesquisa sobre a computação *offloading* em Névoa onde se destaca três problemas principais: (i) quais informações são necessárias para decidir sobre *offloading*, (ii) como partitionar uma aplicação para *offloading* e (iii) como projetar um esquema de *offloading* ideal, considerando que o custo de transferência para Névoa pode ser superior ao tempo de processamento dos dados no próprio dispositivo.
- Serviços de Localização - precisam manter uma lista de localizações sobre os nós vizinhos (móveis ou não), rastrear os usuários móveis finais e compartilhar as informações de localização entre os nós de Névoa envolvidos. Também realiza o mapeamento de locais de rede com locais físicos além da adoção um modelo de

mobilidade que pode ser fornecido pelo usuário ou definido de forma autônoma. O rastreamento e o mapeamento dos nós móveis precisará obter informações em diferentes níveis de comunicação como da camada física e de hardware (endereço físico, GPS, sensor IMU, etc.), da camada de rede (endereço IP) e da camada de aplicação (atividades sociais).

6.3.2.2. Plataforma OpenFog

Em novembro de 2015, a criação do primeiro consórcio voltado ao desenvolvimento de uma infraestrutura padrão para Computação em Névoa reuniu grandes empresas do mercado mundial como Cisco, Microsoft, Intel e ARM, junto com a Universidade de Princeton em New Jersey, EUA. O consórcio baseia-se na premissa de que uma arquitetura aberta é essencial para o sucesso de um ecossistema ubíquo de Computação em Névoa para plataformas e aplicações voltadas à Internet das Coisas.

A plataforma OpenFog é projetada como uma extensão do modelo em Nuvem tradicional, onde implementações em sua arquitetura podem residir em múltiplas camadas da topologia de rede. O objetivo é facilitar a implantação de aplicações com requisitos de interoperabilidade, desempenho, segurança, escalabilidade, capacidade de programação, confiabilidade, disponibilidade, facilidade de manutenção e agilidade.

Sua arquitetura deve oferecer suporte a uma infinidade de clientes ou dispositivos de borda. Ela pode funcionar em conjunto com serviços de Nuvem para realizar armazenamento, computação, comunicação em rede e tarefas de gerenciamento otimizadas com base em requisitos de carga de trabalho. Neste sentido, deve oferecer uma infra-estrutura necessária para permitir a construção de serviços *Fog-as-a-Service* (FaaS) visando tratar desafios em negócios. A infraestrutura e os componentes da arquitetura abaixo mostram como FaaS pode ser expandido sobre a arquitetura de referência.

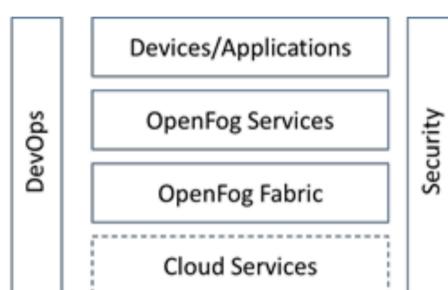


Figura 6.14. Visão da Infra-estrutura OpenFog. Fonte: [OpenFog 2016]

- *Serviços de Nuvem* - disponibilizam a infraestrutura em Nuvem para tarefas computacionais que precisam operar em um escopo mais amplo de informações ou sobre dados de borda pré-processados para estabelecer políticas. Estes devem ser usufruídos de forma a não impedir sua autonomia operacional.

- *Infraestrutura OpenFog* - é composto por componentes que permitem a construção de uma infraestrutura computacional homogênea em que serviços úteis podem ser entregues aos ecossistemas agregados (por exemplo, dispositivos, *gateways* de protocolo e outros nós de Névoa). A infraestrutura homogênea é geralmente construída sobre hardware heterogêneo e plataformas desenvolvidas por vários fornecedores.
- *Serviços OpenFog* - são construídos sobre a infraestrutura OpenFog como uma arquitetura de microserviços em Névoa. Estes serviços podem incluir aceleração de rede, NFV, SDN, entrega de conteúdo, gerenciamento de dispositivos, gerenciamento de topologia, processamento de eventos complexos, codificação de vídeo, *gateways* de protocolo, tráfego de *offloading*, *cache* de dados, criptografia, compressão, plataforma e algoritmos de análise, etc.
- *Dispositivos/Aplicações* - são sensores, atuadores e aplicativos em execução autônoma, dentro de uma infraestrutura de Névoa ou abrangendo diferentes provedores.
- *Segurança* - encapsulam as funcionalidades dentro de cada camada da arquitetura com mecanismos de controle de acesso para que a plataforma em Névoa e os ecossistemas agregados possam operar em um ambiente seguro, garantindo as transferências de dados entre seus componentes.
- *DevOps* - com foco em automação, são habilitados por um conjunto padronizado de procedimentos e *frameworks*. Fornecem agilidade para correções ou atualizações de software através de uma integração contínua e controlada.

Alguns temas recorrentes que aparecem no desenvolvimento de OpenFog representam os pilares da sua arquitetura. O emprego correto de cada um desses pilares como base para plataforma é a chave para uma implementação bem sucedida.

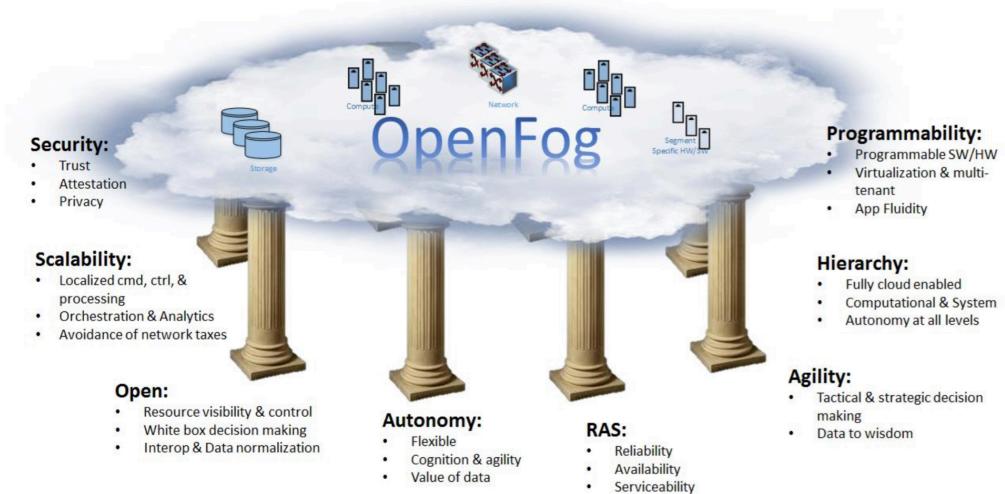


Figura 6.15. Pilares da plataforma OpenFog. Fonte: [OpenFog 2016]

6.4. Desafios para a Computação em Névoa

Neste tópico, vamos identificar e discutir potenciais desafios no contexto da Computação em Névoa, onde alguns deles podem indicar a direção para trabalhos futuros nesta área. Os desafios atuais serão introduzidos através da análise das soluções vigentes e dos problemas que envolvem a integração entre os paradigmas de Nuvem e Névoa.

A fim de levantar os desafios relacionados à integração dessas tecnologias, será feito um paralelo entre os requisitos não atendidos pela computação em Nuvem, e como estes poderiam ser atendidos pela computação em Névoa. As redes de nevoeiro podem contornar os problemas para criar um ambiente mais flexível e confiável.

A seguir serão abordadas as questões envolvendo os modelos de programação e comunicação na Névoa, como os dispositivos envolvidos se comunicam e os problemas relacionados. A necessidade de gerenciamento de recursos e os principais desafios associados com a segurança, integridade e como prover privacidade nestes ambientes. Além das dificuldades em prover qualidade de serviço, implicando nas características de conectividade, confiabilidade, capacidade de processamento e armazenamento e atraso. Outros pontos a serem discutidos é um modelo de negócio sustentável, o impacto do consumo de energia e a necessidade de padronização para a Névoa.

6.4.1. Modelos de Programação

A transferência das tarefas de processamento para fora dos dispositivos ou *offloading* tem sido uma área de pesquisa ativa no domínio da computação móvel. Os dispositivos móveis que possuem restrições de recursos podem se beneficiar deste paradigma no desempenho de suas aplicações, com economia de armazenamento e tempo de bateria [Yi et al. 2015b]. No entanto, esta carga de trabalho é transferida para a Nuvem, que nem sempre é possível ou razoável de realizá-la devido às limitações e restrições que podem ser impostas [Dastjerdi et al. 2016].

Para tratar o problema do *offloading* [Orsini et al. 2015] propõem um *framework* adaptativo para Computação em Névoa chamado *CloudAware*, o qual destina tarefas de processamento tanto para a Nuvem quanto para os dispositivos localizados na borda da rede, ou seja, a Névoa. O *CloudAware* foi projetado com o objetivo de dar suporte às interações *ad-hoc* com baixa latência. Assim, visa facilitar o desenvolvimento de aplicações móveis e escaláveis, contribuindo para acelerar a computação com economia de energia e de largura de banda em diversos cenários de mobilidade dos usuários.

De acordo com [Yi et al. 2015b] o principal desafio de *offloading* na Computação em Névoa é como tratar com a dinamicidade do sistema. Pois, devemos levar em consideração que o acesso às redes *wireless/radio*, os nós e os recursos de Névoa são altamente dinâmicos. O processamento das tarefas fora dos dispositivos nesta infraestrutura está diante de novos desafios e oportunidades, tais como: *i*) definir a granularidade das tarefas a serem processadas, em diferentes hierarquias da Computação em Névoa e Computação em Nuvem; *ii*) particionar a aplicação dinamicamente para processamento das tarefas em Névoa e em Nuvem; e, *iii*) tomar decisões para adaptar o processamento das tarefas diante das mudanças acarretadas pela dinamicidade da rede, dos dispositivos de Névoa e dos recursos, etc. Além disso, [Orsini et al. 2015] acrescentam a necessidade de replicação e

gerenciamento das aplicações em um ambiente não confiável e dinâmico.

É necessário unificar modelos de interfaceamento e programação para facilitar aos desenvolvedores a portabilidade de suas aplicações para Computação em Névoa. Isto se dá pelas seguintes razões: *i*) o modelo de computação centrado na aplicação será importante visto que permitirá otimizações para diferentes tipos de aplicação e seus componentes serão conscientes da aplicação; *ii*) é difícil para os desenvolvedores orquestrar recursos dinâmicos, hierárquicos e heterogêneos para construir aplicações compatíveis em diversas plataformas [Yi et al. 2015c].

[Hong et al. 2013a] apresentam uma API denominada *Mobile Fog* para o desenvolvimento de aplicações futurísticas que visa potencializar a larga escala, a distribuição geográfica e a garantia de baixa latência fornecida por uma infraestrutura em Névoa. A aplicação construída baseada na API *Mobile Fog* possui diversos componentes, cada um rodando em diferentes níveis na hierarquia dos dispositivos, semelhante a arquitetura de referência apresentada na seção 6.2.5. No entanto, ainda é necessário modelos mais gerais para diversas redes onde os nós da Névoa são nós móveis dinâmicos [Yi et al. 2015c].

6.4.2. Comunicação

Os aspectos relacionados à comunicação são desafiantes para os novos paradigmas de computação que tem surgido. É essencial para a sobrevivência dos sistemas e o funcionamento adequado das aplicações, principalmente, as que possuem sensibilidade à atrasos e requerem respostas em tempo real. Na Computação em Névoa, o dispositivo servidor é um componente intermediário da rede que se conecta com os usuários móveis, outros servidores de Névoa e a Nuvem. O servidor de Névoa pode monitorar o comportamento da rede e adaptar as aplicações de acordo com o ambiente [Luan et al. 2016].

[Suryawanshi and Mandlik 2015] e [Luan et al. 2016] afirmam que as pesquisas em comunicação devem levar em consideração como os componentes do sistema interagem. A seguir serão descritos os problemas associados e possíveis soluções envolvendo a comunicação, diante de três aspectos: *i*) dispositivos móveis e a Névoa; *ii*) a Névoa e a Nuvem; e, *iii*) entre as Névoas.

Comunicação entre os dispositivos móveis e a Névoa: ocorre diretamente entre os dispositivos móveis e os servidores de Névoa, através de conexões sem fio de único passo, tais como, WiFi, celular ou *bluetooth* [Luan et al. 2016]. Os servidores de Névoa possuem armazenamento limitado e entrega restrita de serviços localizados. Determinar os serviços de aplicação que ocasionam as menores taxas de faltas para os usuários móveis e selecionar os conteúdos para *cache* em cada servidor de Névoa devem ser temas de estudo. Para solucionar este problema é necessário prever os padrões de requisição de serviços dos usuários, a capacidade de armazenamento disponível e o poder de computação do servidor de Névoa. Como os servidores de Névoa são localizados em regiões específicas, os usuários apresentam características previsíveis na demanda de serviços. A Computação em Névoa também pode ser incorporada com a tecnologia de redes de celular 5G que está emergindo para prover maior cobertura e serviços dedicados.

Comunicação entre a Névoa e a Nuvem: se dá através de conexões sem fio e ca-

beada. A Nuvem é o depósito central de informações e o controlador central dos servidores de Névoa instalados em diferentes localizações. Os servidores de Névoa, localizados em diferentes regiões, podem selecionar os conteúdos da Nuvem e entregar cópias destas informações, a partir de sua *cache*, para os usuários móveis em localizações específicas. O servidor da Nuvem gerencia as aplicações e conteúdos para todo o sistema. Para isso, torna-se necessário tratar a confiabilidade e o controle escalável dos servidores de Névoa na Nuvem e desenvolver esquemas de roteamento de dados escaláveis. A entrega e atualização dos dados da Nuvem para a Névoa pode ser realizada através de SDN. Assim, o mecanismo de roteamento é separado entre o plano de controle e o plano de dados, onde a Nuvem gerencia a rede a partir de uma visão global para estabelecer os caminhos de roteamento dos dados e atualizar os servidores de Névoa distribuídos geograficamente.

Comunicação entre as Névoas: pode ser estabelecida através de conexões sem fio e cabeada. Os servidores de Névoa, localizados em distâncias próximas, podem pertencer a diferentes proprietários e oferecer serviços para usuários móveis similares. Os servidores de Névoa precisam colaborar para entrega de um serviço comum. A colaboração eficiente entre estes servidores, localizados em uma região próxima, pode aliviar o tráfego entre a Nuvem e a Névoa, melhorando o desempenho do sistema com economia de largura de banda e melhoria da taxa de dados. O roteamento entre os nós na Névoa pode ser realizado por dois modos: *i*) centralizado, através de uma abordagem baseada em SDN; e, *ii*) distribuído, através dos mecanismos tradicionais de roteamento, como por exemplo, OSPF (*Open Shortest Path First*).

A transmissão de dados entre os servidores de Névoa é desafiante pelas seguintes questões: *i*) *política de serviço*, os servidores de Névoa em diferentes localizações podem ser empregados por diversas entidades para usos comerciais distintos. Deste modo, podem apresentar heterogeneidade em suas políticas de serviços; *ii*) *topologia*, servidores de Névoa localizados em uma mesma região podem ser conectados à Internet através do mesmo Provedor de Serviços com alta taxa de conexão e baixo custo. Isso permite a colaboração eficiente entre os servidores próximos na Névoa buscando melhor desempenho do sistema, economia do custo associado à largura de banda e melhoria da taxa de dados. *iii) conexões*, o roteamento dos dados entre os servidores de Névoa precisam considerar as características destas conexões. Além de conexões cabeadas, podem ser estabelecidas conexões *wireless* oportunísticas, como por exemplo, em um sistema de veículos conectados em Névoa, onde os conteúdos são enviados entre os servidores de Névoa por contato veicular oportunístico [Luan et al. 2016].

6.4.3. Gerenciamento de Recursos

Geralmente, a Névoa é composta de dispositivos de diferentes tipos, os quais possuem capacidade de rede, poder de armazenamento e computação. Diante das suas especificidades, ainda é difícil para estes dispositivos corresponderem à capacidade de recursos dos tradicionais servidores, como ocorre na Computação em Nuvem.

A implantação de servidores de Névoa em diferentes localizações implica que o operador da rede precisa adaptar seus serviços. A aplicação instalada em cada servidor de Névoa precisa ser customizada baseada em sua demanda local. É necessário antecipar a

demandas de cada um dos servidores de Névoa a fim de empregar recursos de forma adequada, não prejudicando a escalabilidade do sistema. Frente às diferentes demandas de usuários em diferentes localizações, um grupo de servidores de Névoa podem colaborar para fornecer serviço aos usuários móveis próximos. No entanto, é preciso otimizar localmente o uso dos servidores de Névoa [Luan et al. 2016]. Deste modo, um gerenciamento de recurso eficiente é essencial para os ambientes de Computação em Névoa.

[Aazam and Huh 2015] apresenta um modelo de gerenciamento de recursos orientado a serviços que prevê o uso dos recursos pelos clientes e pré-aloca os recursos baseado no comportamento do usuário e a probabilidade de usá-los no futuro. Deste modo, a previsão permite maior justiça e eficiência quando os recursos são consumidos. Em [Lewis et al. 2014] é proposto um mecanismo de provisionamento de recursos para *cloudlets* táticas, onde as aplicações são particionadas para executar de modo leve nos clientes, que rodam nos dispositivos móveis, e a computação intensiva é realizada nos servidores. Uma estratégia para fornecer infraestrutura para suportar computação *offloading* e plataforma de dados em dispositivos na borda da rede. *Cloudlets* se refere ao cenário em que o dispositivo de Névoa fornece infraestrutura para processar tarefas de outros dispositivos.

O gerenciamento de rede em Névoa é essencial para o oferecimento dos serviços de modo eficiente. Entretanto, oferecer serviços em cenários de larga escala, como ocorre em IoT, não é uma tarefa simples. [Yi et al. 2015b] sugere o uso de tecnologias que estão emergindo, como SDN e NFV. Estas tecnologias são propostas para criar ambientes de redes mais flexíveis e de fácil manutenção. O emprego de SDN e NFV na Computação em Névoa pode facilitar a implementação e o gerenciamento, aumentar a escalabilidade da rede e reduzir custos, tais como: alocação de recursos, migração de VM, monitoramento de tráfego, controle de aplicações cientes de contexto e interfaces programáveis.

6.4.4. Modelo de Negócio

A Computação em Névoa precisa de um modelo de negócio sustentável para manter-se funcionando de maneira adequada. De acordo com pesquisas realizadas, [Yi et al. 2015b] estabelece que os fornecedores de recursos da Névoa podem ser: *i*) fornecedores de serviços Internet ou suporte *wireless*, que podem construir a Névoa em suas infraestruturas; *ii*) fornecedores de serviço da Nuvem, que desejam expandir seu serviço centralizado da Nuvem para a borda da rede; *iii*) usuários fin, que desejam negociar sua computação extra, armazenamento de sua Nuvem privada local para reduzir os seus custos.

Entretanto, o modelo de negócio ainda não foi estabelecido, para isso é necessário resolver algumas questões, como por exemplo, em termos de faturamento, como se dará o preço dos diferentes recursos e qual será a fração de valor paga aos diferentes proprietários da Névoa. Para reforçar estas questões de política de preços torna necessário a contabilidade e o monitoramento da Névoa em diferentes granularidades, como ocorre no uso de serviços tradicionais.

Um modelo de negócio interessante para acelerar o uso da Computação em Névoa é o modelo baseado em incentivos aos usuários. Os proprietários de Nuvens privadas locais, localizadas na borda da rede, podem fornecer seus serviços para a Névoa, com capacidade de computação e armazenamento. A partir da perspectiva técnica de Computação na Nuvem e virtualização, o fornecedor de serviço para Névoa pode arrendar o seu

poder de computação e armazenamento ocioso e receber pagamento para reduzir os seus próprios custos [Yi et al. 2015b].

6.4.5. Segurança, Integridade e Privacidade

A Computação em Nuvem enfrenta problemas de segurança que podem ser estendidos para Névoa. Além disso, são adicionados desafios de segurança ao ambiente de Computação em Névoa por sua localização e natureza descentralizada, instalados em locais sem proteção e o devido rigor na vigilância [Dastjerdi et al. 2016]. Os ataques empregados na Computação em Névoa podem comprometer a disponibilidade do sistema e usuários maliciosos podem praticar espionagem e sequestro de dados [Stojmenovic et al. 2015].

Detecção de intrusos. Os mecanismos usados para proteção de dados, como a encriptação, tem falhado em prevenir ataques de roubos de dados, principalmente quando executados internamente no provedor de serviço da Nuvem [Stolfo et al. 2012]. Considerando a Névoa como uma pequena Nuvem, podemos aplicar técnicas de detecção de intrusos [Modi et al. 2013]. Segundo [Stojmenovic et al. 2015], a intrusão nestes ambientes pode ser detectada através do uso de método baseado em assinatura e método baseado em anomalias. No método baseado em assinatura, os padrões de comportamento do usuário são observados e checados com um banco de dados existente de possíveis maus comportamentos. No método baseado em anomalias, o comportamento observado é comparado com o comportamento esperado para verificar se há desvios.

Em [Stolfo et al. 2012], os autores propõem uma abordagem para prover segurança aos dados na Nuvem através da análise do perfil de comportamento do usuário e o uso ofensivo da tecnologia *decoy*. Os dados são monitorados continuamente para detectar padrões de acesso anormais, decorrentes do perfil de comportamento do usuário. Quando um acesso é considerado suspeito, constatado através de perguntas de desafio, é lançado um ataque de desinformação, retornando grandes quantidades de informações *decoy* para o atacante. Assim, protege os dados do usuário do uso indevido. O ambiente de Névoa é utilizado para disparar armadilhas, arquivos *decoy*, quando um ataque é detectado. Deste modo, não causa interferência nas atividades normais dos usuários.

[Stojmenovic et al. 2015] expuseram os problemas de segurança em Névoa a partir de estudos sobre um típico ataque de homem do meio. Nos experimentos realizados, os *gateways* que servem como dispositivos de Névoa foram comprometidos. Os usuários da Névoa se conectam a pontos de acesso falsos que fornecem serviços enganosos como legítimos. O cenário estabelecido é uma comunicação por vídeo chamada, no qual o usuário utiliza a tecnologia 3G para enviar dados para um usuário na WLAN.

Uma vez que o atacante toma o controle do *gateway*, a comunicação privada das vítimas pode ser sequestrada. O atacante pode retransmitir ou modificar os dados em seu próprio computador e enviá-los para o *gateway*. Assim, o *gateway* transmite os dados do atacante para o usuário na WLAN. O experimento teve como objetivo avaliar as características deste ataque através da análise do consumo de CPU e memória. A partir dos experimentos, concluiu-se que o ataque homem do meio em Névoa pode não ser identificado, visto que o consumo de memória e CPU é desprezível. Os autores concluem que o ataque homem do meio é difícil de evitar e defender, tendo potencial para se tornar um típico ataque na Computação em Névoa.

Modelo de Confiança. A Névoa pode ter diferentes provedores, o que dependerá do modelo de negócio implementado, conforme descrito na seção 6.4.4. No entanto, a flexibilidade existente compromete a confiança da Névoa. Um nó de Névoa pode agir como trapaceiro e influenciar outros nós a se conectarem a ele. Uma vez conectados, os nós trapaceiros podem manipular as requisições dos usuários fins ou da Nuvem, coletar ou até mesmo adulterar os dados para lançar novos ataques. Modelos de confiança baseados em reputação tem sido amplamente empregados em P2P, comércio eletrônico e redes sociais online. Segundo [Yi et al. 2015c], o projeto de um sistema de reputação para Computação em Névoa precisa levar em consideração as seguintes questões: *i*) como alcançar identidades persistentes, únicas e distintas; *ii*) como tratar ataques intencionais e acidentais; e, *iii*) como punir e resgatar a reputação dos nós. A existência de nós trapaceiros será uma grande ameaça para a segurança e privacidade dos dados. Este problema é difícil para tratar em ambientes de Névoa por conta dos diferentes esquemas de gerenciamento de confiança e da dinamicidade do sistema, que torna difícil a manutenção de uma lista com os nós desonestos.

Autenticação. [Stojmenovic and Wen 2014] consideram que o principal desafio da segurança na Computação em Névoa é a autenticação, em vários níveis dos nós. O uso de Infraestrutura de Chave Pública (PKI - *Public Key Infrastructure*) pode solucionar este problema [Chen et al. 2014]. No entanto, [Yi et al. 2015c] afirmam que as autenticações baseadas nas tradicionais PKI não são eficientes e não são escaláveis. Em [Stojmenovic et al. 2015] é proposto um tipo de autenticação chamada *Stand-Alone Authentication* que é capaz de autenticar o usuário mesmo quando não há conexão com o servidor da Nuvem. O direito de autenticação é delegado pelo Servidor de Autenticação para um dispositivo de Névoa. Esta abordagem é baseada em uma encriptação híbrida, no uso do Padrão de Criptografia Avançado (AES - *Advanced Encryption Standard*) e de *smart card*.

Técnicas de execução em ambiente confiáveis (*Trusted Executed Environment*, TEE) são propostas como uma potencial solução para os problemas relacionados à autenticação em Computação na Névoa [Marforio et al. 2014]. Métodos baseado em cálculo de influência podem ser usados para detectar nós de Névoa trapaceiros ou desqualificados e, assim, reduzir o custo com a autenticação [Han et al. 2011] [Behrisch et al. 2011]. As tecnologias emergentes de autenticação baseadas em biometria para dispositivos móveis e Nuvem irão beneficiar a Computação em Névoa [Yi et al. 2015c].

Controle de Acesso. O controle de acesso tem sido uma ferramenta confiável para garantir a segurança em sistemas que envolvem dispositivos inteligentes e Nuvem [Yi et al. 2015b]. Em virtude da natureza da Computação em Nuvem estar relacionada com a prestação de serviços, o controle de acesso é usualmente implementado através de criptografia [Yi et al. 2015c]. [Yu et al. 2010] apresenta um controle de acesso de dados baseado em fina granularidade, através da exploração de técnicas de encriptação baseadas em atributos (*Attribute-Based Encryption*, ABE). Em [Dsouza et al. 2014] é proposto um controle de acesso baseado em políticas para Computação em Névoa. Neste trabalho, foram identificados os desafios existentes em políticas de gerenciamento para Computação em Névoa que tornam críticos o suporte ao compartilhamento seguro, a colaboração e reuso de dados em ambientes heterogêneos. O *framework* apresentado visa o gerenciamento de políticas acompanhado com critérios de políticas e esquemas relevantes. Os autores demonstram a viabilidade e aplicabilidade da proposta através de cenários de caso

de uso em sistemas de transporte inteligente que requer análise e agregação de dados em tempo real e transmissão dinâmica de informações entre os dispositivos que fazem parte dos sistemas. Durante a colaboração e compartilhamento de dados podem surgir conflitos e problemas, os quais podem ser tratados dinamicamente pelo *framework* enquanto ocorre a transferência de informações de forma segura para o destino final.

Integridade. Diversas aplicações na Internet demandam por segurança e integridade [Zao et al. 2014]. Se os dados permanecem em rota por mais tempo, mais vulneráveis eles estão aos ataques, mesmo quando encriptados. Assim, sempre é desejável ter poucos passos entre os clientes e os servidores. A Computação em Névoa fornece a menor distância possível agregando outras vantagens da Nuvem. Deste modo, a Computação em Névoa é preferível à Computação em Nuvem em muitas situações [Firdhous et al. 2014].

Privacidade. De modo geral, os usuários da Internet estão preocupados com o risco da falta de privacidade. Mecanismos que preservam a privacidade tem sido proposto em diversos cenários, como por exemplo, Nuvem, redes sem fio, redes sociais, entre outros. A preocupação dos usuários não é diferente nos ambientes de Computação em Névoa, principalmente, por conta da natureza deste ambientes, onde os dados dos usuários podem ser processados em *hardwares* e *softwares* de outros proprietários. Com isto, introduz preocupações sobre a privacidade dos dados e sua visibilidade por partes não autorizadas. Por esta razão precisamos investigar técnicas e mecanismos para assegurar a confiança entre as partes que estão cooperando [Suryawanshi and Mandlik 2015]. Na Névoa, os algoritmos utilizados para preservar a privacidade podem ser executados entre a Névoa e a Nuvem, desde que os recursos de computação e armazenamento sejam suficientes para ambos, o que nem sempre é possível nos dispositivos fins. No entanto, técnicas como encriptação homomórfica podem ser usadas para permitir privacidade durante a agregação dos dados nos *gateways* locais sem decriptação [Yi et al. 2015b].

6.4.6. Qualidade de Serviço

A qualidade de serviço é uma métrica importante para o provimento de serviços através da Névoa. [Yi et al. 2015b] analisa a qualidade de serviço da Computação em Névoa sob quatro aspectos: conectividade, confiabilidade, capacidade e atraso. Cada um destes aspectos serão descritos a seguir:

Conectividade. O ambiente de Névoa envolve dispositivos heterogêneos com capacidade de expandir a conectividade da rede. A retransmissão na rede, particionamento e agrupamento fornece novas oportunidades para reduzir custos. A seleção de nós de Névoa pelos usuários terá um grande impacto no desempenho do sistema. Para otimizar o desempenho e disponibilidade dos serviços de Névoa, pode-se selecionar dinamicamente um subconjunto de nós de Névoa como retransmitidores para uma determinada área ou usuário, com restrições de atrasos, largura de banda, conectividade e consumo de energia.

Confiabilidade. É uma das primeiras preocupações quando projetamos sistemas de Computação em Névoa, onde há integração de um grande número de dispositivos distribuídos geograficamente. Segundo [Madsen et al. 2013], para termos uma Névoa confiável é essencial levarmos em consideração as falhas que podem ocorrer, tais como: *i*) os dispositivos podem falhar individualmente; *ii*) falhas na rede e falta de cobertura de rede em algumas regiões; *iii*) falhas na plataforma de serviço; e, *iv*) falhas na interface do

usuário conectado ao sistema. Normalmente, a confiabilidade pode ser melhorada através de *check-pointing* periódicos para recuperação após as falhas ocorrerem, reescalonamento das tarefas falhas ou replicação para explorar as execuções em paralelo. No entanto, em um ambiente altamente dinâmico como uma Névoa, pode não ser possível a recuperação e o reescalonamento. Caso houvesse, introduziria latência e não poderia adaptar-se às mudanças. A replicação pode ser usada em vários nós de Névoa, que devem cooperar para melhorar o desempenho do sistema.

Capacidade. Possui dois aspectos: largura de banda e capacidade de armazenamento. Para alcançar altas taxas de largura de banda e armazenamento deve-se analisar como os dados são distribuídos nos nós da Névoa, considerando a sua localização. Trabalhos foram desenvolvidos na área de Nuvem e de redes de sensores. Estes problemas estão diante de novos desafios na Computação em Névoa que vêm desde o projeto, na interação entre a Névoa e a Nuvem e em como acomodar diferentes cargas de trabalho. Além dos problemas relacionados à busca de conteúdos dispersos nos nós da Névoa devido a dinâmica da localização dos dados e grande capacidade total de volume. A economia de largura de banda e redução de atrasos pode ser obtida pelo uso de *cache* nos nós da Névoa, sendo interessante reprojetar a *cache* para explorar localidade temporal e ampla cobertura no ambiente de Névoa.

Atraso. Algumas aplicações precisam da Computação na Névoa para fornecer processamento de *streaming* em tempo real. Estas aplicações são sensíveis à latência. Para satisfazer as exigências de latência das aplicações, [Hong et al. 2013b] propõe um sistema de processamento de evento espaço temporal oportunístico que usa tratamento de requisições continuamente baseado em predição. O sistema prediz futuras requisições em uma região para usuários em movimento e antecipam o processamento de eventos para tornar as informações disponíveis quando os usuários alcançarem a localização. Após avaliação, o sistema proposto alcançou resultados significativos, com latência próxima de zero em vários casos. Em [Ottenwälter et al. 2014] é apresentado o RECEP, um sistema para aumentar a escalabilidade dos sistemas móveis que exigem o processamento de eventos complexos (*Complex Event Processing*, CEP) e a agregação de dados de sistemas distribuídos em tempo real. O RECEP explora a sobreposição de interesses dos usuários móveis através de métodos que utilizam o processamento de maneira eficiente para reduzir a requisição de recursos.

6.4.7. Consumo de energia

Os ambientes de Névoa são formados por um grande número de dispositivos distribuídos geograficamente, tendo a computação distribuída como principal aspecto. Levando em consideração a natureza dos ambientes em Névoa, estes podem ser menos eficientes em energia do que os ambientes centralizados em Nuvem. Deste modo, a redução do consumo de energia em ambientes de Névoa se torna um desafio [Dastjerdi et al. 2016].

Em [Deng et al. 2015] é apresentado um estudo sobre o *trade-off* entre o poder de consumo e o atraso em sistemas de Computação em Nuvem e Névoa. Os autores formalizaram matematicamente o problema de alocação da carga de trabalho entre a Névoa e a Nuvem. Decomporam o problema principal em três subproblemas: *i*) *trade-off* entre o poder de consumo e o atraso em Computação na Névoa; *ii*) *trade-off* entre o poder de con-

sumo e o atraso em Computação na Nuvem; e, *iii*) minimização do atraso de comunicação no envio, através do subsistema WAN (*Wide Area Network*), durante a transmissão dos dados da Névoa para Nuvem. Através de simulações e resultados numéricos foi possível mostrar que a Computação em Névoa pode melhorar significativamente o desempenho da Nuvem através da economia de largura de banda e redução na latência de comunicação. Os autores concluem que os subproblemas podem ser solucionados independentemente através de técnicas de otimização, dentro do seu subsistema correspondente.

6.4.8. Padronização

Os mecanismos de padronização se tornam necessários para que cada membro da rede (terminal, dispositivos na borda da rede, etc.) possa interagir e cooperar. Os protocolos são necessários para que os membros da rede anunciem sua disponibilidade para hospedar componentes de *software* de terceiros e para que outros usuários possam enviar suas tarefas para serem executadas. Deste modo, é fundamental o desenvolvimento de padrões de protocolos, arquiteturas e APIs para facilitar a interconexão entre objetos inteligentes heterogêneos e a criação de serviços aprimorados que possam satisfazer as necessidades dos usuários [Suryawanshi and Mandlik 2015].

6.5. Considerações Finais

A Computação em Névoa é construída pela convergência de um conjunto de tecnologias que atravessaram processos de desenvolvimento e amadurecimento independentes. A integração destas tecnologias em um cenário único busca responder às novas exigências introduzidas pela ubiquidade dos dispositivos, requerendo mais agilidade das redes de comunicação e do gerenciamento de serviços em Nuvem, além de mecanismos extensíveis para privacidade dos dados.

De forma geral, uma infraestrutura em Névoa oferece às tecnologias de Nuvem mecanismos para lidar com o imenso volume de dados gerados diariamente pela Internet das Coisas. O processamento mais próximo de onde os dados são produzidos é a forma mais adequada de resolver os desafios atuais relacionados a sua explosão em volume, variedade e velocidade. As tecnologias de Névoa também podem acelerar a consciência e a resposta à eventos, eliminando requisições e transferências custosas de dados da borda da rede para o centro da Nuvem. Também protege informações sensíveis e valiosas extraídas da Internet das Coisas, analisando os dados dentro dos muros das empresas e organizações. Como resultado, a Névoa vai mudar dramaticamente muitas das práticas atuais em quase todas as camadas das arquiteturas de Nuvem, no suporte ao desenvolvimento de aplicações, no gerenciamento de recursos e serviços, contabilidade, colaboração, etc.

A Computação em Névoa vai dar origem a novas formas de competição e cooperação entre os provedores na Internet. Entretanto, não é fácil determinar como os diferentes atores no mercado irão se alinhar para oferecer serviços em Névoa de forma global nos próximos anos. É previsto que novos protagonistas entrarão em cena no papel de usuários ou provedores. As organizações que adotarem a Computação em Névoa devem obter uma percepção mais profunda e rápida das informações, levando a um aumento na agilidade dos negócios para alcançar níveis de serviço e segurança mais elevados.

Referências

- [Aazam and Huh 2015] Aazam, M. and Huh, E.-N. (2015). Dynamic Resource Provisioning Through Fog Micro Datacenter. In *Pervasive Computing and Communication Workshops (PerCom Workshops), 2015 IEEE International Conference on*, pages 105–110. IEEE.
- [Aazam et al. 2014] Aazam, M., Khan, I., Alsaffar, A. A., and Huh, E.-N. (2014). Cloud of Things: Integrating Internet of Things and Cloud Computing and The Issues Involved. In *Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on*, pages 414–419. IEEE.
- [ABI Research 2015] ABI Research (2015). Internet of Everything Semiannual Update. Disponível em: <https://www.abiresearch.com/market-research/service/internet-of-everything/>. Acesso em: 16 dez. 2015.
- [Ahlgren et al. 2012] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlman, B. (2012). A Survey of Information-Centric Networking. *Communications Magazine, IEEE*, 50(7):26–36.
- [Ahmad et al. 2016] Ahmad, M., Amin, M. B., Hussain, S., Kang, B. H., Cheong, T., and Lee, S. (2016). Health fog: a novel framework for health and wellness applications. *The Journal of Supercomputing*, pages 1–19.
- [Alam et al. 2012] Alam, M. R., Reaz, M. B. I., and Ali, M. A. M. (2012). A review of smart homes - past, present, and future. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 42(6):1190–1203.
- [Atzori et al. 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*, 54(15):2787–2805.
- [Auto-ID 2016] Auto-ID (2016). Auto-ID Labs at MIT. Disponível em: <http://www.autoidlabs.org/>. Acesso em: 20 fev. 2016.
- [Bastug et al. 2014] Bastug, E., Bennis, M., and Debbah, M. (2014). Living on the edge: The role of proactive caching in 5g wireless networks. *Communications Magazine, IEEE*, 52(8):82–89.
- [Behrisch et al. 2011] Behrisch, M., Bieker, L., Erdmann, J., and Krajzewicz, D. (2011). Sumo—Simulation of Urban Mobility. In *The Third International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain*.
- [Bonomi 2011] Bonomi, F. (2011). Connected Vehicles, The Internet of Things, and Fog Computing. In *The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA*, pages 13–15.
- [Bonomi et al. 2014] Bonomi, F., Milito, R., Natarajan, P., and Zhu, J. (2014). Fog Computing: A Platform for Internet of Things and Analytics. In *Big Data and Internet of Things: A Roadmap for Smart Environments*, pages 169–186. Springer.

- [Bonomi et al. 2012] Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012). Fog Computing and Its Role in the Internet of Things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16. ACM.
- [Botta et al. 2016] Botta, A., de Donato, W., Persico, V., and Pescapé, A. (2016). Integration of Cloud Computing and Internet of Things: A Survey. *Future Generation Computer Systems*, 56:684–700.
- [Chen et al. 2014] Chen, C., Raj, H., Saroiu, S., and Wolman, A. (2014). cTPM: a Cloud TPM for Cross-Device Trusted Applications. In *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*.
- [Christophe et al. 2011] Christophe, B., Boussard, M., Lu, M., Pastor, A., and Toubiana, V. (2011). The web of things vision: Things as a service and interaction patterns. *Bell labs technical journal*, 16(1):55–61.
- [Cisco IOx 2014] Cisco IOx (2014). Cisco IOx Technical-Overview. Disponível em: <https://developer.cisco.com/site/iox/technical-overview/>. Acesso em: 22 mar. 2016.
- [Daraghmi et al. 2013] Daraghmi, Y.-A., Yi, C.-W., and Stojmenovic, I. (2013). Forwarding methods in data dissemination and routing protocols for vehicular ad hoc networks. *Network, IEEE*, 27(6):74–79.
- [Dash et al. 2010] Dash, S. K., Mohapatra, S., and Pattnaik, P. K. (2010). A Survey on Applications of Wireless Sensor Network Using Cloud Computing. *International Journal of Computer science & Engineering Technologies (E-ISSN: 2044-6004)*, 1(4):50–55.
- [Dastjerdi et al. 2016] Dastjerdi, A. V., Gupta, H., Calheiros, R. N., Ghosh, S. K., and Buyya, R. (2016). Fog Computing: Principles, Architectures, and Applications. *arXiv preprint arXiv:1601.02752*.
- [Deng et al. 2015] Deng, R., Lu, R., Lai, C., and Luan, T. H. (2015). Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing. In *2015 IEEE International Conference on Communications (ICC)*, pages 3909–3914.
- [Díaz et al. 2016] Díaz, M., Martín, C., and Rubio, B. (2016). State-of-the-art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computing. *Journal of Network and Computer Applications*.
- [Dinh et al. 2013] Dinh, H. T., Lee, C., Niyato, D., and Wang, P. (2013). A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches. *Wireless communications and mobile computing*, 13(18):1587–1611.
- [Distefano et al. 2012] Distefano, S., Merlini, G., and Puliafito, A. (2012). Enabling the Cloud of Things. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pages 858–863. IEEE.

- [Dsouza et al. 2014] Dsouza, C., Ahn, G.-J., and Taguinod, M. (2014). Policy-driven Security Management for Fog Computing: Preliminary Framework and a Case Study. In *Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on*, pages 16–23. IEEE.
- [Duan et al. 2015] Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C., and Hu, B. (2015). Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends. In *Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on*, pages 621–628. IEEE.
- [Elijah 2016] Elijah, G. (2016). Carnegie Mellon University - Elijah Gabriel Research Group: Cloudlet-based Mobile Computing. Disponível em: <http://elijah.cs.cmu.edu>. Acesso em: 22 mar. 2016.
- [ETSI ISG MEC 2015] ETSI ISG MEC (2015). ETSI Industry Specification Group, Mobile Edge Computing. Disponível em: <http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing>. Acesso em: 10 jan. 2016.
- [Fadlullah et al. 2014] Fadlullah, Z. M., Quan, D. M., Kato, N., and Stojmenovic, I. (2014). Gtes: An optimized game-theoretic demand-side management scheme for smart grid. *Systems Journal, IEEE*, 8(2):588–597.
- [Firdhous et al. 2014] Firdhous, M., Ghazali, O., and Hassan, S. (2014). Fog Computing: Will it be the Future of Cloud Computing? In *Proceedings of the 3rd International Conference on Informatics & Applications, Kuala Terengganu, Malaysia*, pages 8–15.
- [Fox et al. 2012] Fox, G. C., Kamburugamuve, S., and Hartman, R. D. (2012). Architecture and Measured Characteristics of a Cloud Based Internet of Things. In *Collaboration Technologies and Systems (CTS), 2012 International Conference on*, pages 6–12. IEEE.
- [Fritsch and Walker 2014] Fritsch, J. and Walker, C. (2014). The Problem with Data. In *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pages 708–713. IEEE Computer Society.
- [Gao et al. 2015] Gao, Y., Hu, W., Ha, K., Amos, B., Pillai, P., and Satyanarayanan, M. (2015). Are cloudlets necessary? Disponível em: <http://reports-archive.adm.cs.cmu.edu/anon/anon/2015/CMU-CS-15-139.pdf>. Acesso em: 15 mar. 2016.
- [Gartner Inc. 2015] Gartner Inc. (2015). Gartner’s 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. Disponível em: <http://www.gartner.com/newsroom/id/3114217>. Acesso em: 20 fev. 2016.
- [Gartner Inc. 2016] Gartner Inc. (2016). Research Methodologies: Gartner Hype Cycle. Disponível em: <http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp>. Acesso em: 15 fev. 2016.

- [Github 2016] Github (2016). Elijah Gabriel Research Group - Open Edge Computing. Disponível em: <https://github.com/openedgecomputing>. Acesso em: 22 mar. 2016.
- [Google Trends 2016] Google Trends (2016). Google Trends. Disponível em: <http://www.google.com/trends>. Acesso em: 11 fev. 2016.
- [Greenberg et al. 2008] Greenberg, A., Hamilton, J., Maltz, D. A., and Patel, P. (2008). The cost of a cloud: Research problems in data center networks. *ACM SIGCOMM computer communication review*, 39(1):68–73.
- [Gubbi et al. 2013] Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, 29(7):1645–1660.
- [Ha and Satyanarayanan 2015] Ha, K. and Satyanarayanan, M. (2015). OpenStack++ for Cloudlet Deployment. *School of Computer Science Carnegie Mellon University Pittsburgh*.
- [Han et al. 2011] Han, H., Sheng, B., Tan, C. C., Li, Q., and Lu, S. (2011). A Timing-Based Scheme for Rogue AP Detection. *Parallel and Distributed Systems, IEEE Transactions on*, 22(11):1912–1925.
- [Hong et al. 2013a] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., and Koldehofe, B. (2013a). Mobile Fog: A Programming Model for Large-scale Applications on The Internet of Things. In *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing*, pages 15–20. ACM.
- [Hong et al. 2013b] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., and Koldehofe, B. (2013b). Opportunistic spatio-temporal event processing for mobile situation awareness. In *Proceedings of the 7th ACM international conference on Distributed event-based systems*, pages 195–206. ACM.
- [Idland et al. 2015] Idland, E., Øverby, H., and Audestad, J. A. (2015). Economic markets for video streaming services: A case study of netflix and popcorn time. *Norsk Informatikkonferanse (NIK)*.
- [Jin et al. 2013] Jin, R., Wang, B., Zhang, P., and Luh, P. B. (2013). Decentralised online charging scheduling for large populations of electric vehicles: a cyber-physical system approach. *International Journal of Parallel, Emergent and Distributed Systems*, 28(1):29–45.
- [Kashi and Sharifi 2013] Kashi, S. S. and Sharifi, M. (2013). Connectivity weakness impacts on coordination in wireless sensor and actor networks. *Communications Surveys & Tutorials, IEEE*, 15(1):145–166.
- [Khalid et al. 2016] Khalid, M., Yousaf, M. M., Iftikhar, Y., and Fatima, N. (2016). Establishing the State of the Art Knowledge Domain of Cloud Computing. In *Advanced Computer and Communication Engineering Technology*, pages 1001–1014. Springer.

- [Klas 2016] Klas, G. I. (2016). Edge Cloud to Cloud Integration for IoT, Y.I Readings - News, Opinions, Analysis. Disponível em: <http://yucianga.info/?p=1008>. . Acesso em: 20 fev. 2016.
- [Lewis et al. 2014] Lewis, G., Echeverría, S., Simanta, S., Bradshaw, B., and Root, J. (2014). Tactical Cloudlets: Moving Cloud Computing to The Edge. In *Military Communications Conference (MILCOM), 2014 IEEE*, pages 1440–1446. IEEE.
- [Li and Shimamoto 2012] Li, C. and Shimamoto, S. (2012). An open traffic light control model for reducing vehicles' emissions based on etc vehicles. *Vehicular Technology, IEEE Transactions on*, 61(1):97–110.
- [Liu et al. 2015] Liu, K., Ng, J. K. Y., Lee, V. C. S., Son, S. H., and Stojmenovic, I. (2015). Cooperative data scheduling in hybrid vehicular ad hoc networks: Vanet as a software defined network. *IEEE/ACM Transactions on Networking*, PP(99):1–1.
- [Luan et al. 2016] Luan, T. H., Gao, L., Li, Z., Xiang, Y., We, G., and Sun, L. (2016). A View of Fog Computing from Networking Perspective. *arXiv preprint arXiv:1602.01509*.
- [Madsen et al. 2013] Madsen, H., Albeanu, G., Burtschy, B., and Popentiu-Vladicescu, F. (2013). Reliability in the Utility Computing Era: Towards Reliable Fog Computing. In *Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on*, pages 43–46. IEEE.
- [Manzalini and Crespi 2016] Manzalini, A. and Crespi, N. (2016). An Edge Operating System Enabling Anything-as-a-Service. *IEEE Communications Magazine*, 54(3):62–67.
- [Marforio et al. 2014] Marforio, C., Karapanos, N., Soriente, C., Kostiainen, K., and Capkun, S. (2014). Smartphones as Practical and Secure Location Verification Tokens for Payments. In *NDSS*.
- [Mell and Grance 2010] Mell, P. and Grance, T. (2010). The NIST definition of cloud computing. *Communications of the ACM*, 53(6):50.
- [Mineraud et al. 2015] Mineraud, J., Mazhelis, O., Su, X., and Tarkoma, S. (2015). A Gap Analysis of Internet-of-Things Platforms. *arXiv preprint arXiv:1502.01181*.
- [Mitton et al. 2012] Mitton, N., Papavassiliou, S., Puliafito, A., and Trivedi, K. S. (2012). Combining Cloud and Sensors in a Smart City Environment. *EURASIP journal on Wireless Communications and Networking*, 2012(1):1–10.
- [Modi et al. 2013] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., and Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1):42 – 57.
- [Moura and Hutchison 2016] Moura, J. and Hutchison, D. (2016). Review and Analysis of Networking Challenges in Cloud Computing. *Journal of Network and Computer Applications*, 60:113–129.

- [Nandyala and Kim 2016] Nandyala, C. S. and Kim, H.-K. (2016). From cloud to fog and iot-based real-time u-healthcare monitoring for smart homes and hospitals. *Atlantic*, 10(2).
- [Netflix 2016] Netflix (2016). Netflix open connect. Disponível em: <https://openconnect.itp.netflix.com>. Acesso em: 15 mar. 2016.
- [NetworkWorld 2015] NetworkWorld (2015). Microsoft, inter-view about Micro Datacentres (MDC). Disponível em: <http://www.networkworld.com/article/2979570/cloud-computing/microsoft-researcher-why-micro-datacenters-really-matter-to-mobiles-future.html>. Acesso em: 10 fev. 2016.
- [Nielsen Norman Group 2014] Nielsen Norman Group (2014). Nielsen's Law of Internet Bandwidth. Disponível em: <http://www.nngroup.com/articles/law-of-bandwidth/>. Acesso em: 20 dez. 2015.
- [Nitti et al. 2015] Nitti, M., Pilloni, V., Colistra, G., and Atzori, L. (2015). The Virtual Object as a Major Element of the Internet of Things: a Survey. *IEEE Communications Surveys and Tutorials*, 99:1–12.
- [OpenFog 2016] OpenFog (2016). Open Fog Architecture Overview. Disponível em: <http://www.openfogconsortium.org/wp-content/uploads/OpenFog-Architecture-Overview-WP-2-2016.pdf>. Acesso em: 16 jan. 2016.
- [Openstack 2015] Openstack (2015). Openstack Open Source Cloud Computing Software. Disponível em: <https://www.openstack.org/>. Acesso em: 20 mar. 2016.
- [OpFlex 2014] OpFlex (2014). OpFlex: An Open Policy Protocol White Paper. Disponível em: <http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731302.html>. Acesso em: 20 mar. 2016.
- [Orsini et al. 2015] Orsini, G., Bade, D., and Lamersdorf, W. (2015). Computing at the Mobile Edge: Designing Elastic Android Applications for Computation Offloading.
- [Ottenwälder et al. 2014] Ottenwälder, B., Koldehofe, B., Rothermel, K., Hong, K., and Ramachandran, U. (2014). Recep: Selection-based reuse for distributed complex event processing. In *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems*, pages 59–70. ACM.
- [Peng 2004] Peng, G. (2004). Cdn: Content distribution network. *arXiv preprint cs/0411069*.
- [Rahimi et al. 2003] Rahimi, M., Shah, H., Sukhatme, G. S., Heideman, J., and Estrin, D. (2003). Studying the feasibility of energy harvesting in a mobile sensor network. In *Robotics and Automation, 2003. Proceedings. ICRA'03. IEEE International Conference on*, volume 1, pages 19–24. IEEE.

- [Rao et al. 2012] Rao, B., Saluia, P., Sharma, N., Mittal, A., and Sharma, S. (2012). Cloud Computing for Internet of Things & Sensing Based Applications. In *Sensing Technology (ICST), 2012 Sixth International Conference on*, pages 374–380. IEEE.
- [Sarkar et al. 2015] Sarkar, S., Chatterjee, S., and Misra, S. (2015). Assessment of the Suitability of Fog Computing in the Context of Internet of Things. *IEEE Transactions on Cloud Computing*, PP(99):1–1.
- [Satyanarayanan et al. 2009] Satyanarayanan, M., Bahl, P., Caceres, R., and Davies, N. (2009). The Case for VM-Based Cloudlets in Mobile Computing. *Pervasive Computing, IEEE*, 8(4):14–23.
- [Satyanarayanan et al. 2015] Satyanarayanan, M., Schuster, R., Ebling, M., Fettweis, G., Flinck, H., Joshi, K., and Sabnani, K. (2015). An Open Ecosystem for Mobile-Cloud Convergence. *Communications Magazine, IEEE*, 53(3):63–70.
- [Sehgal et al. 2012] Sehgal, A., Perelman, V., Kuryla, S., and Schönwälder, J. (2012). Management of Resource Constrained Devices in the Internet of Things. *Communications Magazine, IEEE*, 50(12):144–149.
- [Shah and Pâris 2007] Shah, P. and Pâris, J.-F. (2007). Peer-to-Peer Multimedia Streaming Using BitTorrent. In *Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE International*, pages 340–347. IEEE.
- [Shi et al. 2015] Shi, Y., Ding, G., Wang, H., Roman, H. E., and Lu, S. (2015). The fog computing service for healthcare. In *Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on*, pages 1–5. IEEE.
- [Shimojo et al. 2015] Shimojo, T., Takano, Y., Khan, A., Kaptchouang, S., Tamura, M., and Iwashina, S. (2015). Future mobile core network for efficient service operation. In *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*, pages 1–6.
- [Simsek et al. 2016] Simsek, M., Aijaz, A., Dohler, M., Sachs, J., and Fettweis, G. (2016). 5G-Enabled Tactile Internet. *IEEE Journal on Selected Areas in Communications*, 34(3):460–473.
- [Stojmenovic 2014a] Stojmenovic, I. (2014a). Fog computing: a cloud to the ground support for smart things and machine-to-machine networks. In *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian*, pages 117–122. IEEE.
- [Stojmenovic 2014b] Stojmenovic, I. (2014b). Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *Internet of Things Journal, IEEE*, 1(2):122–128.
- [Stojmenovic and Wen 2014] Stojmenovic, I. and Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*, pages 1–8. IEEE.

- [Stojmenovic et al. 2015] Stojmenovic, I., Wen, S., Huang, X., and Luan, H. (2015). An overview of fog computing and its security issues. *Concurrency and Computation: Practice and Experience*.
- [Stolfo et al. 2012] Stolfo, S. J., Salem, M. B., and Keromytis, A. D. (2012). Fog computing: Mitigating insider data theft attacks in the cloud. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*, pages 125–128. IEEE.
- [Sudha and Viswanatham 2013] Sudha, S. and Viswanatham, V. M. (2013). Addressing security and privacy issues in cloud computing. *Journal of Theoretical and Applied Information Technology*, 48(2):708–719.
- [Suryawanshi and Mandlik 2015] Suryawanshi, R. and Mandlik, G. (2015). Focusing on mobile users at edge and internet of things using fog computing. *International Journal of Scientific Engineering and Technology Research*, 04(17):3225–3231.
- [Taivalsaari and Mikkonen 2015] Taivalsaari, A. and Mikkonen, T. (2015). Cloud Technologies for the Internet of Things: Defining a Research Agenda Beyond the Expected Topics. In *Software Engineering and Advanced Applications (SEAA), 2015 41st Euromicro Conference on*, pages 484–488. IEEE.
- [Tang et al. 2015] Tang, B., Chen, Z., Hefferman, G., Wei, T., He, H., and Yang, Q. (2015). A hierarchical distributed fog computing architecture for big data analysis in smart cities. In *Proceedings of the ASE BigData & SocialInformatics 2015*, page 28. ACM.
- [TinyOS 2016] TinyOS (2016). Main development repository for TinyOS (an OS for embedded, wireless devices). Disponível em: <https://github.com/tinyos/tinyos-main>. Acesso em: 20 mar. 2016.
- [Vaquero and Rodero-Merino 2014] Vaquero, L. M. and Rodero-Merino, L. (2014). Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. *ACM SIGCOMM Computer Communication Review*, 44(5):27–32.
- [Vermesan and Friess 2014] Vermesan, O. and Friess, P. (2014). *Internet of Things - From Research and Innovation to Market Deployment*. River Publishers.
- [Wei et al. 2014] Wei, C., Fadlullah, Z. M., Kato, N., and Stojmenovic, I. (2014). On optimally reducing power loss in micro-grids with power storage devices. *Selected Areas in Communications, IEEE Journal on*, 32(7):1361–1370.
- [Yao et al. 2013] Yao, D., Yu, C., Jin, H., and Zhou, J. (2013). Energy Efficient Task Scheduling in Mobile Cloud Computing. In *Network and Parallel Computing*, pages 344–355. Springer.
- [Yi et al. 2015a] Yi, S., Hao, Z., Qin, Z., and Li, Q. (2015a). Fog Computing: Platform and Applications. In *Hot Topics in Web Systems and Technologies (HotWeb), 2015 Third IEEE Workshop on*, pages 73–78. IEEE.

- [Yi et al. 2015b] Yi, S., Li, C., and Li, Q. (2015b). A Survey of Fog Computing: Concepts, Applications and Issues. In *Proceedings of the 2015 Workshop on Mobile Big Data*, pages 37–42. ACM.
- [Yi et al. 2015c] Yi, S., Qin, Z., and Li, Q. (2015c). Security and Privacy Issues of Fog Computing: A Survey. In *Wireless Algorithms, Systems, and Applications*, pages 685–695. Springer.
- [Yu et al. 2010] Yu, S., Wang, C., Ren, K., and Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Infocom, 2010 proceedings IEEE*, pages 1–9. Ieee.
- [Zao et al. 2014] Zao, J. K., Gan, T.-T., You, C.-K., Chung, C.-E., Wang, Y.-T., Méndez, S. J. R., Mullen, T., Yu, C., Kothe, C., Hsiao, C.-T., et al. (2014). Pervasive Brain Monitoring and Data Sharing Based on Multi-tier Distributed Computing and Linked Data Technology. *Frontiers in human neuroscience*, 8.
- [Zaslavsky et al. 2013] Zaslavsky, A., Perera, C., and Georgakopoulos, D. (2013). Sensing as a Service and Big Data. *arXiv preprint arXiv:1301.0159*.
- [Zhang et al. 2015] Zhang, B., Mor, N., Kolb, J., Chan, D. S., Lutz, K., Allman, E., Wawrzynek, J., Lee, E., and Kubiatowicz, J. (2015). The Cloud is Not Enough: Saving IoT from the Cloud. In *7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 15)*.
- [Zhang et al. 2010] Zhang, Q., Cheng, L., and Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. *Journal of internet services and applications*, 1(1):7–18.
- [Zhang et al. 2013] Zhang, W., Tan, G.-Z., and Ding, N. (2013). Traffic Information Detection Based on Scattered Sensor Data: Model and Algorithms. *Adhoc & Sensor Wireless Networks*, 18.
- [Zhou et al. 2011] Zhou, B., Cao, J., and Wu, H. (2011). Adaptive traffic light control of multiple intersections in wsn-based its. In *Vehicular technology conference (VTC Spring), 2011 IEEE 73rd*, pages 1–5. IEEE.
- [Zikopoulos et al. 2011] Zikopoulos, P., Eaton, C., et al. (2011). *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. McGraw-Hill Osborne Media.