IoT , Fog Computing e Edge Computing: Integração Entre Essas Tecnologias e a Segurança Implementada Nelas

João Vicor Macedo Giombelli

Universidade Federal de Santa Catarina Florianópolis, SC, Brasil

Resumo – Neste artigo serão abordadas conceitos que estão extremamente interligados e que cada vez mais levantam dúvidas com relação a segurança dos dados que elas acessam e transportam. São elas: Internet das Coisas (IoT), Fog Computing e Edge Computing. E o foco deste artigo será em como pode e é feita a segurança unindo essas tecnologias. Também será observado os principais problemas, e soluções possíveis para permitir a integração dessas tecnologias.

1. INTRODUÇÃO
   1. Motivação

Com uma crescente demanda por soluções “IoT” nas empresas, a necessidade de dados serem processados rapidamente, substancialmente e no local é essencial. É aqui que entra a “Fog Computing” e a “Edge Computing”. E para que a transmissão e o acesso de dados sejam eficazes, a segurança é crucial.

* 1. Justificativa

O conceito de Internet das Coisas (IoT) e a ideia de um mundo onde quase tudo estará conectado apresentam diversos desafios, como a segurança e privacidade das informações coletadas e transportadas para as plataformas de gerenciamento IoT.

* 1. Objetivos
     1. Objetivo Geral

Este artigo tem o objetivo de fornecer conhecimentos sobre como está a segurança nas áreas de IoT, Fog Computing e Edge Computing.

* + 1. Objetivos específicos
* Apresentar coneceitos básicos de IoT, Fog Computing e Edge Computing.
* Analisar a segurança e privacidade ao utilizar Fog Computing, Internet das Coisas e Edge Computing
  1. Organização do Artigo

Este artigo está organizado da seguinte forma: A Seção 2 explica os conceitos básicos

da teoria de Internet das Coisas, Fog Computing e Edge Computing. A Seção 3 traz os

trabalhos correlatos, a integração das tecnologias embasadas e o estado da arte entre essas tecnologias.

1. CONCEITOS BÁSICOS
   1. Internet das Coisas (IoT)

O conceito primordial associado à Internet das Coisas (IoT - Internet of Things) relaciona-se à capacidade que os objetos possuem de se comunicar, reportando informações acerca de seu estado e funcionamento.

* 1. FoG Computing

Fog Computing é uma arquitetura de rede distribuída, mais perto dos clientes, na borda da rede. Isso possibilita uma baixa latência e evita que todo o tráfego dos dispositivos seja direcionado para o centro da rede, na nuvem. Tal arquitetura permite diversas novas aplicações que estão surgindo com a Internet das Coisas, que possuem requisitos que não

podem ou são mal atendidos pela arquitetura centralizada da Computação em Nuvem.

* 1. Edge Computing

No conetexto de Internet das coisas, Edge Computing se refere à infraestrutura computacional que existe perto das fontes de dados, como por exemplo, máquinas industriais (turbinas de vento, ressonância magnética). Estes dispositivos normalmente ficam distantes da computação centralizada existente na nuvem.

1. TRABALHOS CORRELATOS

Segue um breve resumo e comentários das referências escolhidas como base para a construção deste artigo.

* 1. Fog Computing Como Arquitetura de Rede Distribuida para Internet Das Coisas

Sena em seu artigo explica sucintamente sobre o funcionamento da Fog Computing e depois nos apresenta a questão de segurança em IoT. “Os desafios com a Internet das Coisas são maiores, especialmente por não temos apenas o mundo virtual (cibernético) como na internet comum, mas também temos os sistemas ci-berfísicos, como Internet das Coisas e Fog Computing.” E com isso ele quer dizer que para que não ocorram falhas na segurança desses dispositivos, a sua segurança deve ser atualizada constantemente prevenindo roubo de dados. Só que isso depende de pessoas ou empresas que muitas vezes elas podem não ter a capacidade ou o incentivo para fornecer tais atualizações. E então cita que é ai que entra o Fog Computing, que permite prover serviços na borda de rede (Edge Computing), próximo ao cliente. Diminuindo assim o caminho e os elementos de redes envolvidos na transmissão de dados. Ainda diz que para diminuir os problemas com privacidade violada deve–se garantir que:

• Apenas os dados realmente necessários para a funcionalidade do dispositivo sejam

coletados;

• Qualquer dado coletado seja desidentificado ou que seja anônimo;

• Todos os dados coletados sejam protegidos por criptografia;

• O dispositivo e seus componentes protejam as informações pessoais;

•Apenas pessoas autorizadas devem ter acesso a informações pessoais;

• Limites sejam impostos para a coleta de dados;

• Que usuários finais sejam avisados caso os dados coletados sejam maiores do que

esperado.

* 1. Interconexão segura de dispositivos IoT à nuvem através de edes virtuais privadas(VPNs)

Os autores constam que os dispositivos IoTs enfrentam desafios com segurança da informação já conhecidos, como ataques DoS (*Denial of Service*), interceptação e modificação de comunicação, por exemplo, assim como problemas relacionados à privacidade, integridade, confidencialidade, identificação e confiança. Além disso, no cenário da Internet das Coisas, esses problemas serão cada vez maiores e mais preocupantes, haja vista o número de objetos conectados à rede, interconexões entre IoTs e, em alguns casos, a sensibilidade das informações coletadas por esses dispositivos.

A OWASP (*Open Web Application Security Project's*), em 2014, levantou uma lista de vulnerabilidades na Internet das coisas: interface web insegura; autenticação e autorização insuficientes; serviços de rede inseguros; falta de criptografia no transporte dos dados; entre muitas outras. No artigo é sugerido que a utilização de redes virtuais privadas (VPN) poderia solucionar o problema relacionado à segurança no transporte dos dados à nuvem, proporcionando privacidade, confidencialidade e integridade.

Então eles realizaram um teste utilizando o modelo host-to-site, entre dispositivo IoT e a nuvem. No final dos testes eles concluem que o uso de VPNs utilizando o protocolo IPSec provou conseguir trazer o nível de segurança necessário no transporte dos dados de IoT devicesà nuvem. Mas ainda citam que “os objetos do modelo IoT ainda estão em evolução e serão necessários mais estudos relacionados à segurança dos mesmos para incrementar as camadas de proteção dos dados coletados, produzidos e transmitidos por eles”.

* 1. Computação em Névoa: Conceitos, Aplicações e Desafios

Os autores citam que 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.

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 Considerando a Névoa como uma pequena Nuvem, podemos aplicar técnicas de detecção de intrusos. 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. Mesmo assim os autores são adeptos do uso de Fog Computing e dizem que 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”.

Fog Computing : Implementation of Security and Privacy to

Comprehensive Approach for Avoiding Knowledge Thieving Attack

Exploitation Decoy Technology

Os autores questionam bastante a segurança da Computação em nuvem e dizem que qualquer agência das Nações Unidas que possui acesso não autorizado á nuvem pode explorar por arquivos e dados. O sistema de segurança atual, não está pronto para estabelecer se o usuário é legitimo ou não, ainda mais com o crescimento de dispositivos conectados à internet. É apresentada então como funciona o sistema de login em Fog Compution sugerido por eles e como ele é mais seguro que a nuvem. Quando o admin tenta logar no sistema, 2 passos são necessários: primeiramente entrar com o nome de usuário e o 2º passo seria colocar a senha. Caso esteja correto ele pode acessar todos os dados conectados, mas caso queira fazer download de algum ele deve responder uma pergunta de segurança. Se a resposta for errada, é fornecido para ele um arquivo falso ( com letras trocadas), assim enganando quem não tem a devida permissão.

4. Aspectos Relevantes

Internet das Coisas está cada vez mais difundida, que está tornando-se importante integrá-la com a computação em nuvem por causa da quantidade de dados que podem ser gerados e a exigência para ter utilização de recursos virtuais e capacidade de armazenamento, e também, para tornar possível criar mais utilidade a partir dos dados gerados pela Internet das coisas e desenvolver aplicações inteligentes para os usuários.

É nítida a complementariedade das duas tecnologias, e esta é a principal razão pela qual muitos pesquisadores têm apostado nessa integração. Na tabela, a seguir, é possível visualizar esta comparação.

|  |  |  |
| --- | --- | --- |
|  | Internet das coisas | Nuvem |
| Deslocamento | Infiltrado | Centralizada |
| Acessibilidade | Limitado | Ubíquo |
| Componentes | Coisas do mundo real | Recursos virtuais |
| Capacidades computacionais | Limitado | Virtualmente ilimitado |
| Armazenamento | Limitada ou nenhuma | Virtualmente ilimitado |
| Papel da Internet | Ponto de convergência | Prestação de serviços |
| Big data | Fonte de informações | Recursos para gerenciar |

Os ​*drivers* para a integração dessas duas categorias geralmente são enquadrados em três categorias: comunicação, armazenamento e computação, enquanto alguns outros têm implicações em todas as categorias, e são ditos transversais.

Na categoria de comunicação, dados e compartilhamento de aplicativos são dois *CloudIoT* drivers importantes. Graças ao paradigma ​*CloudIoT*​, aplicações ubíquas personalizadas podem ser entregues através da IdC, enquanto a automatização pode ser aplicada tanto para recolher dados e para distribuição de baixo custo. A Nuvem oferece uma solução eficaz e barata para se conectar, controlar e gerenciar qualquer coisa de qualquer lugar a qualquer momento usando portais personalizados e aplicativos embutidos.

Com relação a categoria de armazenamento. IdC implica, por definição, uma grande quantidade de fontes de informação (ou seja, as coisas), que produzem uma enorme quantidade de dados não-estruturados ou semi-estruturados, que também tem as características típicas de Big Data. Uma vez dentro da nuvem, os dados podem ser tratados de forma homogênea por meio de APIs bem definidas, podem ser protegidos através da aplicação de segurança de nível superior, e pode ser acessado diretamente e visualizado a partir de qualquer lugar.

Na parte de computação, os dispositivos da Internet das coisas têm de processamento de recursos energéticos e que não permitem complexo, processamento de dados no local limitado. A Nuvem oferece capacidades de processamento virtualmente ilimitadas e um modelo de uso ​*on-demand*​. Isto representa mais um importante ​*CloudIoT* ​*driver*​: necessidades de processamento da IdC pode ser adequadamente satisfeitas para a realização de análise de dados em tempo real, para a implementação escalável, aplicações colaborativas e etc.

Entre as propriedades transversais, encontram-se: facilidade de uso, custo reduzido, escalabilidade, interoperabilidade, flexibilidade, confiabilidade, eficiência, disponibilidade e segurança. De acordo com todos as literaturas pesquisadas, a Computação em Nuvem está sendo vista como complementar ao cenário da internet das coisas, ou seja, acredita-se que a nuvem preencha algumas deficiências da IdC.

1. Problemas existentes

Este tópico é dedicado à análise dos principais desafios relacionados a aplicações CloudIot. A seguir, uma tabela feita por Botta, Donato, Persico e Pescapé (2015), com os desafios típicos levantados pelos cenários de aplicação:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Privaci dade | Aspectos legais e sociais | Grande escala | Segurança | Confiabil idade | Atuação | Heterogei neidade |
| Smart Home e  Smart Metering |  |  |  |  | ✓ | ✓ | ✓ |
| Video vigilância |  |  |  | ✓ | ✓ | ✓ | ✓ |
| Cuidados de saúde | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cidades  Inteligentes e  Comunidades | ✓ | ✓ |  | ✓ | ✓ | ✓ | ✓ |
| Smart Energy e  Smart Grid | ✓ | ✓ |  | ✓ | ✓ | ✓ | ✓ |
| Automóvel e  Mobilidade  Inteligente |  |  |  | ✓ | ✓ | ✓ | ✓ |
| Logística inteligente |  | ✓ | ✓ |  | ✓ |  | ✓ |
| Monitoramento ambiental |  |  | ✓ | ✓ | ✓ | ✓ |  |

* 1. Segurança e Privacidade

Quando as aplicações críticas da Internet das coisas avançarem para a Nuvem, preocupações surgirão, por exemplo, devido à falta de confiança no prestador de serviços, o conhecimento sobre os acordos de nível de serviço (SLAs), e conhecimento sobre a localização física dos dados. Consequentemente, os novos desafios exigem uma atenção específica.

Segundo Botta et al. (2015), o sistema distribuído em questão é exposto a possíveis ataques (por ex. SQL Injection, cross site scripting, e side-channel) e vulnerabilidades importantes (por exsession hijacking e VM escape). Multilocação também pode comprometer a segurança e levar a vazamento de informações sensíveis. Além disso, a criptografia de chave pública não pode ser aplicada em todas as camadas, devido às restrições de energia de computação impostas pelas coisas. Estes são exemplos de temas que estão atualmente sob investigação, a fim de enfrentar o grande desafio de segurança e privacidade no CloudIoT.

* 1. Heterogeneidade

Um grande desafio na CloudIoT está relacionada com a grande heterogeneidade de dispositivos, sistemas operacionais, plataformas e serviços disponíveis e, possivelmente, usados para aplicações novas ou melhoradas, de acordo com Botta et al. (2015).

Também é uma preocupação não negligenciável. Serviços em nuvem normalmente vêm com interfaces proprietárias, fazendo com que a integração de recursos e mash-up de ser devidamente personalizados com base nos provedores específicos.

Serviços e aplicações IdC foram tipicamente concebida como soluções verticais isoladas, em que todos os componentes do sistema estão firmemente acopladas ao contexto aplicação específica. Para cada aplicativo / serviço possível, os provedores têm de examinar cenários alvo, analisar os requisitos, selecione ambientes de hardware e software, integrar subsistemas heterogêneos, desenvolver, fornecer infra-estrutura de computação, e fornecer manutenção do serviço.

* 1. Desempenho

Muitas vezes, as aplicações CloudIoT garantem desempenho específico e requisitos de QoS em vários níveis (isto é, de comunicação, computação e aspectos de armazenamento) e, em alguns cenários específicos atingir esses requisitos não pode ser facilmente alcançado. Botta et al. (2015) afirma que, em particular, ter uma rede aceitavelmente estável para alcançar a nuvem é um grande desafio, considerando-se que o aumento da banda larga não seguiu a evolução do armazenamento e de computação.

Na verdade, em vários cenários (por exemplo, quando é necessária a mobilidade) provisionamento de serviços de dados e precisa ser executada com alta reatividade. Pontualidade pode ser muito influenciada por questões imprevisíveis e aplicações em tempo real são principalmente susceptíveis a desafios de desempenho. Usabilidade e experiência do usuário também pode ser afetada por QoS deficientes (por exemplo, quando streaming de multimídia é necessário) .

* 1. Confiabilidade

Quando CloudIoT é adotado para aplicações de missão crítica, preocupações com a confiabilidade normalmente surgem por exemplo, no contexto da mobilidade inteligente, os veículos são muitas vezes em movimento e a criação de redes de veículos e comunicação é muitas vezes intermitentes ou não confiáveis.

Quando os aplicativos são implantados em ambientes com recursos limitados existe um certo número de desafios relacionados com a falha do dispositivo ou a impossibilidade de alcance desse dispositivo, de acordo com Botta et al. (2015).

De um lado, as capacidades de nuvem ajudar a superar alguns desses desafios (por exemplo, Nuvem aumenta a confiabilidade dos dispositivos, permitindo descarregar tarefas pesadas e, portanto, para aumentar a duração da bateria; Por outro lado, introduz incertezas relacionadas com a virtualização de data center ou exaustão de recursos . A falta de análises de confiabilidade e do desenvolvimento de estudos de casos específicos exacerbar o desafio.

* 1. Grande escala

Dispositivos​ CloudIoT permitem criar aplicações inovadoras que visam a integração e análise de informações provenientes do mundo real (incorporados) . Alguns dos cenários descritos exigem implicitamente a interação com um número muito grande destes dispositivos, geralmente distribuídas em ambientes de área ampla.

* + 1. grande escala dos sistemas resultantes torna desafios típicos mais difícil de superar (por exemplo, as exigências sobre a capacidade de armazenamento e capacidade computacional para processamento adicional se tornar árdua para estar satisfeito quando enfrenta os dados de longa duração coletadas em alta velocidade).

Além disso, a distribuição dos dispositivos de Internet das coisas faz tarefas de monitoramento mais difícil uma vez que eles têm de enfrentar latência dinâmica e problemas de conectividade.

* 1. Big Data

Com um número estimado de 50 bilhões de dispositivos que serão ligados em rede em 2020, atenção especial deve ser dada ao transporte, armazenamento, acesso e processamento da grande quantidade de dados que irão produzir. Graças ao recente desenvolvimento de tecnologias, a Internet das coisas vai ser uma das principais fontes de dados grandes, e Cloud permitirá para armazená-lo por muito tempo e para realizar análises complexas sobre ele.

* + 1. ubiquidade dos dispositivos móveis e difusão de sensores, na verdade, faz uma chmada para plataformas de computação escaláveis (todos os dias 2,5 quintilhões de bytes de dados são criados). Manipulação de dados convenientemente é um desafio fundamental, assim como o desempenho geral do aplicativo é altamente dependente das propriedades do serviço de gerenciamento de dados, afirma Botta et al. (2015).

* 1. Redes de sensores

Redes de sensores foram definidos como o principal facilitador da Internet das coisas e como uma das cinco tecnologias que irão moldar o mundo, oferecendo a capacidade de medir, inferir, e compreender indicadores ambientais, de ecologias delicados e recursos naturais para ambientes urbanos.

Os recentes avanços tecnológicos fizeram eficiente, de baixo custo e dispositivos miniaturizados baixo consumo de energia disponível para uso em grande escala, aplicações de sensoriamento remoto. Além disso, smartphones, embora limitada pelo consumo de energia e confiabilidade, vêm com uma variedade de sensores (GPS, acelerômetro, bússola digital, microfone e câmera), permitindo uma ampla gama de aplicações móveis em diferentes domínios de Internet das coisas. Neste contexto, o tratamento oportuno dos dados do sensor enormes e streaming, sujeitos a restrições e incertezas de energia e de rede, tem sido identificada como o principal desafio, especula Botta et al. (2015).

Nuvem oferece novas oportunidades na agregação de dados de sensores e exploração dos agregados para ampliar a cobertura e relevância, mas ao mesmo tempo afeta a privacidade e segurança.. Além disso, sendo a falta de mobilidade um aspecto típico de dispositivos comuns IdC, a mobilidade dos sensores introduzidas por smartphones assim como eletrônicos de vestir representa um novo desafio.

* 1. Nevoeiro de computação

Nevoeiro de computação é uma extensão da computação clássica Nuvem para a borda da rede (como a névoa é uma nuvem perto do chão). Ele foi projetado para suportar aplicações da Internet das coisas caracterizadas por limitações de latência e exigência de mobilidade e de geo-distribuição.

Apesar de computação, armazenamento e rede são recursos tanto da nuvem e da névoa, o último tem características específicas: localização borda e reconhecimento de local implicando baixa latência; distribuição geográfica e um grande número de nós em contraste com a Nuvem centralizada; apoio à mobilidade (através de acesso sem fio) e interação em tempo real (em vez de processos batch); suporte para interação com o Cloud.

Alguns autores propõem uma análise que mostra como a construção de projetos de computação de nevoeiro é um desafio. De fato, a adoção de abordagens baseadas em nevoeiro requer vários algoritmos e metodologias relacionadas com a confiabilidade das redes de dispositivos inteligentes, e que operam sob condições específicas que pedem técnicas de tolerância a falhas específicas.

1. Soluções possíveis

Identificados vários problemas existentes nessa integração de tecnologias, iremos abordar a possíveis soluções um dos principais desafios: a heterogeneidade. Díaz M, et al (2016) identificaram algumas propostas para a integração.

Há vários open source e plataformas proprietárias disponíveis para Cloud e integração da Internet das coisas. A maioria delas são destinadas a resolver um dos principais problemas neste campo que está relacionado com a heterogeneidade das coisas e das nuvens. Estas plataformas tentam colmatar esta lacuna na implementação de um middleware para as coisas em direção à nuvem, e eles geralmente fornecem uma API para as aplicações.

* 1. Middleware OpenIoT

OpenIoT (https://github.com/OpenIotOrg/openiot) é um middleware de código aberto, co-financiado pela União Europeia Sétimo Programa-Quadro, para obter informações sobre os sensores, atuadores e dispositivos inteligentes e oferecendo serviços de Internet das coisas com base em serviços públicos em uma plataforma de nuvem.

OpenIoT aproveita o estado da arte sobre os quadros de middleware de RFID / WSN e Internet das coisas como XGSN e AspireRFID. Sensores virtuais também são promovidas por OpenIoT, permitindo o conceito de Sensoriamento-as-a-Service. A inclusão principal é a estrutura semântica, utilizando ontologias, permitindo semântica interação e interoperabilidade entre sistemas externos e oferecendo interfaces abertas dados vinculados. OpenIoT também projetou um conjunto de aplicações sobre a plataforma de nuvem, para permitir a especificação de on-the-fly de solicitações de serviços à plataforma OpenIoT, visualização de dados e configuração e os componentes de monitoramento ao longo dos sensores e serviços OpenIoT

* 1. Plataforma Nimbits

Nimbits (http://www.nimbits.com/) é uma plataforma de código aberto para conectar as coisas na nuvem, e uns aos outros. Actualmente, Nimbits pode ser baixado e instalado de forma privada, além de usar um Nimbits nuvem pública implantados no Google App Engine.

Nimbits é composto por dois componentes principais: um servidor web que registra e processa geo e dados em tempo carimbado, e executa regras do usuário sobre os dados, tais como notificações push, e-mails e mensagens XMPP; e uma biblioteca Java para o desenvolvimento e ligação de novos aplicativos na plataforma.

Além disso, Nimbits contém uma biblioteca de apoio Arduino e um App Android para gerenciar e visualizar todas as cópias de dados ligados. Os dados são enviados por clientes usando o JSON (JavaScript Object Notation) formato. Os usuários podem configurar pontos de dados a comportar-se de muitas maneiras em cascata quando novos dados são gravados, gerando diferentes gatilhos e alertas em cada situação.

Várias partes do Nimbits são fornecidos com uma licença de código aberto, mas os principais componentes não contêm uma licença de código aberto, embora este último pode ser baixado gratuitamente agora.

6.3. Plataforma Xively

Xively (https://xively.com/) é uma plataforma de Internet das coisas como um serviço para o desenvolvimento de aplicações sobre coisas ligadas. Xively oferece diferentes métodos de comunicação para conectar coisas, como RESTFul, HTTP, Sockets e MQTT (Message Queue Telemetry Transport). Formatos de dados diferentes, tais como JSON, XML e CSV, e bibliotecas oficiais para dezenas de línguas e plataformas como o Arduino, Android, Java e C.

O Xively API foi construído para ler e gravar dados e gerenciar produtos e dispositivos. Xively foi concebido para apoiar um processo de desenvolvimento em três fases: desenvolvimento para dispositivos de teste e aplicações, implantação para transformar os protótipos em produtos e gerenciamento dos produtos de dosagem e oferecer suporte a dispositivos em tempo real. Isto pode ser feito pela interface web oferecido pelo Xively.

Além disso, a plataforma contém a segurança end-to-end para proteger canais de comutação e de permissões refinadas. Xively tem uma licença proprietária, permitindo que os usuários e sistemas para conectar com a sua plataforma.

6.4. Sensor Cloud

SensorCloud (http://www.sensorcloud.com/) aproveita as tecnologias de computação em nuvem para fornecer uma plataforma de armazenamento de dados, visualização e gestão. Para a interligação Internet das coisas, a empresa microstrain oferece um gateway específico, que coleta dados de seus sensores e empurra-lo para SensorCloud.

Além disso, dados de outros dispositivos da Internet das coisas pode ser publicado em

SensorCloud através da API RESTful oferecido. SensorCloud também incorpora o MathEngine-um conjunto de ferramentas de software para processar, analisar e monitorar dados em um sensor mecanismo para fazer upload de seus próprios scripts para processar dados e um motor de alertas (como outras plataformas de integração). Por último, SensorCloud oferece vários planos de usar a sua plataforma, desde os gratuitos com 25.000 transações por mês.

6.5. Stack4Things

Stack4Things propõe uma extensão da plataforma OpenStack a fim de permitir uma infra-estrutura orientada a nuvem para gerenciar a Internet das coisas. Stack4Things conta com o OpenStack como uma plataforma de nuvem, bem como gerente de infra-estrutura virtual para fornecer serviços de nível superior aplicados à Internet das coisas.

Os componentes s4tProbe constituem os componentes finais do sistema, que são implantados em placas Arduino Yun. Os componentes s4tProbe ligam a Internet das coisas com a plataforma OpenStack proporcionando um design baseado em puxar através do protocolo AQMP e um design baseado impulso através Coap. A plataforma OpenStack foi estendido para suportar novas funcionalidades UI, integrar componentes s4tProbe e fornecer processamento de eventos complexos.

1. Projeto e Desenvolvimento de uma Proposta

Nesta seção abordaremos uma proposta, elaborada por Doukas e Maglogiannis, de um sistema de assistência médica que utilizaria IoT e Cloud, utilizando uma plataforma de nuvem para IoT. Para isso, sensores são utilizados para capturar sinais biológicos do usuário (como freqüência cardíaca, ECG, saturação e temperatura do oxigênio), dados de movimento (através de acelerômetros) e dados contextuais (como localização, temperatura ambiente, status da atividade, etc.)

Os principais componentes da arquitetura proposta são:

* + - Os sensores portáteis e móveis que adquirem sinais biológicos do paciente, movimento e informações contextuais.
    - O gateway do sensor que coleta todos os sinais dos sensores e encaminha-os para a Internet. Pode ser um telefone móvel ou uma plataforma de microcontrolador capaz de se comunicar com a Internet. Ele também envia informações sobre o status dos sensores (por exemplo, operação adequada, níveis de fonte de energia, etc.).
    - As APIs de comunicação fornecidas pela plataforma Cloud. Estes últimos são interfaces leves (como REST Web Services) do que podem ser usados pelos gateways do sensor para enviar dados do sensor e recuperar informações. A API também pode ser utilizada por aplicativos externos para processamento de dados, gerenciamento de alertas, cobrança, etc.
    - O aplicativo de gerenciamento consiste em um aplicativo baseado na web que é atualizado em tempo real e fornece visualização dos dados do sensor (em gráficos, etc.) e informações importantes sobre o contexto do paciente (como localização, status da atividade, etc.).
    - A infraestrutura Cloud que hospeda as interfaces e o aplicativo de gerenciamento. Ele fornece os recursos essenciais (como servidores de CPU, armazenamento e aplicativos) para a implantação do aplicativo web e as interfaces que permitem a comunicação com os sensores e os vários sistemas externos.



Figura 2 - Desenho da Proposta

Os sensores estão ligados a um Arduino que coleta dados através do software incorporado apropriado e transmite-os em um telefone móvel baseado em Android através de uma interface Bluetooth. Um aplicativo apropriado foi desenvolvido para o Android que coleta os dados e encaminha-os para a Nuvem.

* 1. parte da nuvem consiste em um aplicativo Java EE que fornece a interface gráfica de gerenciamento e as interfaces para a comunicação com os sensores. Como uma infra-estrutura da nuvem, a plataforma Jelastic foi selecionada. O Jelastic é um fornecedor de plataforma como um serviço (PaaS) Cloud que permite aos usuários implantar aplicativos baseados em Java que fornecem todos os componentes essenciais (instâncias do servidor de aplicativos, bancos de dados, balanceadores de carga, etc.) e toda a escalabilidade apropriada. O Jelastic fornece acesso total ao ambiente de tempo de execução do servidor de aplicativos, que permite a implantação de extensões Java adicionais, como criptografia e bibliotecas de autenticação.

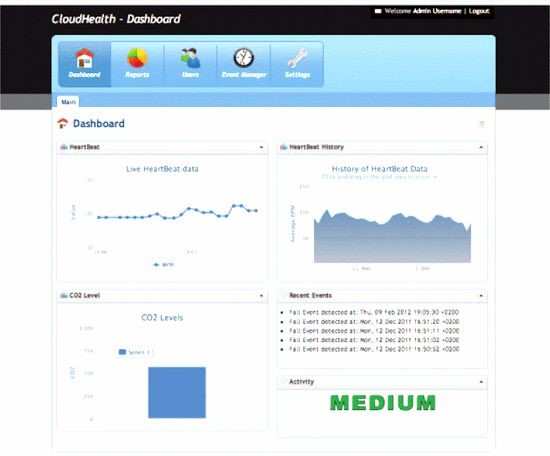


Figura 3 - Interface CloudHealth

1. Conclusões

* 1. Internet das coisas, e o número cada vez maior de dispositivos, tecnologias e plataformas neste campo, levaram a Internet das coisas para ser uma tecnologia global e estendida em muitas áreas. No entanto, devido às limitações da Internet das coisas como apresentados neste trabalho e a necessidade de recursos complexos para atender as demandas existentes, tecnologias atuais, como Cloud Computing, são apropriados como um complemento neste campo.

Neste trabalho foi possível identificar os aspectos complementares da Cloud e Internet das coisas e os principais motores para integrá-los em um ambiente único. Desde a adoção do paradigma CloudIoT possibilitando várias novas aplicações, que deriva os principais desafios de pesquisa de interesse para cada um deles.

Foram analisados os principais desafios, a fim de identificar as direções de pesquisa atuais. Finalmente, nós examinamos as plataformas e projetos disponíveis, comparando seus principais aspectos e questões em aberto identificadas e direções futuras pesquisas neste campo.

A respeito das plataformas, todas as propostas pesquisadas têm suporte API REST e uma interface web de gestão. A maioria das propostas estão disponíveis on-line para uso e implantação de uma infra-estrutura da Internet das coisas, exceto para Stack4Things e OpenIoT, mas o último tem o código fonte disponível online.

Para os aspectos de segurança das plataformas, a maioria dos componentes fazem uso de tokens de modo a permitir uma forma segura de autenticação, identificação e permissões sobre um conjunto de usuários ou dispositivos. Por outro lado, SensorCloud e CloudPlugs protegem a sua comunicação através de protocolos seguros, mas eles não fazem uso de tokens, pois ele pode ser excessivamente pesada para dispositivos embarcados.

Com base nas comparações realizadas e os elementos pesquisados, os usuários podem selecionar os elementos necessários com base em suas próprias necessidades, a fim de obter uma integração perfeita. A maioria dos componentes pesquisados têm licenças de código aberto, portanto, qualquer usuário pode desenvolver uma plataforma com estes componentes e levantamento novos componentes para melhorar este documento e a investigação neste domínio.

1. Trabalhos Futuros

Segurança e Privacidade são os principais desafios na implantação de infra-estruturas de IoT. Os dispositivos IoT são normalmente associados a dispositivos restritos, por isso são mais vulneráveis a ataques e ameaças. Por outro lado, em muitas situações, os sistemas IoT usam informações sensíveis como informações pessoais ou infra-estruturas críticas, portanto a privacidade com dispositivos, nuvem e rede são aspectos-chave. Roman et al. (2013) mencionou a importância da segurança e da privacidade para impulsionar a abordagem da Internet das Coisas no mundo real. Eles enumeraram os mecanismos de segurança que podem ser integrados no IoT:

* + - Protocolo e segurança de rede que oferece mecanismo de comunicação seguro de ponta a ponta;
    - Gerenciamento de identidade para obter autenticação e autorização para assegurar que os dados são produzidos por uma determinada entidade e restringir o controle de acesso;
    - Privacidade sobre os dados gerados;
    - Confiança entre entidades e usuários interação e governança para apoiar decisões políticas e estabilidade;
    - E tolerância a falhas para prevenir e detectar ataques. Por último, e os mais difíceis de evitar são modelos de ataque no IoT como DoS (Denial of service), danos físicos, espionagem, captura de nó para extrair informações e controlar entidades.

Além disso, a segurança e a privacidade são uma das principais preocupações sobre a adoção da nuvem.

Outro aspecto considerado é a Computação em Nuvem: Mesmo que a Computação em Nuvem possa ajudar a evitar algumas limitações de IoT, há situações como suporte à mobilidade, geo-distribuição, localização e baixa latência que precisam ser tratadas e Cloud Computing não tem meios para enfrentá-las.

Uma nova plataforma, chamada Fog Computing (Aazam e Huh, 2014), quer fornecer serviços de armazenamento, computação e rede entre o Cloud Computing e dispositivos finais. Ele é chamado de Nevoeiro porque nevoeiro é uma nuvem perto do solo e seu principal objetivo é estender Cloud Computing para trazê-lo mais perto de dispositivos IoT.

Em certas situações, os dados não são necessários para a nuvem ou devem ser processados com latência e mobilidade muito baixas, de modo Fog Computing pode fornecer os requisitos necessários em IoT através de uma plataforma distribuída e colaborativa em colaboração com dispositivos IoT. No entanto, devido às limitações de IoT, a Fog Computing não pode fornecer funcionalidades como análises complexas, acesso de dados a um grande número de usuários e armazenamento de dados históricos, o que é complementado com Cloud Computing.

Outro item mencionado é a arquitetura Lambda (LA) (Marz e Warren, 2015) é um paradigma composto por plataformas de nuvem - uma fila distribuída, processamento em lote e fluxo e lojas de dados distribuídos - projetado para oferecer consultas arbitrárias sobre dados arbitrários em tempo real. Devido às características temporais dos dados IoT e à necessidade de extrair conhecimentos e previsões de dados históricos, mesmo em algumas situações com tempo real, acreditamos que o LA é um paradigma certo para o IoT, o que trará os seguintes benefícios: armazenamento, Processamento em tempo real, escalabilidade e aprendizado de máquinas.

O processamento em tempo real é um requisito necessário para muitas situações, por exemplo, infra-estruturas críticas e sistemas de saúde. Além disso, em outros cenários, o verdadeiro conhecimento reside nos dados, já que pode ser usado para evitar que certas situações surjam e agirem antecipadamente, ea LA estimula esses cenários. Além disso, as habilidades de LA para gerenciamento de ambiente inteligente em larga escala e armazenamento / análise de Big Data são mostradas em Villari et al. (2014). Além destes benefícios, LA não é centrado em qualquer tecnologia em particular, para que cada usuário pode escolher a tecnologia necessária com base em suas necessidades.

REFERÊNCIAS BIBLIOGRÁFICAS

# -Countinho A, Carneiro E, Greve F, “Computação em Névoa: Conceitos, Aplicações e Desafios” Cap. 6. 2016 .Disponivel em: <https://www.researchgate.net/profile/Antonio\_Augusto\_Coutinho/publication/309312665\_Computacao\_em\_Nevoa\_Conceitos\_Aplicacoes\_e\_Desafios/links/5809143f08ae040813483c45/Computacao-em-Nevoa-Conceitos-Aplicacoes-e-Desafios.pdf.> Acessado em 20/08/2017.

# -EDUARDO ANTÔNIO DE SENA, “FOG COMPUTING COMO ARQUITETURA DE REDE DISTRIBUÍDA PARA INTERNET DAS COISAS, BRASÍLIA”, 25 DE JUNHO DE 2016. Acessado em 20/08/2017.

-SônegoA , MarcelinoR, GruberV, “A Internet das Coisas aplicada ao conceito de eficiência energética: uma análise quantitativo-qualitativa do estado da arte da literatura”, 2016 <http://revistas.ufpr.br/atoz/article/view/47860/29517->. Acessado em 20/08/2017.

- Tchordach B, Simplício D, Barros J, Calçada S, “

Interconexão segura de dispositivos IoT à nuvem através de redes virtuais privadas (VPNs)” ,

FaSCi-Tech – Periódico Eletrônico da FATEC-São Caetano do Sul, São Caetano do Sul, v.1, n. 12, Abr. 2017, p. 18 a 31. -. Disponível em : < http://www.fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/107> . Acessado em 20/08/2017.

# - Li G, Zhou H, Feng B, et al, “Fuzzy Theory Based Security Service Chaining for Sustainable Mobile-Edge Computing” 16/02/2017. Disponivel em : <https://www.hindawi.com/journals/misy/2017/8098394/> . Acessado em 20/08/2017.

-Alberto C, “Gerenciamento de Nuvem Computacional usando critérios de Segurança”, 25 de setembro de 2015 . Disponivel em: <<http://www.reposip.unicamp.br/bitstream/REPOSIP/275592/1/Silva_CarlosAlbertoda_D.pdf> . > Acessado em 20/08/2017.

-Babar S, Mahalle P, Stango A,”Proposed Security Model and Threat Taxonomy for the

Internet of Things (IoT), 2010. Disponivel em: <ftp://ftp.inf.puc-rio.br/pub/docs/FomularioSolicitacoes/MarkusEndler-04-14.pdf. > Acessado em 20/08/2017.

-Kurikala G, Gupta K, Swapna A, “Fog Computing : Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack

Exploitation Decoy Technology”, 2017. Disponivel em :

< <http://ijsrcseit.com/paper/CSEIT172428.pdf>> Acessado em 21/08/2017.