Thiago de Souza Ventura – 15200622

Redes de Computadores I – 2017/2

Título:

A Presença de Cloud Computing no contexto de Internet Das Coisas

Resumo:

Esse artigo está sendo feito por partes baseado no assunto que envolve a IoT (Internet of Things) ou internet das coisas, que basicamente é um assunto muito discutido nos dias de hoje, sendo um tópico muito presente quando se fala sobre "avanços tecnológicos".

1.Introdução:

1.1.Motivação:

Minha motivação é basicamente o fato de a internet estar tão presente na vida das pessoas, e a tendência é estar cada vez mais.

1.2.Justificativa:

Basicamente falando, o conceito de Internet das Coisas consiste em atribuir uma função de conectar ("on/off") qualquer aparelho a internet (ou a outro aparelho).

Aparelhos celulares são provavelmente os exemplos mais famosos e você com certeza já tem ou viu um. Mas não se engane, tem muito mais exemplos que muitas vezes você nem imagina que possam ser conectados a uma rede ou a outro item remotamente, como por exemplo, o motor de um avião. Portanto, será interessante aprender um pouco sobre o futuro que nos espera, que seria "um mundo conectado".

1.3.Objetivos:

Geral:

A intenção será sempre apresentar as informações de forma mais simples possível, sobre o assunto para que seja de leitura rápida e interessante à todos os tipos

de leitores. Basicamente o objetivo geral desse artigo é você entender a importância do tema apresentado para a vida das pessoas, e como é presente nelas. Também é objetivo geral entregar um conhecimento geral sobre o tema, para esse fim as informações gerais estarão simplificadas, e possuirá algumas informações extras que serão mencionadas abaixo.

Específico:

Então, caso só um conhecimento geral não seja suficiente para o leitor, esse artigo também abordará algumas informações mais específicas e detalhadas para maior entretenimento daqueles que sentem mais prazer lendo sobre o assunto em questão. Pesquisas realizadas, análises estatísticas, são algumas das coisas planejadas para esse artigo.

1.4.Organização do artigo:

Esse artigo estará organizado da seguinte forma: A seção 1 será a introdução (se você está lendo isso você provavelmente sabe, se não sabe sugiro que volte ao começo desta seção para ter uma leitura mais dinâmica), A seção 2 estará apresentando os conceitos básicos para você conhecer o tema abordado neste artigo,e por fim, a seção 3 apresentará trabalhos correlatos e uma discussão breve sobre problemas e soluções apresentados nesses artigos.

2.Conceitos Básicos:

2.1.Internet das Coisas:

O conceito básico de "IoT" já foi apresentado acima, então você provavelmente já sabe, mas vale ressaltar que basta ter como conectar/desconectar algo para ele pertencer a "IoT". Mas você pode se perguntar: "como assim pertencer? ". Bem, a resposta para esta pergunta é a seguinte: A "IoT" pode ser definida como uma network de "coisas" conectadas ("coisas" inclui pessoas). A Gartner(www.gartner.com) estima que haverá até 8.6 bilhões de "coisas" conectadas sendo utilizadas no mundo todo em 2017, um aumento de 31% de 2016, e passará dos 20 bilhões por volta de 2020. Está nítido que o número só tende a aumentar(e muito), o que faz desse um dos temas mais importantes da atualidade.

Talvez você ache que não mudará muito seu jeito de viver, afinal quem não trabalha muito com tecnologia hoje, realmente não tem uma ligação tão grande com a "IoT" como especialistas em Redes e técnicos em informática precisam ter. Porém, a nova regra para o futuro será: "*Anything that can be connected, will be connected* ", ou seja, tudo o que pode ser conectado, assim será. Com isso em mente, e levando em conta as pesquisas de crescimento intenso da "IoT" ao redor do mundo, não demorará muito para conectarem coisas que você não imaginaria que pudessem ser conectadas,

como por exemplo, uma simples vassoura. As relações básicas seriam 3: pessoa-pessoa, pessoa-coisa e coisa-coisa. Apesar de que sua vida provavelmente será diferente de alguns anos pra cá, as mudanças têm o objetivo de facilitar sua vida, conectando cada vez mais, e quebrando barreiras de alcance cada vez mais longos.

2.2.Fog Computing:

Para descrever o Fog Computing devemos entender o que é Cloud Computing. Cloud Computing é um modelo alternativo e eficiente ao gerenciamento e uso de Data Centers(DCs) privados para criação de aplicações Web e Processamento em Lote. Simplificando, "você aluga" poder de máquinas para fazer seus processamentos e aplicações. Assim, quando não estiver mais utilizando, você pode fazer a "devolução". Entretanto esse modelo vira um problema quando falamos de aplicações muito sensíveis a latência, que precisam de centros distributivos nas proximidades para não ultrapassar o limite máximo de atraso. E assim chegamos a Fog Computing.

Fog Computing é uma extensão do Cloud Computing ao limite da rede, habilitando novos tipos de aplicações e serviços. As principais características de Fog Computing são: Baixa latência, alta distribuição geográfica, mobilidade, predominância do acesso via wireless, etc. Fog Computing é uma plataforma virtualizada que providencia computação, armazenamento, e serviços de rede entre aparelhos terminais e o Data Center tradicional de Cloud Computing, geralmente localizado(mas não sempre) no limite da rede. Enfim, por causa de suas inúmeras características, Fog Computing tem várias aplicações na "IoT", sendo 3 delas conexão de veículos, grades inteligentes e sensores wireless.

2.3.Edge Computing:

Assim como Fog Computing, o Edge também é uma extensão de Cloud Computing que possui o objetivo de aprimorar a experiência com a utilização da nuvem para armazenamento, processamento, etc.

"Hoje os modelos de nuvem não são desenvolvidos para o volume, variedade e velocidade de dados que a Internet Das Coisas gera" – Cisco, 2015. Como Cloud Computing foi sendo ultrapassado pelo gigante avanço em "IoT", era necessário passar esse modelo a um próximo estágio, que pudesse atender as altas demandas que a Internet Das Coisas gera. Com base nisso teve-se início a fase Edge Computing e Fog Computing, que melhorou o desempenho das redes, aproximando a fonte aos aparelhos que a utilizam. Newton dizia: "The key difference between the two architectures is exactly where that intelligence and computing power is placed", ou seja, a diferença chave entre Fog e Edge Computing é ONDE a força computacional estará armazenada. No Fog Computing essa força é armazenada numa "Node" geralmente localizadas nas extremidades da rede, como descrito no tópico anterior. Já o Edge Computing leva

diretamente a aparelhos programáveis. De acordo com Newton, Edge Computing simplifica a comunicação e reduz o risco de falha criando ligações de aparelhos físicos a PACs (Programmable Automation Controllers) para análise do aparelho enquanto ainda o programa do sistema central. Os PACs que determinarão se os dados serão armazenados no local, ou mandados para a nuvem para uma análise mais aprofundada.

2.4.Segurança IoT:

Com o maravilhoso mundo que o digital oferece aos empreendedores, a pressa em desbravar as possibilidades da IoT e ganhar mercado, muitas vezes pode fazer com que startups e desenvolvedores individuais deixem de lado os inúmeros testes que são aconselháveis no desenvolvimento tecnológico.

Por outro lado, os próprios usuários precisam se acostumar com o ritmo frenético de novidades, atualizando seus dispositivos (especialmente as tecnologias vestíveis, ou wearables) com as versões mais recentes dos sistemas, além de não esquecer de adquirir e manter atualizadas ferramentas de segurança.

Para a maioria dos especialistas em segurança na Internet das Coisas, o futuro, além de ser uma preocupação dos desenvolvedores, está nas mãos dos usuários. Cabe a eles optar por sistemas originais e atualizados, adquirir aplicativos somente de fontes confiáveis, fazendo downloads de lojas oficiais, por exemplo.

No ambiente corporativo, um conselho é isolar o tráfego dos dispositivos e usuários que se encaixam no campo da Internet das Coisas em uma rede wi-fi exclusiva. Isso faz com que o controle do pessoal de TI fique mais preciso. Também ajuda na garantia de que a operação da empresa não será prejudicada com a enorme quantidade de coisas conectadas — já passamos do momento de proibir que um funcionário venha para o trabalho com seu tênis Nike que é conectado a um aplicativo, por exemplo.

Internet das Coisas é um mundo novo, um mundo de oportunidades, mas também é um desafio. Este desafio requer atenção, uma nova mentalidade; requer discussão e busca de soluções em segurança.

3.Trabalhos Correlatos:

3.1.Cidades Inteligentes: Uma arquitetura de Gerenciamento Autonômica no Contexto de IoT (2017):

O gerenciamento de infraestrutura de redes é uma atividade fundamental para a manutenção da rede e da qualidade dos serviços providos por ela. Este gerenciamento tem se tornado bastante complexo e custoso à medida que as redes ficam maiores e mais heterogêneas. Desta forma, os custos com o gerenciamento aumentam e a possibilidade de erros humanos também. Um ambiente que oferece esses desafios é a “Internet of Things” (IoT). O gerenciamento na IoT envolve além da infraestrutura de rede, o

gerenciamento de seus nós (dispositivos finais). Cidade Inteligente (CI) é outro ambiente como esses desafios de gerenciamento pois ele engloba a IoT, no entanto, é ainda mais complexo devido a sua grande escala e único domínio administrativo. Neste contexto, mecanismos tradicionais de gerencia de redes e dispositivos não são eficientes. Assim, esse trabalho propõe AutoManIoT, uma solução arquitetural de gerenciamento autonômico de rede e de dispositivos para o cenário de IoT e CIs. A arquitetura utiliza uma abordagem de provisionamento dinâmico e elástico dos serviços de rede através das tecnologias Redes Definidas por Software (SDN) e Virtualização de Funções de Rede (NFV). Essas tecnologias permitem melhorar a eficiência do controle e da operação da rede e ainda aproximar o gerenciamento da rede dos requisitos da aplicação.

3.2.Uma Plataforma Escalável para Desenvolvimento de Aplicações de IoT (2017):

A Internet das coisas (IoT) é um paradigma emergente que conecta dispositivos físicos ao mundo digital, permitindo a construção de uma miríade de aplicações. Desenvolver aplicações para de IoT não é uma tarefa trivial. Tais aplicações precisam ser construídas atendendo requisitos de escalabilidade a fim de suportar um grande número de dispositivos conectados, além de armazenar e processar a enorme quantidade de dados produzida. Além disso, as aplicações precisam lidar com protocolos distintos. Nessa perspectiva, o presente artigo apresenta a EcoCIT, uma plataforma de middleware escalável que provê suporte para a integração de dispositivos de IoT à Internet, bem como ao desenvolvimento e execução de aplicações de IoT com requisitos de escalabilidade através do uso serviços computacionais providos sob demanda por plataformas de computação em nuvem.

3.3.Internet das Coisas Aplicada a Negócios – Um Estudo Bibliométrico (2016):

A Internet das Coisas é uma inovação tecnológica, baseada em artefatos já consolidados como a Internet e objetos inteligentes. A crescente aplicação da Internet das Coisas nos negócios torna necessária uma avaliação de estratégias, benefícios e dificuldades enfrentadas na aplicação da tecnologia. O principal objetivo deste artigo é apresentar as diversas definições de Internet das Coisas, a partir dos artigos mais citados, e como objetivo secundário, apresentar estatísticas de publicação por ano e termos correlatos, como computação ubíqua. Uma das conclusões é que os artigos relacionados à temática de negócios correspondem a apenas 5% dentre todos os artigos recuperados por essa pesquisa, considerando apenas os artigos publicados em periódicos, o que demonstra que existe um grande campo de pesquisa em Administração.

3.4. Suporte IoT para Otimização de espaços físicos em ambiente Industrial (2016):

A globalização e a consequente evolução dos mercados conduziram a um aumento da procura e oferta de produtos. Estes fatos refletiram-se dando origem à conhecida sociedade de consumo presente nos dias de hoje. Como consequência dos fatos enumerados advém a crescente necessidade de transporte e armazenamento de produtos, o que se traduz em maiores custos para as empresas e consequentemente para o consumidor final. Assim, a necessidade de melhorar e otimizar estes processos torna-se uma questão pertinente, que desde cedo ganhou o seu lugar junto da comunidade científica. Melhorar o processo de otimização de espaço em veículos de transporte ou armazéns, revelou-se uma solução eficaz de forma a reduzir custos. Portanto, torna-se imperativo criar um sistema que permite a otimização destes processos de uma forma automática. Assim esta tese propõe a criação de um sistema que permita a otimização do espaço de uma forma automática e que tenha em consideração aspetos relevantes, minimizando custos e maximizando recursos úteis. Para tal esta solução apresenta uma forma melhorada para a classificação dos problemas de otimização de espaço, uma rede de sensores capaz de adquirir a informação referente aos produtos a acomodar, e por fim, toda a arquitetura necessária à implementação deste sistema em ambiente industrial.

4.Aspectos Relevantes:

O artigo The Computer of 21st Century de Mark Weiser, publicado em setembro de 1991 na Scientific American é um marco na pesquisa sobre a Internet das Coisas. O texto é tido como a primeira publicação sobre a computação ubíqua, o desaparecimento das tecnologias no tecido da vida cotidiana e aparece citado em praticamente toda a literatura sobre o assunto.

O termo “internet das coisas”, propriamente, só aparece em 2001 no livro branco de Brock, também pesquisador do Auto-ID Center (BROCK, 2001). Entretanto, Kevin Ashton, outro pesquisador do Auto-ID Center, reclama para si a paternidade do termo. Ashton diz que em 1999, usou a expressão pela primeira vez enquanto falava sobre as potencialidades do RFID na cadeia de abastecimento da multinacional Procter & Gamble. (ASHTON, 2009; UCKELMANN et al, 2011) Naquele momento, ele falava de uma internet das coisas para chamar a atenção dos empresários para o fato de que existem coisas que computadores fazem melhor do que as pessoas que tem tempo, atenção e precisão limitadas.

Outro possível nascimento do termo foi no ano de 1999, quando o então diretor do consórcio de pesquisa “Things that Think” do MIT Media Lab, Neil Gershenfeld, publicou “When Things Start to Think” (1999). O livro prevê e descreve algumas experiências de computação usável, nanotecnologia e preocupações relacionadas às emoções e direitos civis em uma realidade onde objetos processam informação.

Logo depois, aparece o primeiro eletrodoméstico ‘inteligente’: em junho de 2000, a LG apresentou sua geladeira inteligente durante um evento na Coreia do Sul11. O produto deveria fazer par com outros dispositivos, todos conectados à Internet e

gerenciáveis através de um sistema da própria LG. Na ocasião, o presidente da LG nos Estados Unidos, Simon Kang disse que o eletrodoméstico não apenas resfriava os alimentos como "Consumers can use the Internet refrigerator as a TV, radio, Web appliance, videophone, bulletin board, calendar and digital camera" 12.

Como observa o site Postscapes, no início dos anos 2000 a ideia de uma rede de objetos conectados produzindo e trocando informação começa a ganhar visibilidade. O Guardian publicou em 2003 uma reportagem sobre etiquetas de RFID e a EPC Network do Auto-ID Centre13. Em setembro de 2004, foi a vez da Scientific American levantar a questão das casas inteligentes, sensores interligados e tecnologias que permitam que tudo seja conectado em um artigo assinado por Neil Gershenfeld e outros pesquisadores do MIT Media Lab14. Em 2005, o termo apareceu pela primeira vez no New York Times relacionado às discussões na Cúpula das Nações Unidas para a era da informação naquele ano15, seguida de uma reportagem sobre as maravilhas e perigos dessa tecnologia, poucos dias depois16.

A partir de 2005, a discussão sobre a Internet das Coisas se generalizou, começou a ganhar a atenção dos governos e aparecer relacionada a questões de privacidade e segurança de dados. Foi neste ano que a Internet das Coisas se tornou a pauta do International Telecommunication Union (ITU), agência das Nações Unidas para as tecnologias da informação e da comunicação, que publica anualmente um relatório sobre tecnologias emergentes. Assim, depois da barda larga e da internet móvel, a Internet das Coisas ganhou a atenção do órgão e passou a figurar como o "próximo passo da tecnologias 'always on' [...] que prometem um mundo de dispositivos interconectados em rede" (ITU, 2005, p. 1).

2005 ainda foi o ano do lançamento do Nabaztag17, um objeto com a forma de um coelho que, conectado a Internet, poderia ser programado para receber a previsão do tempo, ler e-mails ou notícias, entre outras aplicações. Com diversas possibilidades de uso, o Nabaztag foi o primeiro objeto inteligente comercializado em escala e que tinha uma função menos "industrial". Novas versões do Nabaztag continuam a ser produzidas e a primeira versão do software do coelhinho foi disponibilizada em código aberto.

O livro Shaping Things de Bruce Sterling também foi publicado em 2005. A obra apresenta os spimes, objetos "desenhados em telas, fabricados digitalmente e rastreáveis no tempo e no espaço" (STERLING, 2005, p. 11). A referência aos spimes de Sterling é constante e seu livro foi o primeiro a esboçar critérios para o desenvolvimento desses objetos.

Em 2006, Adam Greenfield também se preocupou com os objetos conectados e lançou o livro Everyware. O texto fala sobre uma visão de processamento distribuída no ambiente a ponto de fazer os computadores, como os conhecemos hoje, desaparecerem. Além de definir o everyware e como ele deveria funcionar, o trabalho de Greenfield mostra o potencial das tecnologias ubíquas para o bem-estar (saúde, trabalhos perigosos, muito delicados ou repetitivos) e os perigos relacionados à vigilância e privacidade.

Em 2008, foi publicado The Internet of Things de Rob Van Kranenburg, livro que assim como Shaping Things e Everyware, busca falar sobre um novo paradigma no qual objetos produzem informação e é uma das grandes referências teóricas sobre a IoT. O texto levanta questões sobre a agência humana em ambientes que processam informação de forma autônoma, as novas formas de expressão. O autor expressa preocupações sobre a vigilâncias que as coisas conectadas podem exercer e a necessidade de se apropriar dessa tecnologia.

Naquele momento, já era possível ver a Internet das Coisas em funcionamento. Em 2008 foi lançado o Patchube.com, plataforma que conecta dispositivos e fornece controle e armazenamento de dados em tempo real. Recentemente, a plataforma mudou seu nome para Cosm, mas continua a operar sob a mesma API e com as mesmas características. A iniciativa permite que usuários conectem seus próprios sensores ou dispositivos e tem um papel importante na apropriação não-industrial da IoT.

No mesmo ano aconteceu a primeira Internet of Things Conference em Zurique na Suiça18, evento que teve suas discussões compiladas em um livro publicado no mesmo ano sob a organização de Christian Floerkemeier, Marc Langheinrich, Elgar Fleisch, Friedemann Mattern e Sanjay E. Sarma. Uma segunda edição foi realizada em 2010 em Tóquio e a terceira edição está marcada para outubro de 2012 em Wuxi na China. Todas as edições foram organizadas por uma comissão formada entre representantes da grande indústria de tecnologia e pesquisadores.

Um ano depois da conferência internacional, Salvador sediou o primeiro evento da temática no Brasil. Organizado pelo CIMATEC SENAI e pela Saint Paul Etiquetas Inteligentes, o 1º Congresso de Tecnologia, Sistemas e Serviços com RFID aconteceu de 26 a 29 de agosto na capital baiana. Na segunda edição, o evento mudou de nome para Congresso Brasileiro de Internet das Coisas e RFID, aconteceu em Búzios em outubro de 2011, mas manteve o foco empresarial nas discussões e industrial nas aplicações apresentadas nos cases.

No Brasil, além do congresso, 2010 marcou a implantação do Centro de Operações do Rio, quartel general da prefeitura da cidade do Rio de Janeiro que opera com tecnologia de cidades inteligentes da IBM. No COR um telão de 80 m² mostra o mapa da cidade com camadas de informação e imagens de câmeras que permitem visualizar o trânsito, condições climáticas e ocorrências diversas.

5.Problemas Existentes:

Os pesquisadores de segurança estão trabalhando duro para identificar vulnerabilidades associadas a muitos dos produtos IoT existentes, porém nem todas as vulnerabilidades serão identificadas e corrigidas antes de um ator mal-intencionado fazer uso delas.

A Rapid7 publicou recentemente um relatório sobre exposições e vulnerabilidades de babás eletrônicas conectadas. Neste relatório, eles descreveram um conjunto de vulnerabilidades potencialmente exploradas com base em acesso físico ao dispositivo, acesso direto à rede local (LAN) e através da internet. Pode-se imaginar o risco que isso causa a privacidade ou segurança de uma residência e de seus ocupantes?

A VTech, fabricante de brinquedos educativos de alta tecnologia para crianças, como dispositivos de aprendizado eletrônico, anunciou que sofreu uma violação de segurança em dezembro de 2015, expondo dados pessoais de 12 milhões de pessoas. O interessante deste evento foi que os próprios dispositivos não foram comprometidos. No entanto, os serviços online com os quais os dispositivos se conectam não estavam suficientemente protegidos.

Especificamente, um relatório afirmou que a violação explorava uma vulnerabilidade de injeção SQL e os serviços de registro de conta não usavam TLS. Considere que essas vulnerabilidades não estavam relacionadas a falhas nos próprios dispositivos IoT, mas sim a falhas descobertas na infraestrutura que suporta os dispositivos. Os dispositivos IoT não operam no vácuo, eles são parte de um ecossistema muito maior que também deve ser assegurado de forma adequada.

Os wearables, ou dispositivos vestíveis, também estão vulneráveis. Um estudo feito pela Open Effect mostrou que muitos fabricantes de dispositivos vestíveis ainda não tinham aproveitado os novos recursos de privacidade projetados na especificação Bluetooth 4.2. Verificou-se que o rastreamento de uma pessoa com um wearable era teoricamente possível.

Outra grande preocupação está relacionada à segurança de dispositivos médicos conectados. Em 2008, antes mesmo da disseminação da IoT, o pesquisador Daniel Halperin e seus colegas publicaram o documento intitulado "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses". Este documento abordou os dispositivos médicos implantáveis reprogramáveis através de conexão sem fio (IMDs), que incluem marca-passos, desfibriladores e bombas de drogas implantáveis. Os pesquisadores descreveram não apenas questões de privacidade associadas a esses dispositivos, mas também a capacidade de alterar as configurações do dispositivo, modificar ou desativar terapias e até mesmo oferecer um choque elétrico fatal ao paciente.

Para Cláudio Braghini, especialista em tecnologia e processos de negócios, a pressão para estar "na moda tecnológica" para que sejam obtidas certas conveniências que aparecem na mídia, em sites especializados ou mesmo para "criar um showroom tecnológico", fará com que muita gente coloque as novidades de maneira rápida,sem pensar nas consequências.

Em vista de todos esses problemas, a Cloud Security Alliance publicou um guia de boas práticas para desenvolvimento seguro de projetos de IoT chamado "Future-proofing the Connected World - 13 Steps to Developing Secure IoT Products". O

documento é resultado do trabalho realizado pelo grupo IoT Working Group e foi criado para auxiliar desenvolvedores de produtos e serviços relacionados a IoT a entenderem as medidas básicas de segurança que devem ser implementadas durante o processo de desenvolvimento.

O documento possui aproximadamente 70 páginas e aponta 13 considerações e diretrizes para mitigar alguns dos principais problemas encontrados no desenvolvimento de dispositivos IoT. Adicionalmente, também apresenta uma discussão sobre os principais desafios de segurança para IoT, os resultados de uma pesquisa conduzida pelo grupo de trabalho, uma discussão sobre as opções disponíveis para segurança, entre outros temas.

6.Soluções Possíveis:

Atualmente, a conectividade está presente em quase tudo. Desde uma smarTV conectada em casa, no ambiente doméstico, até automatizações mais complexas em ambiente corporativo, como o uso de sensores no Agronegócio, a fim de evitar a perda das lavouras por conta de intempéries climáticas ou pragas. Ou seja, com essa transmissão crescente de dados, em suportes e segmentos diversos, a comunicação entre objetos e internet pode estar vulnerável, a ponto de sofrer algum tipo de ataque, seja para indisponibilidade, mau funcionamento, controle do dispositivo e até mesmo vazamento de informações, entre outros.

A segurança da informação para esse tipo de realidade exige técnicas mais sofisticadas, diferente das tradicionais utilizadas no segmento da segurança virtual. Se pensarmos no potencial de crescimento da IoT, sobretudo no ambiente corporativo, a segurança virtual não pode ser deixada de lado neste contexto. Segundo pesquisa promovida pelo McKinsey Global Institute (MGI), o segmento de IoT pode impactar a economia global entre US$ 4 e US$ 11 trilhões por ano até 2025, incluindo países como o Brasil. Ou seja, quais medidas adotar para que a IoT fique segura?

A resposta é complexa, pois exige a combinação de elementos básicos de segurança da informação, que vêm sendo consolidados ao longo de algumas décadas, além de técnicas altamente inovadoras que ainda estão em fase de amadurecimento. No caso das técnicas de defesa, existe um amplo desafio de criar padronizações, mecanismos e selos de certificação que assegurem que estes dispositivos que ganharam conexões e outras funcionalidades sigam alguns princípios básicos. É importante que a indústria amadureça estes modelos, para conscientizar os fornecedores a incluir a pauta de segurança no desenvolvimento destes produtos.

A produção destes dispositivos é muito orientada para atender funcionalidades, e ainda não se preocupa como deveria com aspectos de segurança, que vão desde a oferta de protocolos de comunicação segura, até estruturas robustas de autenticação, controle

de acesso e gerenciamento de logs/registros. Isso é um grande problema, pois mesmo em casos relacionados à indústria, é comum que mesmo diante da miniaturização, os dispositivos possuam poder de processamento e armazenamento consideráveis.

Portanto, acima de tudo, quando bem utilizadas, algumas premissas minimizam potencialmente os impactos e eventuais exposições para empresas, no uso intensivo de IoT dentro de seus negócios. Elas são:

- Utilizar uma rede segmentada para estes dispositivos;
- Criar controle de acesso rigoroso para o que estes dispositivos podem acessar, tanto em outras redes, como a própria internet;
- Definir pré-requisitos de aquisição destes dispositivos, que levem em consideração protocolos e padrões de segurança, tanto de comunicação quanto autenticação e armazenamento de informações;
- Criar um mecanismo de centralização de logs desses dispositivos para identificar eventuais anomalias de uso ou acesso;
- Monitoramento constante ou visibilidade em NOC (Network Operation Center) e SOC (Security Operation Center) dos eventos destes dispositivos.

Portanto, a regra de ouro é sempre a mesma: não utilize estes recursos para atividades críticas que você não tenha como controlar ou garantir a segurança de maneira adequada. Ou seja, não acesse um banco através de uma televisão, ou não coloque o controle de produção de um equipamento super caro totalmente online.

Manter os dispositivos devidamente atualizados e estar alinhado com o fabricante em termos de reports de incidentes de segurança é uma facilidade importante, simples, que na maioria dos casos é negligenciada. O principal passo ainda é a prevenção. As facilidades tecnológicas oferecem uma atratividade forte para muitos usuários. Mas não se deve fechar os olhos: utilize estes dispositivos somente para o que é realmente necessário e evite acessar através dos mesmos itens de muita importância para você. No ambiente corporativo, é importante buscar especialistas para definir a arquitetura adequada para evitar e minimizar potenciais ataques.

7.Conclusão e Trabalhos Futuros:

7.1.Conclusão:

Descrevemos a visão e definimos características-chave da Fog Computing, uma plataforma para entregar um rico portifólio de novos serviços e aplicativos à beira da rede. Os exemplos motivadores salpicados durante toda a discussão variam de visões conceituais a protótipos de soluções de pontos existentes. Nós imaginamos o Fog como

sendo uma plataforma unificadora, suficientemente rica para oferecer esta nova geração de serviços emergentes e permitir o desenvolvimento de novas aplicações.

7.2.Trabalhos Futuros:

Com o objetivo de passar na disciplina de Redes I e aprofundar o conhecimento na área, estarei a realizar trabalhos práticos relacionados ao assunto. O trabalho prático mais próximo será feito escolhendo uma ferramenta de gerência de redes SNMP (Simple Network Management Protocol), por exemplo, PRTG, Zabix, Zenoss, Nagios, WhatsUp, Cacti... instalando a mesma, instalando agentes em algumas máquinas (ou usar agentes instalados em switch, hub, modem...), se necessário, e obtendo o valor de algumas variáveis (objetos gerenciados), no mínimo 5 variáveis (exemplo: velocidade de interfaces, número pacotes de entrada e saída, informações sobre conexões estabelecidas...) que devem ser observadas, no mínimo, durante 5 dias (com possíveis interrupções). Devo fazer um relatório também, o qual deve comentar sobre a ferramenta de gerência usada e descrever as características dos objetos gerenciados monitorados para explicar e interpretar os resultados obtidos (ou seja as medições realizadas). Para cada gráfico apresentado devem ser realizados os respectivos comentários, explicando os resultados obtidos. No relatório também deve ser apresentada a topologia da rede, mostrando a posição dos recursos e/ou serviços que foram gerenciados (monitorados), indicando o local em que foram realizadas as medições.

Referências Bibliográficas:

Jacob Morgan, **A Simple Explanation Of 'The Internet Of Things'. Disponivel em: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6d69a5f61d09. Acesso em agosto de 2017**.

Egham, **Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Disponivel em: http://www.gartner.com/newsroom/id/3598917. Acesso em agosto de 2017.**

Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli**, Fog Computing and Its Role in the Internet of Things. Disponivel em: http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf. Acesso em agosto de 2017.**

David Greenfield, **Fog Computing vs. Edge Computing: What's the Difference?. Disponivel em: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference. Acesso em agosto de 2017.**

Pablo Tibúrcio , Marcelo Santos , Stênio Fernandes, **Centro de Informática (CIn) – Universidade Federal de Pernambuco (UFPE) Recife – PE – Brasil. Disponível em: http://csbc2017.mackenzie.br/public/files/4-wpietfirtf/3.pdf. Acesso em Setembro de 2017.**

Gustavo Perri Galegale, Érica Siqueira, Carolina , Bertolucci Hilário e Silva, Cesar Alexandre de Souza, **Universidade de São Paulo, São Paulo, São Paulo, Brasil. Disponível em: http://www.revistas.usp.br/jistem/article/view/125817/122709. Acesso em Setembro de 2017.**

Jorge Pereira , Thais Batista , Flavia C. Delicato , Paulo F. Pires, **Departamento de Informática (DIMAp) Universidade Federal do Rio Grande do Norte (UFRN) Natal – RN /// Departamento de Ciência da Computação (DCC) Universidade Federal do Rio de Janeiro (UFRJ) Rio de Janeiro – RJ. Disponível em: http://csbc2017.mackenzie.br/public/files/9-sbcup/18.pdf. Acesso em Setembro de 2017.**

Cristiano José Chainho Pereira, **Universidade Nova de Lisboa – Brasil. Disponível em: https://run.unl.pt/bitstream/10362/20594/1/Pereira_2016.pdf. Acesso em Setembro de 2017.**

Talyta Singer², **Simpósio em tecnologias digitais e sociabilidade – Práticas Interacionais em Rede – Salvador. Disponível em: https://s3.amazonaws.com/academia.edu.documents/37718997/SimSocial-44965.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1505599433&Signature=aW%2Bg0R6ApBVgOg4D4XnVHm2KXfg%3D&response-content-disposition=inline%3B%20filename%3DInternet_das_coisas.pdf. Acesso em Setembro de 2017.**

DINO, **A internet das Coisas precisa avançar na Segurança como avança na inovação. Disponível em: http://www.comunique-se.com.br/release.aspx?title=a-internet-das-coisas-precisa-avancar-na-seguranca-como-avanca-na-inovacao&releaseid=138888&partnerid=11&. Acesso em Setembro de 2017.**

Vert, **São Paulo - R. Luigi Galvani 42, conjuntos 25 e 26 Edifício Berrini Sul Brooklin Novo. Disponível em:http://www.vert.com.br/quem-somos/localizacao/. Acesso em Setembro de 2017.**

Cassio Brodbeck, **OSTEC Business Security – Brasil. Disponível em: http://cio.com.br/opiniao/2017/04/24/internet-das-coisas-cinco-medidas-de-seguranca/. Acesso em Setembro de 2017.**