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

1.1. 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.

1.2. 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.

1.3. Objetivos

1.3.1. Objetivo Geral

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

1.3.2. 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

1.4. 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.

2. CONCEITOS BÁSICOS

2.1. 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.

2.2. 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.

2.3. 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.

3. TRABALHOS CORRELATOS

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

3.1. 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.

3.2. 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 devices à 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".

3.3. 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".

3.4. 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.

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.

-Sônego A , Marcelino R, Gruber V, "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.