SEGURANÇA NO CONTEXTO DE INTERNET DAS COISAS

Fabíola Maria Kretzer – 16100725
Aluna da disciplina INE5414 – Redes de Computadores I
do Departamento Informática e Estatística da Universidade Federal de Santa Catarina
Florianópolis, 12 de Agosto de 2017

Resumo

Será abordado sobre uma tecnologia que está cada vez mais presente no cotidiano das pessoas, a Internet das Coisas (IoT). Este tema foi escolhido por conta da importância que os dispositivos inteligentes vem tomando na vida das pessoas. Um ponto crucial a se ressaltar é que cada dia o ser humano está ficando mais dependente de tecnologias, que já são pensadas pelos pesquisadores para satisfazer as necessidades dos que usam. Essa é uma revolução tecnológica com a finalidade de que cada vez mais equipamentos como eletrodomésticos e meios de transporte sejam conectados a Internet e até mesmo a outros dispositivos, como smartphones e computadores. Mas a IoT traz enormes desafios para sua implementação no mundo real. Um desses desafios é a questão de segurança e privacidade. Este artigo foi escrito com o intuíto de comparar e analisar os trabalhos que já foram feitos ou estão em execução e ainda comentar possíveis propostas para que os dados que circulam na estejam cada vez mais seguros.

1. Introdução

1.1. Motivação

Com a queda de preços de sensores, vem ocorrendo a popularização dos serviços de armazenamento remoto e a big data. A facilidade de acesso a esses recursos também tem fortalecido uma tendência que está cada vez mais presente em nossas vidas: o IoT (Internet of Things). Como o

ser humano está sempre evoluindo, há a busca constate por tecnologias para melhorar a qualidade de vida do ser humano, mas a segurança não evoluiu, e as pessoas devem tomar muito cuidado na utilização desses dispositivos, pois podem se tornar perigosos e acabar com a privacidade das pessoas que as utilizam.

1.2. Justificativa

A IoT tem causado muitas transformações na vida das pessoas e das empresas, que cada vez mais estão interligadas com a Internet das Coisas, isso significa que mais informações pessoais e de negócios serão passadas na nuvem e, com isso, surgem novos riscos de segurança e tipos de ataques. Assim com o aumento da automatização de serviços essenciais, dados pessoais são transferidos para os dispositivos com acesso à internet, aumentando a vulnerabilidade e precisando aumentar a segurança na medida com que as informações na nuvem crescem.

1.3. Objetivos

1.3.1. Objetivos específicos

A Internet das Coisas é um novo paradigma que envolve muitas aplicações e possui um impacto muito grande na privacidade das pessoas. Assim, objetivo desse artigo é entender as vulnerabilidades e desenvolver ideias e aplicações que podem melhorar a segurança dessa tecnologia. Como objetivo secundário, este artigo traz algumas explicações sobre computação em nuvem (cloud computer). Este por sua vez que é um dos pilares para IoT, pois é através da nuvem que os dispositivos inteligentes são interligados.

1.3.1. Objetivos gerais

- Apresentar dificuldades em solucionar as vulnerabilidades em IoT.
- Apresentar ideias atuais e futuras para aumentar a segurança na Internet das Coisas.
- Apresentar alguns conceitos de Fog que são importantes para entender Internet das Coisas.

1.4. Organização do artigo

O presente artigo encontra-se organizado da seguinte forma: na seção 2 serão discutidos os principais conceitos de Internet das Coisas com ênfase na parte de segurança e de algumas dificuldades atuais. Também será explicado o conceito de computação em nuvem, muito importante no contexto IoT. Na seção 3 serão apresentados alguns trabalhos correlatados com o tema deste artigo. Na seção 4 serão apresentados alguns aspectos relevantes sobre segurança no contexto de Internet das coisas. Na seção 5 serão citados problemas existentes nesta área. Na seção 6 serão discutidas possíveis soluções que podem ser implantados. Na seção 7 será comentado projetos e desenvolvimento de uma ou mais propostas para melhorar a segurança desta área. Na seção 8 serão apresentadas algumas conclusões e trabalhos futuros, que poderão ser realizados sobre este tema.

2. Conceitos básicos

Nas próximas subseções são apresentados alguns conceitos abordados no contexto do artigo.

2.1. Internet das Coisas (IoT)

Internet das Coisas é um conceito tecnológico que interliga objetos do cotidiano das pessoas com a internet. Tem como finalidade facilitar a vida das pessoas, fazendo com que tarefas diárias possam ser feitas com a ajuda de um dispositivo. As aplicações podem envolver desde a área da saúde, até organização pessoal. É um conceito que está sendo capaz de mudar o jeito como o ser humano vive, pensa e trabalha. Funciona com o uso de sensores inteligentes e software que transmitem dados por rede, assim várias coisas estão conectadas e se comunicam umas com as outras e também com o usuário, possibilitando a troca de informações via internet. Há alguns anos poderia se pensar que era apenas uma utopia ou um delírio de alguns pesquisadores que defendiam esse assunto. Mas vem evoluindo muito e hoje já é realidade em muitas partes do mundo. Como em casas inteligentes que tem uma conexão entre vários eletrodomésticos, e possui software responsável por gerenciar toda a casa e ainda podem estar conectados com outros lugares, tornando-se uma cidade inteligente, que por exemplo, avisa o supermercado que a geladeira está vazia, para entregar mais comida ou que avisa o caminhão do lixo que a lixeira está vazia, para ir coletar, e muitas outras coisas simples do cotidiano que podem ser automatizadas.

Segundo o autor Rolf H. Weber (2010), a Internet das coisas (IoT) é uma internet global emergente baseada na arquitetura da informação que facilita a troca de bens e serviços em redes de suprimentos globais. E tem o objetivo de fornecer uma infraestrutura de modo a facilitar o intercâmbio de “coisas” de forma segura e confiável. Pode-se dizer que o amadurecimento dessa

nova tecnologia se deve ao fato do barateamento de sensores, que é a base para um sistema inteligente funcione.

2.2 Computação em nuvem

A computação em nuvem refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet. O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem.(Wikipédia)

Figura 1 – Esquemático de computação em nuvem

Fonte:<https://pt.wikipedia.org/wiki/Ficheiro:ComputaC3%A7%C3%A3o_em_nuvem.svg>

Mesmo sem perceber as pessoas estão utilizando a computação em nuvem, seja utilizando um serviço online como e-mail, jogos e vídeos ou armazenando arquivos. Há alguns anos, a aposta era

a de que ninguém mais precisaria instalar programa algum em seu computador para realizar desde tarefas básicas até trabalhos mais complexos, pois tudo seria feito pela internet. (Danilo Amoroso, 2012)

2.3 Segurança em IoT

A segurança em IoT está ligada a proteção dos dados de seus usuários. Na medida do aumento no uso de Internet das Coisas, mais informações pessoais e de negócios são passadas na nuvem. Assim, surgem cada vez mais problemas relacionados a segurança desse novo paradigma, pois essa tecnologia cresceu mas a segurança que está ao redor dela, não.

Para o autor Paulo Gaona-García (2017), a necessidade de criar redes que interagem com dispositivos ligados à internet, privacidade e a proteção de dados é substancial. Portanto, a segurança da informação é um aspecto bem conhecido, devido a dispositivos conectados à internet estarem crescendo rapidamente, o que representa um aumento de exposição nos dados na rede.

Seema Nath e Subhranil Som (2017) também ressaltam questão de que a confidencialidade dos dados privados dos usuários devem ser assegurados, uma vez que os dispositivos também está gerenciando informações confidenciais.

Um dos problemas diz respeito à “atribuição de tags a objetos que pode não ser conhecida por usuários, e pode não haver um sinal acústico ou visual para chamar a atenção do usuário do objeto. Por isso, indivíduos podem ser seguidos sem que eles saibam disso e deixar seus dados ou, pelo menos, seus vestígios no ciberespaço. Mais agravando o problema, não é mais apenas o estado que está interessado em colecionar os respectivos dados, mas também atores privados, como empresas de marketing.”(Rolf H. Weber, 2010)

3. Trabalhos Correlatos

3.1 Primeiro trabalho correlato

Os autores Gaona-García, Montenegro-Marin, Prieto e Nieto (2017) apresentam em seu artigo “Analysis of Security Mechanisms Based on Clusters IoT Enviroments” uma análise da revisão sistemática de artigos sobre Internet das Coisas (IoT), aspectos de segurança como privacidade e controle de acesso e também analisa questões de segurança que devem se abordados e identificados nesse novo paradigma. Também é apresentado o estado da arte com ênfase em segurança da Internet

das Coisas, alguns aspectos envolvidos, análise de alguns conceitos e segurança no desempenho. É relatado neste artigo um sistema de segurança que propõe neutralizar vulnerabilidades no IoT utilizando PKI que permitem autenticação de identidade baseada em uma chave pública combinada, dando solução para a quantidade excessiva de autenticações. Ao analisar o reconhecimento de impressão digital, foi proposto um modelo com três camadas; sensor, transporte e aplicação, permitindo assim poder analisar cada camada de forma separada. É proposto também um sistema RFID ligada com uma memória junto com um micro-chip, com o objetivo de receber sinais e devolver com alguns sinais à mais. Atualmente uma das medidas chave na a segurança em IoT a proteção de informações que viajam através da Internet. Na maioria dos casos, esta informação viaja através de redes sem fio ou através de redes públicas, que são vulneráveis a serem atacadas. Se o canal de comunicação não estiver adequadamente protegido por criptografia os dados, podem serem fáceis para um invasor realizar ataques. Assim, as pessoas que atacam a rede podem obter toda a informação que querem e ainda alterar o comportamento ou o desempenho do dispositivo. Para o futuro, estão previstos a cara caracterização de problemas envolvendo Internet das Coisas para que agentes inteligentes possam realizar a identificação adequada dos problemas que acontecem com mais problemas e assim facilitar a identificação de segurança e melhorar a sua implantação na resolução de problemas.

3.2 Segundo trabalho correlato

Segundo os autores Patra e Udai (2016) em seu artigo “Internet of Things—Architecture, applications, security and other major challenges” os equipamentos físicos equipados com sensores atuam no poder da computação. Para ele o conceito de Internet das Coisas é uma noção de “objetos inteligentes” que precisam de sensores conectado a microprocessadores para funcionar. Para os autores esses “objetos inteligentes” estarão no futuro em várias áreas, como a saúde, a automação residencial, o transporte, entre outros, assim estes dispositivos coletam dados, os analisam e iniciam ações, dependendo do ambiente ondo estão instalados. Apesar de a IoT trazer muitos benefícios para as pessoas que utilizam esse sistema o artigo discute vários desafios e ameaças de segurança. O estado atual da Internet está passando por uma revolução que trará sob suas redes transparentes de objetos inteligentes interconectados cada a capacidade de reunir informações e interagir com o mundo real e fazer uso da internet existente. Essas coisas inteligentes prestam ajuda e exigem grande quantidade de dados pertencentes ao usuário. Os dados pessoais recolhidos por estes sistemas são habilitadas pelo sensor devido ao monitoramento contínuo do ambiente de implantação que podem representar sérias ameaças à privacidade e à segurança dos usuários. A presença dessas vulnerabilidades no IoT exige atenção imediata dos pesquisadores na busca de métodos para

proteger a privacidade dos dados pessoais. Apesar de a IoT misturar o mundo real e o virtual de forma perfeita os autores estão preocupados com o aumento da insegurança e das vulnerabilidades nessa tecnologia e afirmam que se continuar a aumentar pode ofuscar muitos os benefícios da Internet das Coisas.

3.3 Terceiro trabalho correlato

Segundo os autores Sicari, Rizzardi, Grieco e Coen-Porisini em seu artigo “Security, privacy and trust in Internet of Things: The road ahead” no cenário da Internet das Coisas a satisfação dos requisitos de segurança e privacidade é fundamental para essa nova tecnologia. Esse requisitos podem incluir confiabilidade dos dados, controle de acesso pela rede IoT, privacidade e confiança dos usuários com os objetos e políticas de privacidade. Para os autores são necessárias medidas flexíveis que são capazes de resolver ameaças de segurança que atacam a rede. A IoT se aproximou das pessoas rapidamente na última década por meio de tecnologias de sistemas de comunicação sem fio como RFID, WiFi, 4G, IEEE 802.15.x, entre outros que se tornou crucial na vida das pessoas. Os autores relatam que no ponto de vista lógico, um sistema IoT pode ser representado como uma coleção de dispositivos inteligentes que interagem em uma colaboração racional para cumprir um objetivo comum. As implementações da IoT podem adotar diferentes arquiteturas de processamento e comunicação, tecnologias e além metodologias de design, com base em seu alvo. Por exemplo, o mesmo sistema IoT poderia aproveitar as capacidades de uma rede de sensores sem fio (WSN) que coleta informações do ambiente em uma determinada área e um conjunto de smartphones em cima dos quais aplicativos de monitoramento corre. Os esforços de pesquisa estão voltados para enfrentar os problemas de segurança e privacidade na IoT e das tecnologias de comunicação em geral. Outro campo de pesquisa é o da segurança IoT em dispositivos móveis, que cada vez mais se difundem hoje pelo mundo. Muitos esforços foram (e estão sendo) gastos pelo mundo comunidade científica para melhorar sistemas abordados acima.

3.4 Quarto trabalho correlato

Segundo os autores Ahlmeyer e Chircu (2016) em seu artigo “SECURING THE INTERNET OF THINGS: A REVIEW” a próxima evolução da Intenet das Coisas é conectar bilhões de outros dispositivos para a Internet. Isso permitirá que as empresas coletem dados de seus clientes e produtos para melhorar a qualidade do atendimento e fazer uma maior organização das necessidades da empresa e do cliente, trazendo mais satisfação aos dois. Mas essa facilidade tem um preço, a insegurança. Especialistas na área dizem que apesar de ter grande importância nos negócios, a IoT

está atrasada quando se refere na implantação de medidas para a melhoria da segurança dos usuários. Uma análise dos autores, identifica três grandes problemas, a falta se segurança em implementações de IoT, a falta de diretrizes detalhadas e padrões de segurança em TI e a falta de leis e regulamentos referente a Internet das Coisas em nível nacional e internacional. O IoT utiliza tecnologias como identificação por radiofrequência (RFID) e sensores para conectar "coisas" no ambiente à internet. Neste contexto, uma coisa pode ser, por exemplo, o monitor de casa de alguém, um rastreador, um aparelho, uma máquina industrial ou um carro, que pode coletar dados sobre seu desempenho ou localização, salvá-lo e processá-lo localmente ou em um servidor e criar alertas com base em regras pré-definidas, como um carro que alerta o usuário quando a pressão do pneu é muito baixa. As projeções atuais indicam que o número de tais dispositivos conectados à IoT aumentará significativamente, mas a segurança relacionada com essa tecnologia, não. Isso traz muitos problemas ligados a privacidade. A pesquisa acadêmica futura pode avançar nossa compreensão dos conceitos relacionados a IoT, identificando barreiras técnicas e econômicas. As práticas de segurança da IoT e os desafios de desenvolver e adotar a segurança atualmente estão tentando descobrir maneiras de melhorar a privacidade.

3.5 Comparação com os trabalhos correlatos

O presente artigo está em nível survey, abordando o tema de segurança em dispositiovos IoT (Intenet das Coisas) e cloud computing (computação em nuvem). Assim sendo retratado conceitos básicos, aspectos que são necessários levar em consideração, problemas que estão presentes no âmbito de Segurança em Cloud Computing e Internet das Coisas, além de apresentar meios de tentar contornar os problemas existentes, apresentado soluções que possam ser usadas futuramente e elaborando uma proposta para melhorar a segurança e a sociedade ficar mais tranquila quanto a questão da vulnerabilidade apresentada nos dispositivos IoT. Para escrever este artigo foram necessárias realizar análises de conceitos envolvendo IoT, e pesquisas sobre informações que estão ligadas com este tema, pois engloba vários objetos e métodos de comunicação para trocar informações. Como base, foram utilizados algumas obras da literatura recente, tanto de pesquisadores que estão há anos trabalhando com essa tecnologia, quanto de pessoas comuns que só escrevem em seus sites apenas para informar os usuários dos riscos e problemas. Este artigo também explicou como fazer um framework incorporado a IoT, baseado no modelo descrito por Sachin Babar (2011) e adaptado pela autora.

4. Aspectos relevantes

A fascinante comunicação entre o mundo físico e o virtual torna tudo mais inteligente e prático. A Internet das Coisas tem um futuro muito promissor, pode ser usada nas casa e no mercado, por exemplo. Em pouco tempo, a tecnologia mudou a forma de agir, pensar e como o ser humano interage com o mundo a sua volta. Coisas que à alguns anos as pessoas faziam pessoalmente, nos dias atuais deixam para os dispositivos conectados à internet. Assim, falar de segurança nessa área ficou cada vez mais importante.

A tecnologia tem permitindo ao mundo muitas facilidades e benefícios, como conversar com pessoa que estão a quilômetros de distância, comprar mercadorias sem sair de casa e outras tantas coisas. Com isso surgem vários problemas com a segurança das pessoas. Atualmente existem protocolos de segurança, como criptografia, que está em constante aprimoramento, para evitar problemas. Mas as pessoas maudosas que querem informações para tirar proveito, conseguem desenvolver métodos cada vez mais eficientes para burlar os sistemas, assim surgindo novas vulnerabilidades.

A IoT permite uma transferência constante e compartilhamento de dados entre coisas e usuários para atingir objetivos específicos. Dentro um ambiente de compartilhamento, autenticação, autorização e o controle de acesso são importantes para assegurar uma comunicação segura. Neste contexto, a falta de recursos computacionais (isto é, poder de processamento, armazenamento) e a natureza de tais redes exige que hajam existente técnicas para este novo ambiente. (Sicari, Rizzardi, Grieco e Coen-Porisini, 2015)

Um ponto a se considerar é o aumento do uso da Internet das Coisas é o barateamento e o aperfeiçoamento dos sensores utilizados nos dispositivos ligados à rede, pois são necessários da IoT . Logo os usuários pagam cada vez menos para ter essa tecnologia em casa. O aperfeiçoamento de dá por conta de que no futuro os sensores, atualmente ligados por fio, poderão ser substituídos por sensores sem-fio melhorando o sistema quando é necessário fazer algumas mudanças no sistema. Além de poder fazer o transporte de sensores para uma melhor cobertura do lugar onde irá ser instalado.

Ainda é preciso observar outros aspectos, como a forma que as pessoas vão interagir, se acostumar e usar essa tecnologia. Para Evans (2011) a Internet das coisas (IoT) mudará tudo - incluindo nós mesmos. Isso pode parecer uma declaração ousada, mas considere o impacto que a internet já teve na educação, comunicação, negócios, ciência, governo e humanidade. Claramente, a Internet é uma das mais importantes e poderosas criações em toda a história humana. Agora considere que a IoT representa a próxima evolução da Internet, dando um grande salto na sua capacidade de reunir, analisar, distribuir e obter dados que possamos transformar em informação, conhecimento, e, finalmente, sabedoria. Neste contexto, o IoT torna-se imensamente importante. Mas é preciso

tomar cuidado, pois mentes maudosas podem utilizar esta tecnologia para tirar proveito de informações disponíveis na nuvem, que são guardadas com pouca segurança.

O lado humano é tão importante observar que Gabriela Kiryakova, Lina Yordanova e Nadezhda Angelova (2017) em seu artigo elas também consideram a reação das pessoas e como essas questões em que direção a Internet das Coisas levarão a mudanças nas atividades e processos educacionais têm muitas respostas e precisam de discussões e debates. A Internet das coisas tem potencial para mudar significativamente o processo educacional e as relações dos participantes. Pode afetar os processos de ensino e aprendizagem, incluindo as abordagens de criação de conhecimento e sua disseminação. A disponibilidade de dispositivos mais técnicos e tecnologias de acompanhamento ajuda a transformar a aprendizagem em um processo mais humano.

Outros aspectos a serem levados em consideração é a importância da cloud computing ou em português computação em nuvem. Pois para a Internet das Coisas funcionar a nuvem é muito relevante. Pois no meio IoT é necessário mover os aplicativos, gerenciar os sistemas, armazenar os arquivos que hoje em dia parece que tudo acontece na nuvem. Podemos dizer que a nuvem é algum lugar do outro lado da sua conexão de internet. Um lugar onde você pode acessar aplicativos e serviços, e onde os seus dados são armazenados de forma segura. Esta forma de pensar revolucionou a forma como as empresas e as pessoas consomem tecnologia por três motivos:

- Não é necessário nenhum esforço da sua parte para gerenciar ou dar manutenção em aplicativos.
- A nuvem é efetivamente infinita em tamanho, portanto você não precisa se preocupar em ficar sem capacidade.
- Você pode acessar aplicações e serviços baseados na nuvem de qualquer lugar - tudo o que você precisa é de um dispositivo conectado à internet. (Blog da Salesfore Brasil – 2016 - Adaptado)

5. Problemas existentes

Um dos maiores problemas que a Internet das Coisas enfrenta atualmente é a falta de segurança dos dados que circulam na nuvem, pois esses dados importantes podem ser interceptados e usados de forma maligna. O autor Gaona-García (2017) diz no seu artigo que a intercepção de dados é real e possível, isso pode ser uma prova graças a estudos que tenham gerenciado dispositivos ativadores de limpadores de para-brisas e freios de carros somente através de texto, mensagens, manipulação de dispositivos eletrônicos do veículo, rastreamento sistema de navegação do veículo, anulação do sistema de navegação de um iate de luxo encalhado no meio do mar, entre outros. Falando de computação em nuvem é difícil satisfazer os requisitos de privacidade do cliente.

Com esses estudos alguns problemas podem ser destacados:

I) Problemas de privacidade (onde você pode investigar os direitos seres humanos inerentes a este princípio).

II) Autorização insuficiente,

III) Falta de criptografia

IV) Interface web insegura

V) Software de proteção inadequada.

Outro problema é que os nós inteligentes são implementados para extração de informações confiáveis dos arredores. Quando se faz isso a rede a alcança um sistema de proteção contra falhas. Mas a implantação de um número tão grande de dispositivos faz com que haja a sobrecarga do sistema.

Segundo o autor Patra (2016), um desafio sério para a IoT é a grande quantidade de energia que esse sistema consome, pois precisa de monitoramento contínuo e coleta de dados pelos dispositivos. Além disso, a transmissão dos dados coletados por estes dispositivos para o ponto de controle através do meio sem fio requer mais poder em comparação com a transmissão com fio.

Para Weber (2010), o Transport Layer Security (TLS), com base em uma estrutura de confiança, também poderia melhorar a confidencialidade e integridade no IoT. No entanto, como cada etapa requer uma nova conexão TLS, assim a busca de informações seria afetado negativamente por muitas camadas adicionais.

Segundo Evans (2011), para que a IoT atinja todo seu potencial, os sensores precisarão ser auto-sustentáveis. Imagine mudar as baterias em bilhões de dispositivos implantados em todo o planeta e até mesmo no espaço. Obviamente, isso não é possível. Além do mais, pode trazer graves problemas para o planeta. O que é necessário é uma maneira de os sensores gerarem eletricidade a partir de elementos ambientais, como vibrações, luz e fluxo de ar.

Para Evans (2011) outro problema que impacta na Internet das Coisas é o endereço IP. O mundo ficou sem os endereços IPv4 em fevereiro de 2010. O impacto geral foi visto pelo público em geral, o que pode potencialmente diminuir o progresso da IoT, já que os potenciais bilhões de novos sensores exigirão endereços IP únicos. Além disso, o IPv6 facilita o gerenciamento de redes devido a capacidades de configuração automática e oferece recursos de segurança aprimorados. Embora tenham sido feitos muitos progressos na área de padrões, é necessário mais, especialmente nas áreas de segurança, privacidade, arquitetura e comunicações. O IEEE é apenas uma empresa que trabalha

para resolver esses desafios, assegurando que os pacotes IPv6 possam ser encaminhados em diferentes tipos de rede.

Outro problema no ambiente tecnológico, mais precisamente no âmbito de cloud computing segundo o Blog Penso Tecnologia (2017), ocorreu no mês de fevereiro de 2017, que foi marcado por uma falha gigantesca, que afetou a internet do mundo todo: a queda do serviço de nuvem da Amazon, também conhecida como Amazon Web Services (AWS). Essa divisão da empresa controla 31% do mercado de infraestrutura em nuvem global. Com um problema em um servidor localizado na costa leste dos Estados Unidos, diversos sites e aplicativos, que contam com a plataforma AWS ficaram fora do ar ou com lentidão, afetando diretamente a rede de vários países.

Apesar de muito segura, a nuvem pode sim apresentar falhas de suporte, infra-estrutura ou processos, afinal, nada é 100% estável. Podem ocorrer problemas no sistema, no hardware, falha de energia-elétrica, queda da rede, contaminação por vírus, entre outros. Porém, não por muito tempo. Como dispõe de backup, dentre outros benefícios, corrigir uma falha da nuvem geralmente ocorre de modo rápido e fácil. (Blog Penso Tecnologia – 2017)

6. Soluções possíveis

Os métodos de gerenciamento de identidade resolvem problemas em relação à autenticação de dados e processos entre a nuvem e a comunicação sub-sequencial de dispositivos. Esse método ter um gerente de identidade que autentica os dados e encaminha-os para um serviço de gerencia para validar as instruções do serviço para ser realizado. (Kumar, 2016)

Outro método de segurança proposto é o jogo segurança adaptativa baseada em teoria para smart IoT, o Método de Cox que envolve o uso simulado de estratégias em que os computadores tomam decisões para desenvolver estratégias para prevenir, detectar e evitar ataques. Ele apresenta confiabilidade e análise de risco no rosto de ameaças. Outra possível solução seria a PKI-Like que envolve criptografia nas rotas dos nós para seus destinos e usando uma chave para decodificação e segurança. Os dados são enviados ao longo do caminho, que transmite a chave quando o nó atinge. (Kumar, 2016)

Sicari (2015) apresenta outro método de melhor a segurança em IoT é utilizar vários tipos de camadas middleware. Middleware é um programa de computador que faz a mediação entre software e demais aplicações. É utilizado para mover ou transportar informações e dados entre programas de diferentes protocolos de comunicação, plataformas e dependências do sistema operacional. Proporcionando integração e segurança de dispositivos e dados dentro da mesma rede de

informação. Desta forma os dados são trocados com rígidas restrições, tendo uma melhor proteção das informações passadas via rede. O lado negativo de implementar essa solução é pode não suportar o protocolo IP.

Outra alternativa usando middleware proposta no artigo de Sicari (2015) propõe uma arquitetura de segurança transparente IoT. Suas medidas de proteção baseiam-se em tecnologias existentes para a segurança, como AES (Advanced Encryption Standard, um protocolo de alto nível de segurança, mas que possui a desvantagem de exigir muito processamento), TLS (Transport Layer Security, um protocolo de criptografia projetado para internet) e oAuth (um protocolo de autorização que permite que websites terceiros acessem seus dados sem requerer que o usuário compartilhe informações). Desta forma, a privacidade, autenticidade, integridade e confidencialidade dos dados trocados sã integrados para fornecer segurança para objetos inteligentes e serviços.

Segundo Evans (2011), para o problema do uso de energia sustentável nos sensores houve um avanço significativo, os cientistas anunciaram um nanogenerador comercialmente viável - um chip flexível que usa movimentos corporais, como a pitada de um dedo para gerar eletricidade - no 241º Encontro Nacional e Exposição da American Chemical Society em março de 2011.

Wangham, Domenech e Mello (2013) falam de autenticação e autorização para sistemas distribuídos pervasivos e ubíquos como a IoT são temas de pesquisas atuais e ativos e, provavelmente, diante das suas complexidades e relevâncias, continuarão assim por muitos anos. Esta constatação decorre das inúmeras questões que os sistemas de gestão de identidades devem considerar, tais como: privacidade e anonimato do usuário, uso de algoritmos criptográficos fortes em dispositivos com restrições computacionais, autenticação única (SSO) de dispositivos diante de diferentes tecnologias, controle de acesso de granularidade fina e interoperabilidade semântica entre regras de autorização.

Segundo Wangham, Domenech e Mello (2013) apesar de existirem diversos trabalhos na literatura científica que descrevem soluções de segurança para IoT, vão surgindo novos problemas relacionados a computação em nuvem, por conta disso ainda é necessário superar uma série de desafios científicos e tecnológicos para que estas soluções sejam utilizadas e difundidas em sua forma plena.

Para o Blog Penso Tecnologia (2017) se proteger contra falhas na nuvem, é fundamental contar com um sistema de redundância – que é quando o servidor possui um segundo dispositivo de mesma função, disponível para entrar em ação em situações de falha. Complementar à redundância está o plano de contingência, que consiste em um conjunto de medidas de segurança preventiva, variando de acordo com as ameaças as quais sua nuvem pode estar exposta. Essas medidas devem ser adotadas caso ocorra a falha, definindo o que fazer para manter o servidor ativo.

Além disso o mesmo blog diz que para estruturar esse plano, alguns fatores devem ser levados em conta, como: análise de risco (item que prevê quais falhas podem ocorrer e a quais riscos a nuvem pode estar exposta), administração da crise (parte em que define como as equipes envolvidas na correção da falha devem se portar e o que fazer para corrigir o problema), continuidade de operações (define os procedimentos para reduzir o impacto e a disponibilidade da falha) e recuperação (iIndica como recuperar e restaurar as funcionalidades afetadas).

7. Projeto e desenvolvimento de uma proposta

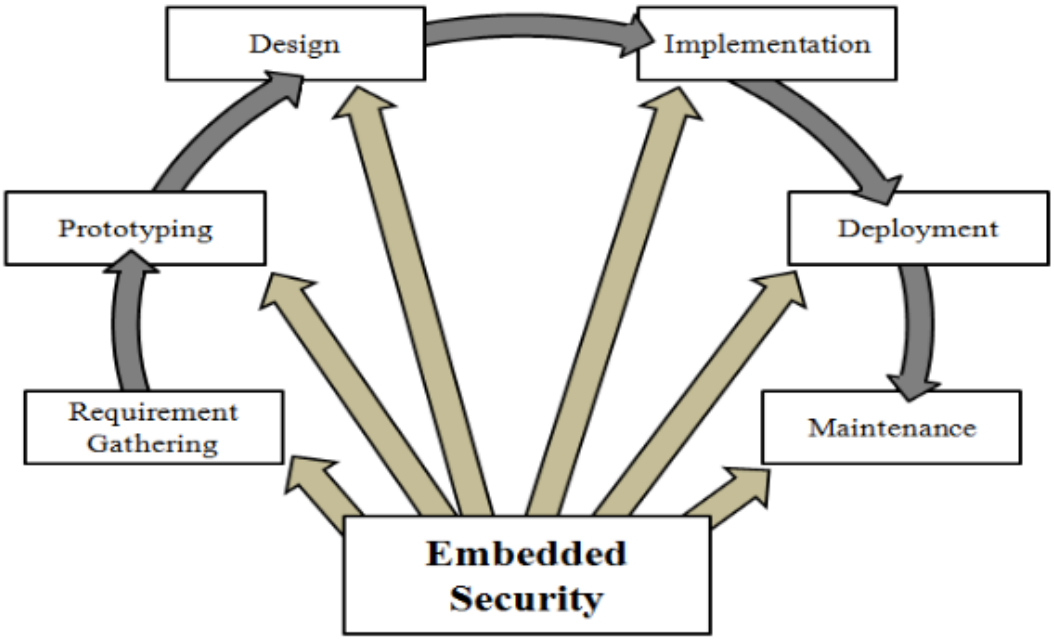
Para Sachin Babar (2011), o básico de segurança para construir um framework incorporado a IoT deve considerar as seguintes coisas:

1. Fator de meio ambiente: em relação ao ambiente em que os dispositivos funcionam, determina os pressupostos, ameaças, vulnerabilidades, ataques e políticas necessárias para o funcionamento seguro.
2. Objetivos de segurança: determine os objetivos de segurança do seu dispositivo. Considere os dados (ativos) ou operação que ele irá proteger e quais as ameaças da exigem.
3. Requisitos: determine seus requisitos de segurança funcional. A idéia básica para enquadrar a arquitetura de segurança para o IoT é, utilizando mecanismos de segurança e protocolos de forma eficaz, para começar com um projeto que leve em consideração a segurança da coleta de requisitos para a manutenção, seguindo o ciclo de vida do desenvolvimento de software.

Para construir o framework de segurança incorporado para o IoT, também precisamos analisar todas as compensações entre desempenho, custo e segurança. Infelizmente, esses três conceitos quase sempre estão em desacordo um com o outro. Mais desempenho significa que o custo aumenta, diminuir o custo significa diminuir a segurança e o desempenho. A proposta é uma arquitetura de segurança baseada em software de hardware para IoT, que deve ser o melhor custo / eficiência ou segurança / desempenho.

Um design econômico usa uma mistura de hardware e software para atingir os objetivos gerais de segurança. Isso fornece motivação suficiente para tentar uma abordagem orientada a síntese para alcançar implementações de sistema de segurança tendo componentes de hardware e software. Tal abordagem se beneficiaria de uma análise sistemática que seja comum em síntese, ao mesmo tempo que crie sistemas rentáveis.

Figura 2 – Etapas de projeto para o framework



Fonte:<https://www.researchgate.net/profile/Jaydip_Sen/publication/252013823_Proposed_Embedded_Security_Framework_for_Internet_of_Things_IoT/links/00b495278c92a797d9000000/Proposed-Embedded-Security-Framework-for-Internet-of-Things-IoT.pdf>

Seguindo os principais recursos do framework de segurança e arquitetura:

Criptografia leve: algoritmos criptográficos otimizados e arquitetura de hardware para requisitos de processamento, memória e processamento extremamente baixos.

Segurança física: módulo de plataforma confiável que levará em consideração as vulnerabilidades do dispositivo de hardware em nível físico.

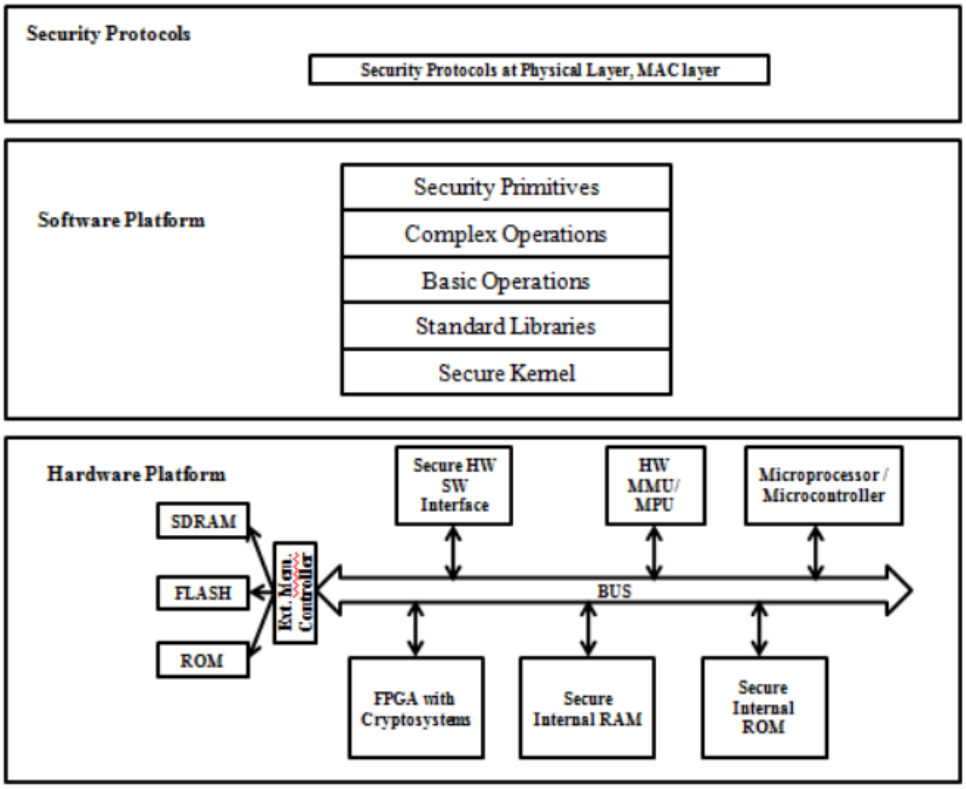
Protocolos de segurança padronizados: desenvolvimento de protocolos padronizados que são leves em relação à comunicação e aos cálculos criptográficos.

Sistemas operacionais seguros: sistemas operacionais ricos com um kernel seguro que assegure uma comunicação segura dentro do processador, fornecendo ambiente de execução de tempo de execução seguro, inicialização segura, conteúdo seguro, etc.

Áreas de aplicação futuras: Compreender o contexto técnico, econômico e social de uma determinada área de aplicação, a fim de desenvolver soluções de segurança adequadas e aceitáveis.

Armazenamento seguro: proteja as informações confidenciais armazenadas em RAM / ROM e armazenamento secundário.

Figura 3 – Estrutura do framework de segurança



Fonte:<https://www.researchgate.net/profile/Jaydip_Sen/publication/252013823_Proposed_Embedded_Security_Framework_for_Internet_of_Things_IoT/links/00b495278c92a797d9000000/Proposed-Embedded-Security-Framework-for-Internet-of-Things-IoT.pdf>

A arquitetura pode ser dividida em nível de hardware e software com protocolos padronizados leves que suportam na camada física. O nível de segurança dentro do dispositivo irá variar dependendo da natureza do conteúdo protegido e do tipo de aplicação. A arquitetura deve fornecer proteção física para chaves secretas, mantendo os componentes como ROM segura, que está manipulando as chaves secretas.

A segurança deve garantir que o dispositivo seja iniciado com o sistema operacional genuíno com privilégios de processo corretos. ROM seguro, ambiente de execução de tempo de execução seguro, unidade de gerenciamento de memória segura são o foco principal para a segurança incorporada. Também sistema operacional rico com funcionalidade de segurança necessária, interface de kernel segura e segurança padronizada compatível Os protocolos para o sistema IoT contribuirão para a arquitetura de segurança segura e o framework para o IoT.

A segurança incorporada para o IoT será crucial e importante com fortes mecanismos de segurança que evitarão danos e perdas econômicas que ofereçam novas oportunidades de negócios. Uma solução considera a segurança desde o início, desde o projeto até a implementação, para detectar as vulnerabilidades do nascimento à morte do sistema. Depois de descobrir as fontes e os motivos das

vulnerabilidades, alguns mecanismos devem ser incorporadas na metodologia de design. Uma estrutura e arquitetura de segurança incorporada depende de definições precisas de parâmetros como restrições de recursos, especificação de rede (protocolos, throughput, topologia, serviços, etc.) e especificações do sistema (protocolos, tamanho do dispositivo, serviço que são gerenciado, especificação multi-taxa, etc.). Isso fornecerá as informações necessárias para definir os limites entre a parte segura e insegura do sistema (níveis de dados e hardware). Um estudo adequado ao nível do sistema permitirá a seleção das soluções candidatas para as peças de hardware e software. Esses candidatos serão usados, juntamente com as especificações, como entradas para a metodologia de co-design de hardware / software que levará a uma estrutura de segurança e arquitetura para o sistema IoT. (Babar, 2011)

8. Conclusão e trabalhos futuros

As pesquisas atuais possuem várias abordagens sobre o tema Internet das Coisas. A primeiro momento a comunidade científica acredita que que IoT possui um potencial limitado, por consequência dos riscos que os usuários enfrentam, como a falta de segurança, roubo de identidade, falhas de dados e hackings que querem essas informações para usar contra as pessoas que tem seus dados roubados. Os desenvolvedores precisam considerar a segurança quando desenvolvendo novos produtos.

Como os dispositivos IoT estão focados principalmente no envio de informações entre dispositivos, ou deles para a Internet; uma das medidas-chave para ser tomado, seria a proteção de informações que viajam através da rede. Assim se o canal de comunicação não estiver adequadamente protegido por criptografia dados, pode ser fácil para um invasor realizar ataques. O hacking pode capturar o tráfego do cliente, corrigi-lo para fingir ser o originador disso, e enviá-lo para o servidor legítimo, de modo que ele atue como intermediário sendo invisível para ambos: a origem e o destino de trânsito. Podendo obter toda a informação que querem mesmo sem modificar desempenho do dispositivo. (Gaona-Garcia, 2017)

Embora os especialistas concordem com a segurança do IoT é extremamente importante, os desenvolvedores que trabalham nas empresas dessas áreas infelizmente estão lentos no quesito de implementar medidas de segurança IoT. Os principais requisitos de segurança estão em cinco áreas: níveis de segurança, atividades de segurança, cadeia de valor de segurança, padrões de segurança e educação de segurança. (Gaona-Garcia, 2017)

Como trabalho futuro, está previsto realizar uma caracterização destes problemas, de modo que agentes inteligentes podem realizar a identificação adequada dos mecanismos de segurança dos

problemas mais frequentes em clusters de aplicação de IoT. Este facilitaria a identificação de alternativas de segurança, o acesso à implantação modelo de dispositivos IoT. Podendo avançar a compreensão por parte dos pesquisadores, da técnica, barreiras econômicas e de adoção para as práticas de segurança do IoT e os desafios de desenvolver e adotar a segurança padrões. (Gaona-Garcia, 2017)

Para Kumar (2016) a articulação com mais e mais dispositivos baseados em IoT são conectados à Internet, resulta na extensão da área de superfície para ataques externos. O autor classifica esses ataques com base em camadas que compõem o IoT e discutiam vários desses ataques com exemplos. Também examinam as literaturas sobre os métodos existentes para proteger a IoT e sua infra-estrutura e resumiu esses métodos de segurança sobre como abordam os problemas de segurança no IoT. As limitações existentes nos métodos de segurança e futuro proposto trabalhos recomendações para superar essas limitações, dentro da ordem para os clientes abraçar a IoT e as aplicações, esta privacidade e problemas de segurança e a limitação das necessidades precisam ser abordadas e implementadas imediatamente, de modo que o potencial da tecnologia IoT e suas aplicações podem ser realizadas.

Os pesquisadores também podem estudar como incorporar explicitamente considerações de segurança em estruturas de modelos de negócios para IoT. A partir de um perspectiva prática, as empresas focadas no mercado IoT e seus funcionários precisam entender a extensão dos riscos de segurança da IoT e as possíveis soluções, e começar a implementar essas soluções e teste sua eficácia. Em última análise, acredita-se que a ação conjunta por parte de os fornecedores de soluções IoT, empresas que utilizam dispositivos IoT, empresas de consultoria, reguladores e instituições educacionais serão necessários para colocar a segurança na vanguarda da conversação do IoT e desenvolver soluções de segurança concretas para IoT. (Ahlmeyer, 2016)

Para os autores brasileiros Michelle, Marlon e Emerson (2013) as características diferenciadas e muitas vezes restritivas da IoT, como a sua natureza distribuída, a facilidade de acesso físico aos objetos e os objetos com recursos computacionais restritos, tornam o provimento da segurança um desafio. Analisando a segurança na Internet das Coisas, dando foco aos aspectos de autenticação e autorização neste cenário, pois os dispositivos na IoT geram, transmitem, modificam e armazenam dados constantemente, sendo que estas informações muitas vezes são confidenciais para seus usuários. Essas informações que estão vulneráveis na nuvem podem ser usados contra os usuários que tem seus dados roubados. Estes dispositivos podem pertencer a mais de uma rede e podem de se deslocar por mais de um domínio, o que afeta as abordagens de autenticação e de controle de acesso.

Referências Bibliográficas

[1] GAONA-GARCÍA, Paulo et al. Analysis of Security Mechanisms Based on Clusters IoT Enviroments. 2017. International Journal of Interactive Multimedia and Artificial Intelligence. Disponível em: <http://www.ijimai.org/journal/sites/default/files/files/2016/08/ijimai20174_3_8_pdf_20224.pdf>. Acesso em: Agosto 2017.

[2] Nath, Seema, and Subhranil Som. "Security and Privacy Challenges: Internet of Things." *Indian Journal of Science and Technology* 10.3 (2017). Disponível em: <http://52.172.159.94/index.php/indjst/article/view/110642>. Acesso em: Agosto de 2017

[3] MAHYAR, Taj Dini; SOKOLOV, V. Yu. Internet of things security problems. **Сучасний захист інформації**, n. 1, p. 120-127, 2017. Disponível em: <http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/szi_2017_1_21.pdf>. Acesso em: Agosto de 2017

[4] Goeke, Lisa. "Security Challenges of the Internet of Things." (2017). Bachelor's Thesis Business Information Technology – Haaga-Helia University of Applied Sciences. Disponível em: <https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1> . Acesso em: Agosto de 2017

[5] Patra, Litun, and Udai Pratap Rao. "Internet of Things—Architecture, applications, security and other major challenges." *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. IEEE, 2016. Disponível em: <https://www.researchgate.net/profile/Udai_Pratap_Rao/publication/308886519_Internet_of_Things_-_Architecture_Applications_Security_and_other_Major_Challenges/links/57f4a16d08ae91deaa5ae4ed.pdf>. Acesso em: Agosto de 2017

[6] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." *System Sciences (HICSS), 2016 49th Hawaii*

International Conference on. IEEE, 2016. Disponível em: <http://tarjomefa.com/wp-content/uploads/2016/09/5288-English.pdf>. Acesso em: Agosto de 2017

[7] Ahlmeyer, Matthew, and Alina M. Chircu. "SECURING THE INTERNET OF THINGS: A REVIEW." *Issues in Information Systems* 17.4 (2016). Disponível em: <http://www.iacis.org/iis/2016/4_iis_2016_21-28.pdf>. Acesso em: Agosto de 2017

[8] SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, v. 76, p. 146-164, 2015. Disponível em: <http://tarjomefa.com/wp-content/uploads/2016/07/5009-English.pdf>. Acesso em: Agosto de 2017

[9] WEBER, Rolf H. Internet of Things–New security and privacy challenges. **Computer law & security review**, v. 26, n. 1, p. 23-30, 2010. Disponível em: <https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf>. Acesso em: Agosto de 2017

[10] AMOROSO, Danilo, O que é computação em Nuvem?, 2012. Disponível em: <https://www.tecmundo.com.br/computacao-em-nuvem/738-o-que-e-computacao-em-nuvens-.htm>. Acesso em: Agosto de 2017

[11] EVANS, Dave. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. CISCO white paper, v. 1, p. 1-11, 2011. Disponível em: <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: Outubro de 2017.

[12] KIRYAKOVA, Gabriela; YORDANOVA, Lina; ANGELOVA, Nadezhda. Can we make Schools and Universities smarter with the Internet of Things? Tem Journal.,p. 80-84. fev 2017. Disponível em: <http://www.temjournal.com/content/61/TemJournalFebruary2017_80_84.pdf>. Acesso em: Outubro de 2017.

[13] WANGHAM, Michelle S; DOMENECH, Marlon Cordeiro; MELLO, Emerson Ribeiro de. Infraestruturas de Autenticação e de Autorização para Internet das Coisas. Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais SBSeg, 2013, p. 156-205. Disponível em:

<https://www.researchgate.net/publication/263161591_Infraestruturas_de_Autenticacao_e_de_Autorizacao_para_Internet_das_Coisas>. Acesso em: Outubro de 2017.

[14] Babar, Sachin, et al. "Proposed embedded security framework for internet of things (iot)." *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. IEEE, 2011. Disponível em: <https://www.researchgate.net/profile/Jaydip_Sen/publication/252013823_Proposed_Embedded_Security_Framework_for_Internet_of_Things_IoT/links/00b495278c92a797d9000000/Proposed-Embedded-Security-Framework-for-Internet-of-Things-IoT.pdf>. Acesso em: Outubro de 2017.

[15] Blog da Salesfore Brasil. O que é Cloud Computing? Entenda a sua Definição e Importância (2016). Disponível em: <https://www.salesforce.com/br/blog/2016/02/o-que-e-cloud-computing.html> Acessado em: Novembro de 2017

[16] Blog Penso Tecnologia. Como lidar com problemas na cloud? (2017). Disponível em: < https://www.penso.com.br/como-lidar-com-problemas-na-cloud/> .Acesso em: Novembro de 2017.