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.
- Identificar problemas existentes nessas áreas.
- Apresentar possíveis soluções aos problemas.
- Fornecer uma visão geral sobre o tema apresentado.

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 apresentadas e o estado da arte entre essas tecnologias. A seção 4 apresenta os aspects relevantes identificados sobre o tema. Seção 5 destaca alguns dos principais problemas enfrentados na segurança em IoT, Fog computing e Edge Computing. A seção 6 traz as principais propostas para solucionar os problemas identificados. Na seção 7, um projeto e desenvolvimento de uma proposta é abordado. Na seção 8 concluímos nosso trabalho, fazendo algumas obeservações e indicando possíveis trabalhos futuros.

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. A IoT pode ser caracterizada como uma rede mundial de coisas/objetos/dispositivos interconectados que se comportam como entidades ativas.
Algumas variações de entendimento existem em função de limites nacionais. Enquanto na Europa e na China o termo Internet das Coisas é bem aceito, nos Estados Unidos as referências mais frequentes são smart objects,smart grid e cloud computing (KRANENBURG et al, 2011) e refletem diferentes linhas de pesquisa e inovação.
O termo Internet of Things (IoT) foi introduzido primeiro para a comunidade de tecnologia emreferência ao gerenciamento automatizado da cadeia de suprimentos. O conceito de permitir que um computador “sentir” as informações de sentido sem intervenção humana foram então aplicado a outros campos, como saúde, tecnologia doméstica, engenharia ambiental e transporte.

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.
Fog Computing é uma plataforma altamente virtualizada que fornece serviços de computação, armazenamento e rede entre dispositivos finais e centros tradicionais de dados de computação em nuvem, tipicamente, mas não exclusivamente na borda da rede.
Os dispositivos de névoa incluem dispositivos de usuários finais, pontos de acesso, borda roteadores e switches. O paradigma do Nevoeiro está bem posicionado para grande análise de dados em tempo real, suporta dados densamente distribuídos, pontos de coleta e oferece vantagens em entretenimento, publicidade, computação pessoal e outras aplicações.

2.3. Edge Computing

Os dados são cada vez mais produzidos à beira da rede, portanto, seria mais eficiente também processar os dados ema borda da rede.
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.

3.5. Comparação com trabalhos correlatos

Neste artigo foram realizadas análises dos conceitos que envolvem IoT, Fog e Edge englobando os vários objetos e métodos de comunicação para trocar informações, dando uma visão de geral das principais características de IoT, Edge e FoG assim como os seus principais desafios, em especial a segurança feitas nessas áreas. No artigo apresentamos um framework que possibilita uma troca de mensagens mais segura e a garantia de entrega da mensagem. Como citado nos trabalhos correlatos um dos principais problemas seria a privacidade, integridade, confidencialidade, identificação e confiança das trocas de informações. Os autores dos trabalhos identificam os problemas e nos mostram possiveis soluções como algumas apresentadas neste artigo. A preocupação dos autores também cai sobre os ataques que podem ser feitos aos dispositvos e neste artigo apresentamos uma possivel solução para autenticação.

4. Aspectos Relevantes

A Internet das coisas rcebeu atenção durante anos e é considerada o futuro da internet. Os dispositivos da Internet das coisas têm de processamento de recursos energéticos e que não permitem complexo, processamento de dados no local limitado. Entretanto, devido ao limitado espaço de armazenamento em dispositivos “smarts”, Cloud Computing é considerada tão promissora quanto pois pode fornecer recursos elátiscos para aplicações nesses dispositivos. A Nuvem oferece capacidades de processamento virtualmente ilimitadas e um modelo de uso *on-demand* . Apesar das tentativas de aumento do uso de aplicações IoT com o poder da Cloud, diversos problemas surgem, pois aplicações IoT necessitam letência baixa, suporte de mobilidade e consciência de localização. Então vem a Fog computing que propôs fornecer computação diretamente na borda de rede, assim podendo entregar novas aplicações e serviços especialmente para o future da Internet

A computação na borda de rede pode render muitos benefícios. Por exemplo, pesquisadores mostraram que o uso de Cloudlets para descarregar tarefas de computação para usar sistemas de assistência cognitiva, melhora tempos de resposta entre 80 e 200 ms e reduz a energia de consumo em 30 a 40%. A tecnologia CloneCloud reduz o tempo de resposta e uso de energia em 95% para aplicações testadas via edge computing.

A IoT se difere das redes de computadores tradicionais em inúmeros aspectos

[Atzori et al. 2010]. Por exemplo, sua escala é maior, sendo composta por centenas ou milhares de nós. Os avanços na miniaturização permitem que as coisas menores tenham cada vez mais a capacidade de interagir e se conectar [Wangham et al. 2013].

Cloud Computing está associado a um novo paradigma para a infra-estrutura de fornecimento de computação [Vaquero et al., 2008], onde o poder de processamento e os aplicativos são oferecidos como serviços.
Embora seja considerada uma nova tecnologia, suas origens remontam à década de 60, quando o cientista da computação John McCarthy previu que a computação seria organizada como um serviço de utilidade pública [Garfinkel, 1999]. Desde então, o uso intensificado da Internet e o surgimento de novas tecnologias permitidas à Cloud Computing oferecem uma ampla gama de serviços, incluindo virtualização de recursos informáticos, desenvolvimento de software e finalização,aplicações de usuários de vários tipos. Esta variedade contribui para a existência de diferentesdefinições do que é Cloud Computing, cada um focado em características específicas.
Com a implementação do IoT agora cada vez mais difundida, estamos entrando na era pós-nuvem, em que dispositivos irá gerar muitos dados no final da rede e Muitas aplicações serão implantadas na borda para processar a informação.
A Cisco System preve que em 2020 um estimado de 50 bilhões de dispositvos estaão conectados à Internet.

5. Problemas existentes

5.1. Fog Computing

Devido a sua localização na borda da Internet, a rede de nevoeiro é heterogenea. O papel dela é conectar todos os componentes que estão no nevoeiro. Só que, controlar uma rede tão grande, manter conectividade e prover serviços sobre isso, especialmente no cenário de Internet da coisas em larga escolar, não é fácil.

5.2. Qualidade de serviço

Qualidade de service em Fog Computing pode ser dividida em 4 aspectos: 1- Conectividade, 2- Confiabilidade, 3- Capacidade e 4- Latência.

1) Conectividade: Em uma rede heterogenea de nevoeiro, retransmissão de rede, particionamento e agrupamento proporcionam novas oportunidades para reduzir custos, aparar dados e expander conectividade.
2) Confiabilidade : Normalmente, confiabilidade pode ser melhorada realizando um controle periódico para retomar após a falha, reprogramação de tarefas ou replicação de tarefas falhas para explorer a execução em paralelo. Mas controle

periódico e reprogramção pode não se encaixar muito bem em Fog Computing, pois sendo muito dinâmica ela terá latência e não poderia se adaptar a mudanças.

3) Capacidade : Os desafios vem de como projetar a interação entre nevoeiro e a nuvem para acomodar diferentes cargas de trabalho. Devido a alocação dinâmica de dados e a uma grande capacidade total em Fog Computing, nós também iriamos precisar redesenhar a busca motor que pode processar consulta de pesquisa de conteúdo espalhado em nodos do nevoeiro.
4) Latência: Aplicações sensíveis, como streaming, mineração ou eventos complexos de processamento, são aplicações que precisam de Fog Computing para prover um processamento de streaming em real-time ao invés de processamento em lote.

5.3. Segurança e privacidade

Na area de Edge Computong, segunraça e privacidade dos dados são os serviços mais importantes que deveriam sem providos. Se uma casa é implantada com IoT, muita informação privada pode ser utilizada analisando seus dados. Por exemplo, se uma pessoa ler os dados de consumO de água e eletricidade da casa, alguém pode facilmente especular se a casa está vazia ou não. Nesse caso, como prover serviços sem prejudicar a privacidade é um desafio.

Para proteger a segurança dos dados e a privavcidade na borda de rede, muitas desafios permanecem em aberto. Primeiramente é conscientizar a comunidade sobre a privacidade e a segurança. Pegando a segurança da rede WiFi por exemplo, entre os 439 milhões de usuários que utilizam conexões wireless, 49% das redes WiFi são inseguras e 80% ainda tem seus roteadores com senhas de fábrica. Para áreas públicas de WiFi, 89% delas são inseguras. Todas as partes interessadas deveriam avisar aos usuários que sua privacidade seria invadida sem aviso prévio na borda de rede.

Segundo é a propriedade dos dados coletados na borda. Justamente o que acontece com aplicações móveis, os dados do usuário final coletados são armazenados e analizados pelo lado do provedor de serviço. Entretanto, deixar os dados na borda onde ele é coletado e deixar o usuário ser total proprietário seria uma solução melhor para segurança de privacidade.

E por terceiro seria a falta de ferramentas eficientes para proteger a privacidade e a segurança de dados na borda de rede. O ambiente altamente dinâmico na borda de rede torna ela muito mais vulnerevel.

6. Soluções possíveis

Identificados problemas existentes, iremos abordar possíveis soluçõespara alguns desses problemas.

6.1 Autenticação

Atualmente existem poucos projetos focados na segurança e privacidade em FoG Computing. Um dos principais problemas sendo a autenticação, a PKI (Public Key Infraestructure); que é um conjuntos de funções politicias e procedimentos necessaries para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais e gerenciar a criptografia de chave pública; poderia resolver esse problema. Outro poderia ser a TEE (Trusted Execution Environment), que se trata de uma area segura do processador principal, ela garente que o código e os dados carregados dentro sejam protegidos em relação à confidencialidade e integridade.

6.2 Libsecurity

Libsecurity é um pacote abrangente que oferece aos desenvolvedores de aplicativos um conjunto de ferramentas de segurança completo, pequeno e provavelmente correto para endpoints e gateways/hubs. Isso inclui uma implementação leve e correta de vários módulos relacionados à segurança, incluindo armazenamento seguro, gerenciamento de usuários e senhas.

6.3 Latência em Edge Computing

Sabemos que o problema da latência ocorre pela forma como a Internet é projetada para operar e os protocolos que utiliza, especialmente o BGP (Border Gateway Protocol) e a Edge Computing pode minimizar este inconveniente. O Border Gateway Protocol (BGP) permite, em diversas situações, que a Internet se mantenha operante mesmo em casos de interrupções ao criar rotas alternativas. Porém, o sistema não é tão efetivo ao calcular quanto tempo um determinado pacote de dados vai demorar para chegar ao seu destino. Neste contexto a arquitetura de Edge Computing pode minimizar o problema de dois modos.

O primeiro é implementar uma série de computadores ao redor da Internet para fazer o cache do conteúdo, armazenando-o mais perto dos usuários que o consomem. Isto é esssencialmente o que fornecedores de CDN (Content Delivery Network) fazem.

Outro modo consiste na instalação pela empresa multinacional de pequenos Data Centers em diversos lugares do mundo, próximos a grandes concentrações de funcionários. Assim, é possível replicar todas as aplicações críticas e sensíveis a atrasos nestes Data Centers como, por exemplo, suítes de comunicação unificada que suportam voz, mensagens instantâneas e vídeo. O resultado final é um desempenho muito melhor devido à redução drástica da latência obtida devido ao acesso à data centers próximos da localização do usuário.

7. Projeto e Desenvolvimento de uma Proposta

Nesta seção abordaremos o FRI (Framework de comunicação seguro) desenvoldido pelo autor Moraes, L. C. D. O. (2016). As abordagens atuais para a Internet das Coisas se concentram principalmente em protocolos de comunicação para integrar “coisas” com padrões de protocolo na Internet considerando computação e memória recursos limitados, bem como a disponibilidade de largura de banda e disponibilidade de energia. O ambiente heterogêneo no contexto da Internet das

Coisas torna a comunicação indispensável. Os vários tipos de dispositivos na IoT muitas vezes tem recursos limitados de memória, processamento, armazenamento. De forma a resolver esses problemas, o FRI utiliza-se de protocolo voltado para o baixo consumo de recursos, provendo mecanismo de confiabilidade no envio da comunicação, e segurança na conectividade com a computação em nuvem visando fornecer uma maior capacidade de armazenamento dos dados e informações trafegadas pela rede para prover uma economia dos recursos dos dispositivos.

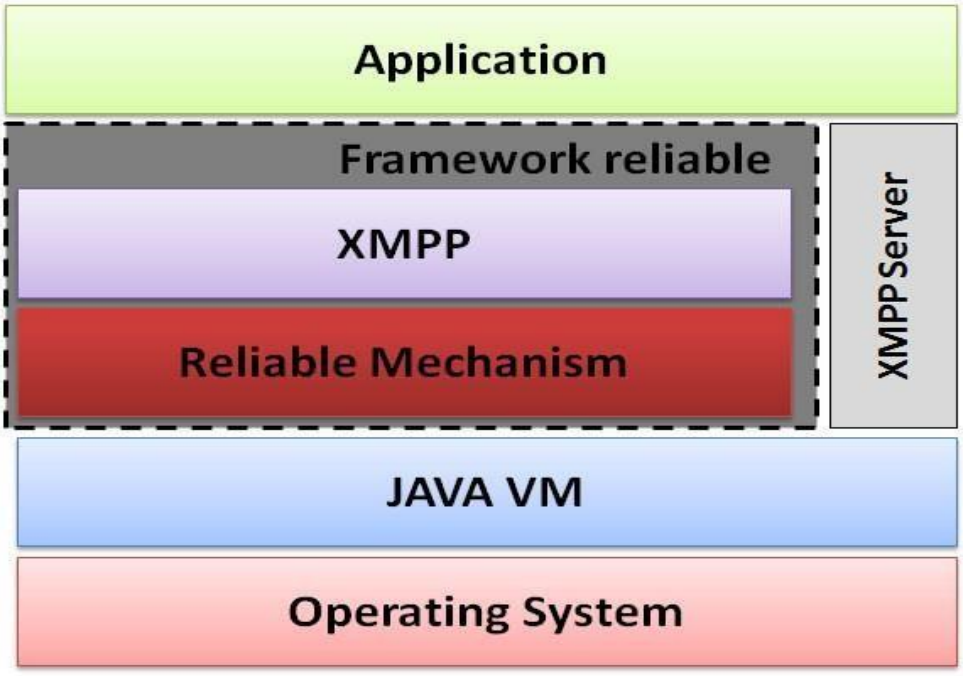
O FRI deve :

-Permitir um desenvolvimento simplificado e eficiente em termos de custos e implantação de serviços de comunicação em tempo real entre objetos;

- Realizar toda comunicação entre objetos de forma segura e confiável em termos de conexão;

- Deve apoiar a integração de aplicativos em dispositivos móveis e a Nuvem.

Dividimos o FRI em camadas, ilustrado através da abaixo, onde cada uma provê uma série de funcionalidades para as demais, provendo em conjunto a solução FRI. A divisão em camadas nos dá a oportunidade de visualizar as entidades centrais da solução.



-Na camada *Application* localiza-se as aplicações que dependem do ambiente no qual está empregado a solução, por exemplo aplicações de monitoramento de performance de equipamentos industriais, aplicações de controle de consumo

de energia, aplicações de temperatura (sensores no *datacenter*), etc.

-Na camada *Framework Reliable* localiza-se o *Framework* proposto composto pelo protocolo de comunicação XMPP Core definido pelo RFC 6120 (protocolo sem adição de extensões, apenas no formato do protocolo simples.

-Na camada *XMPP Server*, o servidor de comunicação em tempo real multi-plataforma baseada no protocolo XMPP é utilizado.

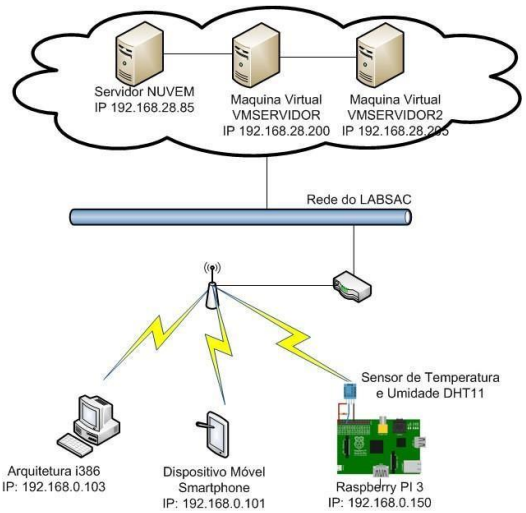
-Na camada *Java VM*, a arquitetura baseada em Java como núcleo sendo a linguagem utilizada para desenvolvimento do FRI é utilizada.

-No componente *Operating System*, plataformas típicas da Internet das Coisas, como TinyOS, Contiki, Raspbian podem ser utilizados.

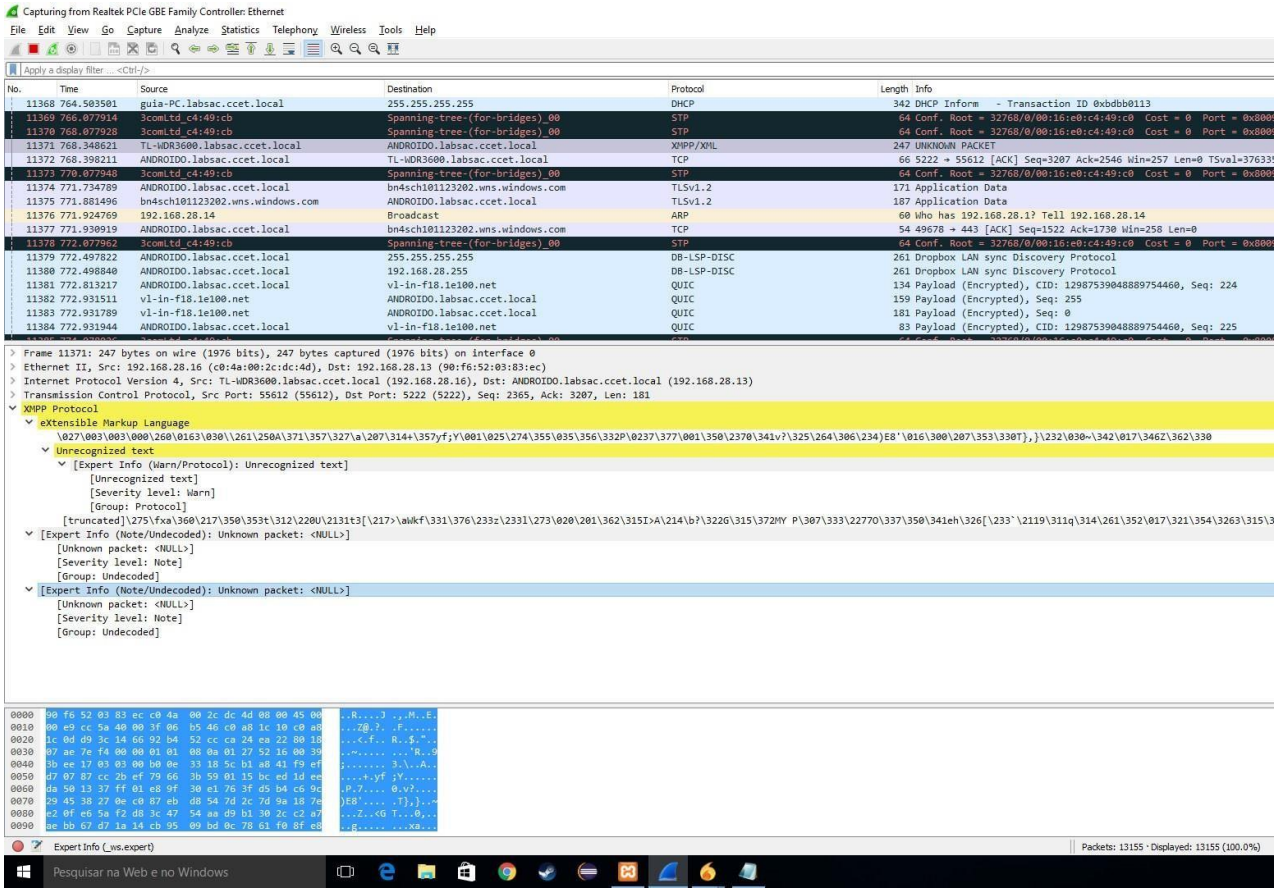
As principais funcionalidades do Framework seriam :

- Envio de mensagem com mecanismo seguro
- Controle da desconexão e reconexão com servidores
- Garantia de entrega de mensagem ao destinatário

Os testes foram feitos com os dispositivos inseridos conforme a Figura abaixo. A rede utilizada é LABSAC, em que os dispositivos Nuvem e VMSERVIDOR, estão conectados por uma rede virtual interna, o VMSERVIDOR possui um endereço IP externo para que haja a comunicação do *Openfire* com as aplicações desenvolvidas utilizando o FRI, que estão sendo executado no dispositivos Smartphone e PC, estes conectados via um roteador sem fio. Utiliza-se como sensor de temperatura e umidade o modelo DHT11 conectado na arquitetura do Raspberry PI 3 para obter os dados de leitura que foram utilizados nas aplicações desenvolvidas.



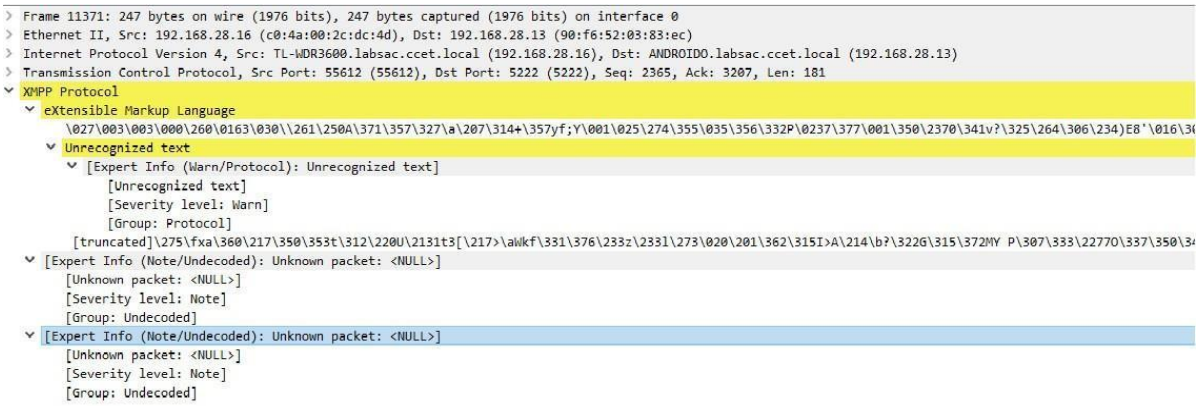
O Servidor *Openfire* inicializado no VMSERVIDOR é um servidor de colaboração em tempo real (RTC) licenciado sob a licença de código aberto Apache, multi-plataforma de comunicação em tempo real. Ele usa o protocolo aberto amplamente adotado pela comunidade que utiliza o protocolo XMPP.



Como teste da verificação do canal de criptografia foi utilizado o *software Wireshark versão 1.12.* Neste teste foi analisado o tráfego da rede no Ambiente de teste proposto acima. Podemos verificar na figura abaixo, a análise do protocolo XMPP encriptado, garantindo assim a confidencialidade e a

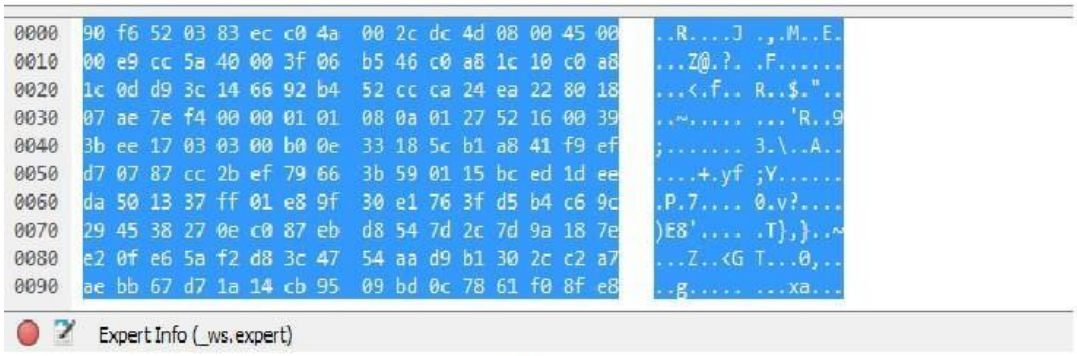
integridade e não-repudio .A figura mostra o conteúdo do pacote, onde neste caso está criptografado.

Na Figura abaixo mostramos os pacotes que estão trafegando pela rede, neste caso foi analisado um pacote de mensagem XMPP



b)

E na Figura abaixo mostramos o conteúdo do pacote, onde neste caso está criptografado.



c)

O framework pode ser implementado em varias aplicações e em diferentes cenários, são exemplos de aplicações que podem utilizar o FRI: sistemas de monitoramento de segurança, controle de temperatura de ambiente, gerenciamento de iluminação integrados, envio de dados de câmeras se segurança, envio de dados de alarmes contra incêndio, aparelhos de ar condicionado, lâmpadas e outros itens.

8. Conclusões e Trabalhos Futuros

Neste tabalho conseguimos concluir que a integração de IoT, FoG Computing e Edge Computing é inevitável. Mas devido a grande quantidade de dados processados e distribuidos, e a grande quantidade de usuários que fazem uso dessas tecnologias trazem um desafio aos provedores desses serviços : garantir a segurança, a confiabilidade e a privacidade dos dados transmitidos e armzenados nas redes utilizadas por IoT, Fog e Edge Computing. Essas três tecnologias vão evoluir rapidamente com cada avanço alcançado em casa uma delas, já que estão extremamente conectadas. Elas são extremamente promissoras só que necessitam muito mais trabalhos e pesquisas em relção a segurança e privacidade, pois atualmente são muito poucos.
O surgimento do IoT e dos dispotivos movéis universalizados mudaram o papel da edge no paradigma da computação do consumidor de dados ao produtor / consumidor de dados. Seria mais eficiente para processar dados na borda do rede. Neste artigo, surgiu o nosso entendimento da computação de borda, com a lógica de que a computação deveria acontecer na proximidade de fontes de dados.

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

A rede na borda apresenta desafios em relação a segurança e privacidade. Por exemplo, um hacker poderia aprender muito lendo dados que entram e saem de uma casa inteligente. Ao capturar eletricidade ou uso de água, o hacker poderia facilmente determinar se a casa provavelmente está desocupada e, portanto, vulnerável ao roubo. A falta de ferramentas eficientes é uma das desafios para proteger a segurança de dados e privacidade na borda da rede.

A infra-estrutura de um ambiente em nuvem é muito complexa. Essa complexidade se traduz em mais esforços necessários para monitorar e gerenciar a segurança. A maior escalabilidade e o tamanho maior das nuvens em relação às infra-estruturas tradicionais de hospedagem de serviços envolvem sistemas de monitoramento de segurança mais complexos, que, portanto, devem ser mais escaláveis, robusto e eficiente.

Trabalhos futuros vão expandir o paradigma de Fog Comptuing em Smart Grid (refere-se a um sistema de energia elétrica que se utiliza da tecnologia da informação para fazer com que o sistema seja mais, confiável e sustentável). Nesse cenário, dois modelos para dispositivos FoG podem ser desenvolvidos. Dispositivos de nevoeiro independetes consultam diretamente a Cloud para atualizações periódicas sobre preços e demandas, enquanto os dispositivos interligados podem consultar-se e criar coalizões para futuros aprimoramentos. Mobilidade entre os nós da névoa e entre o nevoeiro e a nuvem, podem ser investigados. Ao contrário de centros de dados tradicionais, dispositivos de neblina

estão distribuídos geograficamente em plataformas heterogêneas. A mobilidade do serviõ em plataformas precisa ser otimizada.

REFERÊNCIAS BIBLIOGRÁFICAS

-Countinho A, Carneiro E, Greve F, "**Computação em Névoa: Conceitos, Aplicações e Desafios"**Cap.6 .2016. Sociedade Brasileira de Computação 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"** Universidade de Brasília, 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**", Universidade Federal de Santa Catarina 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**" School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China 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 . Unicamp Disponivel em: < http://repositorio.cbc.ufms.br:8080/jspui/bitstream/123456789/2712/1/Carlos%20Alberto%20da%20Silva.pdf > Acessado em 20/08/2017.

-Babar S, Mahalle P, Stango A,"**Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)"**, CNSA 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**", Technoscience Academy, 2017. Disponivel em : < http://ijsrcseit.com/paper/CSEIT172428.pdf> Acessado em 21/08/2017.

-SANTOS, Bruno P. et al. Internet das coisas: da teoriaa prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos, 2016. Disponivel em: http://homepages.dcc.ufmg.br/~bruno.ps/wp-content/uploads/2016/05/minicurso-sbrc-2016.pdf, Acessado em 29/10/17.

- MANDUCA, Alexandre. O despertar dos objetos: os dispositivos na era da internet das coisas. REGIT, v. 5, n. 1, 2016. Disponivel em: http://fatecitaqua.edu.br/revista/index.php/regit/article/view/ART5/pdf_57, Acessado 29/10/17.

- LIU, Chibiao; QIU, Jinming. Study on a Secure Wireless Data Communication in Internet of Things Applications. International Journal of Computer Science and Network Security (IJCSNS), v. 15, n. 2, p. 18, 2015. Disponível em: <http://paper.ijcsns.org/07_book/201502/20150204.pdf>. Acesso em: 29/10/17.

Cintas. IoT Security: Huge Problems and Potencial Solutions. Disponível em: <http://www.cintas.com/ready/healthy-safety/iot-security-huge-problems-and-potentialsolutions/>.
Acesso em 28/10/17.

-Stojmenovic A, Weng S "**The Fog computing paradigm: Scenarios and security issues**", IEEE, 2014. Disponivel em: <http://ieeexplore.ieee.org/document/6932989/> Acessado em 16/09/2017.

-Yi S, Li C, Li Q," **A Survey of Fog Computing: Concepts, Applications and Issues**", ACM New York, NY, USA ©2015. Disponivel em: <http://dl.acm.org/citation.cfm?id=2757397> Acessado em 16/09/2017.

- Moraes, L. C. D. O. (2016). Framework de comunicação seguro e confiável para Internet das Coisas usando o protocolo XMPP. **Disponivel em:**
https://tedebc.ufma.br/jspui/handle/tede/tede/1689 > Acessado em 29/10/2017.

-Shi W, Dustdar S," **The Promise of Edge Computing**", IEEE. Disponivel em: <http://ieeexplore.ieee.org/document/7469991/> Acessado em 16/09/2017.

- AVELAR, Edson Adriano M. et al. Arquitetura de Comunicação para Cidades Inteligentes: Uma proposta heterogênea, extensível e de baixo custo. In: **XXXII Congresso da Sociedade Brasileira de Computação, Curitiba, Brasil**. 2012. .
Disponivel em:
<http://www.multicast.com.br/ucb/projeto-integrado/artigos-exemplo/cidade-inteligente-arquitetura-de-baixo-custo.pdf > Acessado em 29/10/2017.

-LACERDA, Flávia. Arquitetura da Informação Pervasiva: projetos de ecossistemas de informação na Internet das Coisas. 2016. **Disponivel em:**
< http://repositorio.unb.br/handle/10482/19646> Acessado em 29/10/2017.