https://eventos.utfpr.edu.br//sicite/sicite2020

Revisão de técnicas de autenticidade e confiança para computação em névoa

Review of authenticity and trust techniques for fog computing

Geiziely Aparecida Streit Pinto
geiziely@alunos.utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil

Daniel Fernando Pigatto
pigatto@utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil

Recebido: 19 ago. 2020.
Aprovado: 01 out. 2020.

RESUMO

A Computação em Névoa (*Fog Computing*) visa, primeiramente, resolver problemas de latência de comunicação e reduzir a dependência de aplicações com relação a serviços de nuvem. Entretanto, o aumento de nós na camada intermediária de Computação em Névoa abre espaço para um novo desafio a ser abordado que é a garantia de autenticidade e de confiança (*trustness*) dos nós. Estes elementos são importantes dentro do contexto de segurança e essenciais para que uma estrutura distribuída possa funcionar sem haver comprometimento de informações de usuários finais. Este documento investigará trabalhos já publicados na área e identificará formas de se aplicar técnicas de autenticidade e confiança em nós de Computação em Névoa. Utilizando ferramentas de busca direcionadas a pesquisas acadêmicas como Google Scholar, IEEE *Xplore* e o Portal de Periódicos da CAPES. Desta forma pôde se verificar a importância da Computação em Névoa em relação a segurança na troca de informações, onde é possível realizar uma filtragem de nós confiáveis, com relação aos protocolos de confiança, atributos, políticas de nós, entre outras formas de analisar a confiança, de acordo com as características do sistema.

PALAVRAS-CHAVE: Confiança entre nós da névoa. Segurança na névoa. Filtragem de nós de confiança.

ABSTRACT

Fog Computing is primarily aimed at solving communication latency problems and reducing application dependence on cloud services. However, the increase in nodes in the middle layer of Fog Computing opens space for a new challenge to be addressed, which is the guarantee of authenticity and trustness of the nodes. These elements are important within the security context and essential for a distributed structure to function without compromising end-user information. This document will investigate works already published in the field and identify ways to apply techniques of authenticity and trust in Node Computing nodes. Using search tools aimed at academic research such as Google Scholar, IEEE Xplore and Portal de Periódicos in CAPES. In this way it was possible to verify the importance of the Fog Computing in relation to security in the exchange of information, where it is possible to perform a filtering of trustworthy nodes, in relation to the trust protocols, attributes, trust policies, among other ways of analyzing trust, according to the characteristics of the system.

KEYWORDS: Trust among nodes in the fog . Security in the fog. Filtering of trustworthy nodes.

INTRODUÇÃO

O uso da Computação em Nuvem vem se tornando cada vez mais indispensável em organizações por conta da facilidade em guardar e acessar informações (SINGH e CHATTERJEE, 2017). Pode-se definir computação em nuvem como o uso de recurso logístico de computação, assim como a nível de software, através da utilização de serviços oriundos da internet (STERGIOU et al., 2018). Algumas características são destacadas: gerenciamento e acesso a dados da internet sem necessidade de interação humana, dados acessíveis em qualquer dispositivo que atenda aos protocolos de acesso, recursos físicos ou virtuais compartilhados entre os usuários em um ambiente dinâmico, sendo uma tecnologia básica no uso da Internet das Coisas (SINGH e CHATTERJEE, 2017) (STERGIOU et al., 2018).

A Internet das Coisas (IoT) é uma rede de dispositivos que transmitem, compartilham e utilizam dados de um ambiente físico para providenciar serviços individuais, corporacionais e para a sociedade (STERGIOU et al., 2018). A IoT pode ser vista como um caminho para os usuários acessarem funcionalidades e aplicações pessoais (ZHANG et al., 2018). Estes dispositivos conectados à rede precisam repassar os dados coletados para a Nuvem para então receber os serviços requisitados, mas com o aumento no número de dispositivos o carregamento de dados cresceu exponencialmente, trazendo mais desafios entre as comunicações. Para reduzir esses dados nos servidores da Nuvem, foi introduzida uma camada adicional entre a Nuvem e os usuários chamada Computação em Névoa (DEBE et al., 2019).

A computação em Névoa é uma plataforma virtualizada que surgiu como uma tecnologia promissora que poderia trazer as aplicações da nuvem mais perto dos dispositivos físicos da IoT na rede de borda, fornecendo armazenamento, computação e serviços da internet para os usuários (SOLEYMANI et al., 2017)(Al-OTAIBI et al., 2019). Os nós da Névoa geralmente fornecem conexões confiáveis, filtram e guardam os dados antes de repassarem para a nuvem (DEBE et al., 2019).

A importância da implantação da Computação em Névoa em um sistema que envolve comunicação entre um dispositivo e a nuvem é de alta relevância, pois há uma latência na troca de informações, processamento de dados, gasto de energia, entre outros problemas. Com a aplicação da Névoa e utilizando seus nós é possível notar a agilidade e melhora em todo o processo, mas, por sua vez, outros problemas passam a ficar mais evidentes como os relacionados à proteção de dados, privacidade e ataques maliciosos.

Com isso, vêm crescendo as pesquisas com relação à segurança do sistema, principalmente envolvendo confiança e autenticação. A confiança desempenha um papel importante em relações baseadas em interações passadas entre nós e dispositivos. Algumas características, como taxa de perda de pacote de dados, valor direto e valor indireto de confiança são considerados para saber o quão confiável é um nó (WANG et al.,2020). Já a autenticação do remetente deve ser uma das primeiras checadas em qualquer sistema de segurança (SOLEYMANI et al., 2017). Deve haver uma dupla autenticação, seja de um dispositivo que requisita a conexão com um nó ou um nó que queira se conectar a uma nuvem, assim gerando também altos níveis de confiança (MORA-GIMENO et al., 2018). Com o surgimento das redes ad-hoc veiculares (VANETs), que são redes de comunicação sem fio entre

veículos, é cada vez mais necessária a atenção a aspectos de segurança. Para isso, a proposta de chaves de autenticação dinâmicas entre nós da *Fog* aumenta a confiança e veracidade das informações recebidas (Al-OTAIBI et al., 2019).

METODOLOGIA

Para a obtenção das informações aqui apresentadas, foram realizadas pesquisas de artigos que foram publicados a partir de 2012 que pudessem contribuir com técnicas de autenticidade e confiança para computação em Névoa realizadas em seus respectivos trabalhos.

Foram utilizados mecanismos de busca como Google Scholar, IEEE *Xplore* e Portal de Periódicos da CAPES, os quais foram ferramentas essenciais para adquirir informações necessárias para a realização desta revisão. Para encontrar estes artigos, palavras-chave na língua inglesa como *fog computation*, *trust fog, fog computing security, trust problems in the fog system*, *trust fog computation*, foram adotadas.

RESULTADOS E DISCUSSÕES

Uma das questões apontadas nos estudos realizados é o tamanho da abrangência da Computação em Névoa, que consequentemente afeta o controle de segurança sobre os componentes envolvidos na troca de dados entre um dispositivo e a nuvem (ZHANG et al., 2018). O uso dos nós da Névoa como um controle de segurança na comunicação entre nós é uma das propostas dos artigos. Usando esses nós para verificar o nível de reputação e, assim, aumentar o nível de confiança, é possível tornar os sistemas mais seguros e checar cada informação antes de repassar (WANG et al., 2020). Já outro artigo usa Unidades Laterais da Estrada como nós do sistema em redes veiculares (Al-OTAIBI et al., 2019). Segue no Quadro 1 principais técnicas de confiança e autenticidade encontrada nos artigos.

Quadro 1 – Resumo de técnicas de confiança e autenticidade.

Referência	Confiança	Autenticidade
Al-OTAIBI et al., 2019	- Avaliação de confiança com base na velocidade e localização do automóvel.	-Mensagens criptografas. -Chave autenticada. -Chaves simétricas.
DEBE et al., 2019	-Feedback do usuário com notas de reputação para os nós utilizados. -Credibilidade do usuário.	-Contratos inteligentes.
MORA-GIMENO et al., 2018	-Grau de confiança de cada camada com base na conformidade estabelecida. -Nível de segurança de acordo com o grau de confiança de cada camada.	-Velocidade da comunicação de credenciais entre as camadas. -Conexão criptografada.
SOLEYMANI et al., 2017	-Valor de confiança baseada em relações anteriores.	-Tempo de vida e localização da mensagem.
SU et al., 2017	-Nível de segurança e confiança do nó. -Política de proteção. -Contexto colaborativo na Névoa.	-Termos de qualidade. -Comparação de atributos da mensagem enviada com os atributos do nó.

Referência	Confiança	Autenticidade
WANG et al., 2020	-Atribuição de valores de confiança com relação a cada nó. -Um nó, com maior valor de confiança, fica responsável por um grupo de nós.	-Garante a credibilidade dos dados finais coletados. com base na minimização do consumo de energia.
WANG et al., 2018	-Relação de confiança hierárquica. -Relação de confiança direta entre nós. -Relação de confiança abrangente entre nós.	-Analisa os dados com base em tabelas de confianças, histórico do sensor de dados e topologia de rede.
ZHANG et al., 2018	-Inserir uma camada de serviço na FOG. -Propõem PPS baseado em informações de privacidade em contextos na FOG. -Região baseada em confiança, com um nó responsável pela região a sua volta.	-Autoridade de atributo gera chaves de acesso. -Autoridade de certificação e controle de acesso baseado em política.

Fonte: Autoria própria (2020).

Com a grande área de abrangência dos nós da Névoa, uma das formas abordadas foi fazer um deles responsável pela comunicação entre regiões distintas (WANG et al., 2020). A escolha deste nó é realizada com base no nível de confiança e menor gasto de energia, isso tudo coletado pelo sensor de dados, ficando responsável pelo seu grupo de nós correspondente à área delimitada. Desta forma fica a cargo do representante do grupo delegar tarefas e gerenciamento dos recursos computacionais (ZHANG et al., 2018). O nó principal recolhe os dados de outros nós e informações de suas reputações repassando para um sensor coletor de dados de confiança que repassa para nó móvel inteligente, com propriedades de processamento (WANG et al., 2020). Assim este nó móvel percorre os nós principais de cada grupo evitando a perda de energia e tempo procurando informações em nós com baixo nível de confiança, aumentando a segurança ao acessar os dados. Deste modo ao buscar informações, será feito um planejamento do caminho a ser percorrido.

Os nós transmitem e recebem dados a todo tempo e de vários lugares diferentes, como já comentado anteriormente, então é necessário ter um controle sobre o tráfego de mensagens, assim como dos remetentes e suas características. Uma das abordagens realizadas para checar se os nós são de confiança, considera algumas características dos mesmos, mas é importante ressaltar que quanto mais características requeridas durante o processo de interação, mais complicada fica a implantação do sistema, por haver algumas restrições que devem ser seguidas como consumo de energia e baixa latência. Neste caso foram utilizadas três características para obter o estado de confiança do nó: a taxa de perda de pacote, taxa de falha de rotas e atraso de envio (WANG et al., 2018). É possível, também, verificar a confiabilidade dos nós por meio de lógica Fuzzy, que usa como critérios o nível de precisão do local do evento e, em seguida, verifica o nível de confiança baseado em experiências passadas e legitimidade (SOLEYMANI et al., 2017). Assim como no modelo de descentralização do sistema de reputação, onde fica disponível o acesso dos clientes a uma lista de nós que atendam a seus requisitos, é possível utilizar o *Ethereum Blockchain* (DEBE et al., 2019) para manipulação de contratos inteligentes, que possui cinco contratos sendo um deles de Reputação. Após uma interação com o nó da Névoa, o cliente valida o nó baseado na latência, custo ou algo que o afetou individualmente, desta forma os pontos de reputação são modificados conforme o número de interações e a credibilidade de cada

cliente. Com isso, os clientes podem selecionar os nós antes de fazer uma interação, de acordo com seus requerimentos, através de um contrato inteligente.

Um dos principais conceitos da Névoa é a proximidade da borda da internet com o dispositivo, como abordado por alguns artigos, os quais assumem o dispositivo como um nó com processamento inteligente. Foi proposto um modelo para comunicação entre veículos (Al-OTAIBI et al., 2019), onde as Unidades Laterais da Estrada (RSUs) seriam os nós desse sistema. Sendo assim, a troca de informações entre os veículos deixa de acontecer, evitando ataques, sobrecargas computacionais e preservando a privacidade dos usuários, ocorrendo apenas entre o automóvel e as RSUs mais próximas. Dispositivos dos usuários também possuem um papel especial no modelo apresentado (DEBE et al., 2019) onde o mesmo que valida os nós da Névoa, ou seja, o cliente, têm acesso direto aos contratos inteligentes e sua modificação de acordo com suas prioridades.

Já outro artigo faz uso de contextos para assegurar a legitimidade dos dados entre a nuvem e a Névoa e impor um gerenciamento de segurança onde primeiramente ocorre um acordo de termos de qualidade de proteção de dados na Névoa que gera um contexto colaborativo, sendo requerido o contexto de cada participante para verificar os requisitos de segurança. Os nós que vão ser escolhidos para alguma tarefa têm que possuir um termo de proteção de dados, além de se atentar ao nível de segurança e confiança do componente. Após cada nó fazer seu serviço, os dados são enviados ao *sub-contractor*, que é um nó de processamento que faz a checagem dos termos de qualidade de proteção e examina com a política de privacidade do nó proprietário dos dados originais, utilizando o modelo baseado em política de atributo do dado enviado pelo proprietário como requerimento de segurança, que inclui fatores de segurança como confiança e nível de reputação. Com os dados processados na Névoa, cada *sub-contractor* de sua área envia os dados à Nuvem, que faz a checagem dos contextos enviados por todos os *sub-contractor* se todas as regras de agregação de dados forem compatíveis, então os dados são combinados em um módulo e em seguida possui um validador de atributos de segurança que faz a verificação. Ou seja, de ponta a ponta da comunicação entre a Névoa e a Nuvem é realizada a verificação dos parâmetros, políticas, protocolos, atributos, para detectar cada nó suspeito ou informação que não confira com a segurança especificada como o proprietário original dos dados (SU et al., 2017).

A necessidade de manipulação de dados para garantir a segurança, confiabilidade entre troca de mensagens requer uma separação mais eficiente de verificação em módulos que são responsáveis pelas decisões em aceitar ou não a mensagem do remetente (SOLEYMANI et al., 2017). Para alguns casos a Névoa possui centro de bases de dados de sensores, controles de evento e fornecimento de serviços, que auxiliam a estabelecer uma relação de confiança entre CSPs (provedores de serviços da nuvem) e SSPs (provedores de serviços dos sensores) (WANG et al., 2018). As informações que chegam à nuvem também podem ser verificadas por módulos presentes na mesma, sendo, neste caso, três: gerenciador de contexto, RA (*Rule Aggregator*) e RE (*Rule Evaluator),* que comparam mensagens que retornam com as informações enviadas (SU et al.,2017).

Com a inserção de camadas na arquitetura para obter uma segurança maior, diminuir a energia consumida (WANG et al., 2018) ou estabelecer relações de confiança, fica mais difícil acelerar o processo e diminuir a latência entre as

informações, pois cada camada possui protocolos e políticas próprios. Aplicando a computação de borda de acesso múltiplo (MEC) (MORA-GIMENO et al., 2018), é possível facilitar e diminuir o tempo de resposta entre um dispositivo móvel e a nuvem. Ao invés de a nuvem realizar a tarefa, utiliza se o método de fatiamento e, então, a tarefa é realizada pelos nós da Névoa, que é a camada mais próxima do dispositivo. Essas camadas formam a arquitetura MEC, ou seja, composta pela nuvem, Névoa e o dispositivo, podendo variar a quantidade de camadas. Foi proposta a verificação do grau de confiança de cada camada, sendo que quanto maior o grau de confiança, menor é o nível de segurança requerido. Desta forma, se aplicam métodos moldáveis de segurança, evitando gasto de tempo com camadas de grau de confiança maior. Com isso as camadas só precisam verificar o grau de confiança das camadas seguintes para repassar os dados. Cada uma possui três módulos além dos já existentes: gerenciador de confiança, gerenciador de isolamento e gerenciador de integridade.

Para garantir a segurança e privacidade entre os usuários é preciso dificultar o acesso aos dados e informações que trafegam por usuários não confiáveis, com isso a implementação de criptografias pode evitar ou dificultar ataques. Utilizando criptografia baseada em atributos é proposto um sistema que controla o acesso aos dados com atualização de texto cifrado e a terceirização da computação entre a Névoa e IoT para diminuir o custo computacional, sendo que a autoridade de atributo gera chaves públicas de acesso para nuvem, nó e usuário (ZHANG et al., 2018). A troca de informações entre RSUs, que funcionariam como os nós do sistema (Al-OTAIBI et al., 2019), são criptografadas utilizando chaves simétricas para acesso às mensagens. Existem autoridades de confiança autenticadas pela nuvem que validam os dispositivos distribuídos. Chaves de acesso públicas também são geradas para a comunicação entre RSUs e os automóveis. Apesar de alguns sistemas possuírem um grau de confiança, é necessário realizar troca de mensagens criptografadas utilizando tecnologias como SSL/TLS (MORA-GIMENO et al., 2018).

O uso de chaves para acesso é comum na interação entre nuvem, nós da Névoa e dispositivos, as quais servem como autenticação das fontes da informação (Al-OTAIBI et al., 2019). Neste caso há uma autoridade de confiança que envia uma chave inicial para cada nó que em seguida gera uma aleatória, que junto com a autenticada fornecida calcula uma chave simétrica, usada na comunicação entre as RSUs. Cada pequena parte aleatória gerada por cada nó é enviada para as RSU que utilizam cada parte recebida para gerar chaves simétricas para cada unidade. A lista de partes e as chaves simétricas são armazenadas para futuros acessos e a chave de autenticação é particionada para o próximo ciclo. Depois de um período, todos os nós fazem uma atualização destas chaves utilizando a nova chave de autenticação e refazem as chaves simétricas com as partes fornecidas de cada RSU. Se caso um novo nó requisitar acesso, será utilizada a técnica da resposta-desafio onde deverá alcançar o mesmo ciclo das outras RSUs. Caso alcance, ela ganha a chave de autenticação (Al-OTAIBI et al., 2019). Quando os dados são recebidos, verifica-se o ID dos usuários para checar se o remetente da mensagem é confiável. Outra checagem efetuada seria o tempo de vida desta mensagem, ou seja, o tempo total entre a geração da mensagem e o recebimento (SOLEYMANI et al., 2017). A autenticação é necessária para confirmar, por exemplo, se um dispositivo móvel quer acessar uma camada e pode então ser validada, assim como, se o dispositivo móvel quer fazer uma interação com o nó da Névoa e precisa ser autenticado para

estabelecer uma conexão (MORA-GIMENO et al., 2018). Para este artigo foi utilizada a autenticação do usuário por nome e senha.

CONCLUSÃO

Com a análise da literatura percebeu-se, por simulações, que a aplicação dos nós na arquitetura pode detectar ataques maliciosos, nós suspeitos e possíveis ataques de dados incertos (SOLEYMANI et al., 2017). Alguns benefícios vistos seriam que essa camada pode ter acesso aos diferentes níveis de confiança de cada rede, além de possuir tarefas de análise de dados para encontrar possíveis ataques internos e ajudar a estabelecer uma relação de confiança entre provedores de serviço de nuvem e provedores de serviços de sensores (WANG et al., 2018) .

Os resultados referentes aos testes realizados em dispositivos confirmaram que as aplicações que rodam na Névoa sofrem menos ataques de segurança, sendo 3 atingidos de um total de 80, pois ao executarem na Névoa permanecem menos tempo expostos a ataques (MORA-GIMENO et al., 2018).

Utilizando a lógica Fuzzy para verificar o nível de confiança do remetente baseado nas experiências anteriores e checagem de um grupo de regras, foi possível melhorar a decisão em receber ou não a mensagem do remetente (SOLEYMANI et al., 2017). Isso é realizado com a implantação de atributos aos dados com modelo de política de controle de acesso e validando o acesso aos dados com relação ao perfil de política dos nós. Notou-se que o processamento de dados é mais rápido por par de atributos do que por predicados de atributo (SU et al., 2017).

Com base nos experimentos, utilizando protocolo de coleta de dados baseado em confiança comprovou-se que ocorre uma filtragem de nós não confiáveis e assim evita-se o contato com eles, não precisando assim percorrer todos os nós e, consequentemente, diminuindo o uso de energia (WANG et al., 2020).

De acordo com os experimentos realizados com uso do *blockchain* e ferramentas de segurança, verificou-se que o sistema não se mostrou vulnerável a ataques, pois como o *blockchain* é descentralizado pode facilitar algumas entradas pelo acesso a vários nós, mas houve um controle de informações enviadas e recebidas para o correto uso dos contratos inteligentes, impedindo a entrada de ataques (DEBE et al., 2019).

Como um todo é certo notar que a segurança na Névoa é primordial e vem ganhando grande atenção de pesquisadores e estudiosos. Com vários projetos e modelos desenvolvidos e simulados é visto que técnicas parecidas são utilizadas nos trabalhos aqui apresentados. O uso de protocolos, políticas de privacidade, atributos e chaves complexas de acesso para a escolha de nós confiáveis, assim como, pontuações de confiança gerada por interações passadas que envolvem comportamentos esperados dos nós, são as que mais se destacam.

Visto que este meio da computação em Névoa é muito amplo e envolve muitas questões relacionadas à segurança, por se conectar a hardwares distintos, aumenta-se a chance de ataques (ZHANG et al., 2018). Se observa que há muita área de pesquisa que pode ser explorada, principalmente que atenda aos requisitos de baixo consumo e latência sem descartar a segurança na Névoa.

REFERÊNCIAS

AL-OTAIBI, B.; AL-NABHAN, N.; TIAN, Y. Privacy-Preserving Vehicular Rogue Node Detection Scheme for *Fog* Computing. Sensors (Basel, Switzerland), 2019, Vol.19(4), doi:10.3390/s19040965. Disponível em: https://www.mdpi.com/1424-8220/19/4/965/htm. Acesso em: 15 jun.2020.

DEBE, M.; SALAH, K.; REHMAN, M.H.U.; SVETINOVI, D. IoT Public *Fog* Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain. IEEE Access, vol. 7, pp. 178082-178093, 2019, doi: 10.1109/ACCESS.2019.2958355. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8928584&isnumber=8600701. Acesso em: 09 jun.2020.

MORA-GIMENO, F.J; MORA-MORA, H.; MARCOS-JORQUERA, D.; VOLCKAERT, B. A Secure Multi-Tier Mobile Edge Computing Model for Data Processing Offloading Based on Degree of Trust. Sensors (Basel, Switzerland), 01 September 2018, Vol.18(10), p.3211. DOI:10.3390/s18103211. Disponível em: https://doaj.org/article/6ff5b7e7902a4580a8f76a80401b9998. Acesso em: 08 agosto 2020.

SINGH, A.; CHATTERJEE, K. Cloud Security Issues and Challenges: A Survey. Journal of network and computer applications, 01 February 2017, Vol.79, pp.88-115. Disponível em: http://www.sciencedirect.com/science/article/pii/S1084804516302983. Acesso em: 15 jul.2020.

SOLEYMANI, S. A; ABDULLAH, A. H.; ZAREEI, M.; ANISI, M.H; VARGAS-ROSALES, C.; KHAN, M.K; GOUDARZ, S. A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With *Fog* Computing. IEEE Access, vol. 5, pp. 15619-15629, 2017, doi: 10.1109/ACCESS.2017.2733225. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7995031&isnumber=7859429. Acesso em: 20 mar.2020.

STERGIOU, C.; PSANNIS, K. E.; KIM, Byung-Gyu; GUPTA, B. Secure integration of IoT and Cloud Computing. Future generation computer systems, January 2018, Vol.78, pp.964-975. Disponível em: http://www.sciencedirect.com/science/article/pii/S0167739X1630694X. Acesso em: 16 jul.2020.

SU, z.; BIENNIER, F.; LV, Z.; PENG, Y.; SONG, H.; MIAO, J.; Toward architectural and protocol-level foundation for end-to-end trustworthiness in Cloud/*Fog* computing. IEEE Transactions on Big Data, no. 01, pp. 1-1, 5555. 18 maio 2017. DOI: 10.1109/TBDATA.2017.2705418. Disponível em :

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7931685&isnumber=7153538. Acesso em: 12 mar.2020.

WANG, T.; QIU, L.; SANGAIAH, A. K.; XU, G.; LIU, A. Energy-Efficient and Trustworthy Data Collection Protocol Based on Mobile *Fog* Computing in Internet of Things. IEEE Transactions on Industrial Informatics, maio 2020, Vol.16(5), pp.3531-3539. 31 maio 2019. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8727478&isnumber=8999752. Acesso em: 12 mar.2020.

WANG, T.; ZHANG, G.; BHUIYAN, MD Z. A.; LIU, A.; JIA, W.; XIE, M. A Novel Trust Mechanism Based on *Fog* Computing in Sensor–Cloud System. Future generation computer systems, agosto 2020, Vol.109, pp.573-582. 26 junho 2018. Disponível em:https://www.sciencedirect.com/science/article/abs/pii/S0167739X17323658. Acesso em: 20 mar.2020.

ZHANG, P.; ZHOU, M.; FORTINO, G. Security and trust issues in Fog computing: A survey, Future Generation Computer Systems, Volume 88, Pages 16-27, 2018. Disponível em: http://www.sciencedirect.com/science/article/pii/S0167739X17329722. Acesso em: 20 mar.2020.