PROPOSTA DE ARQUITETURA IOT UTILIZANDO FOG COMPUTING E ORQUESTRAÇÃO POR PARÂMETROS

Vinicius Salgueiro Costa, Mayron de França Borges, Pedro de Oliveira M. e Souza,
Igor David Morais, Francisco L. de Caldas Filho e Rafael T. de Sousa Jr
Laboratório LATITUDE, Departamento de Engenharia Elétrica, Universidade de Brasília (UnB), Brasília-DF, Brasil

RESUMO

Internet das coisas tem se mostrado uma tecnologia em expansão, com um aumento significativo de dispositivos e por consequência no volume do trafego gerado pelos mesmos. Para permitir uma maior resiliência de soluções IoT, garantindo que dispositivos possam receber comandos e enviar dados mesmo sem comunicação com redes externas os paradigmas de FoG Computing tem se tornado cada vez mais frequente. Este trabalho tem como objetivo apresentar uma solução de FoG Computing aplicada em redes IoT onde o processamento e armazenamento de dados, além do controle de atuadores é feito remotamente, em um Gateway na mesma rede local dos sensores. O gateway tem o papel de armazenar os dados de sensores e transmi-los conforme determinado pelo orquestrador.

PALAVRAS-CHAVE

Fog Computing, IoT, Middleware, Cloud Computing

1. INTRODUÇÃO

Internet da Coisas – IoT, de acordo com (Bellavista, et al., 2019), se refere à implantação de múltiplos dispositivos inteligentes para dar suporte as atividades diárias. Este conceito, que vem mudando a relação entre as pessoas com o mundo físico e a tecnologia, permite uma conexão entre os dispositivos que interagem entre si e coletar dados sobre o ambiente.

Por se tratar de uma tecnologia cada vez mais utilizada, bem como de fácil acesso, a previsão, segundo (Cisco, 2020), é de que, até 2023, mais de 29 bilhões de dispositivos IoT estarão conectados à rede mundial. Portanto, a quantidade de dados enviados através da rede tem crescido exponencialmente, com uma previsão de tráfico de 4,8 Zettabytes de dados no período de um ano (Cisco, 2019). Com o aumento significativo da quantidade de dados enviados pela internet e a formação de nuvens gigantes de dados, nasce um grande paradigma, no qual os problemas de atraso de resposta de servidores centralizados são cada vez mais frequentes e, consequentemente, o tempo de tomada de decisão dos dispositivos de ponta aumenta consideravelmente (Atlam, et al., 2018).

Uma das maneiras de solucionar o problema em questão se dá através dos conceitos de Edge e *Fog Computing*. Esta proposta de arquitetura permite o processamento, armazenamento, conexão e gerenciamento de dados em dispositivos de rede próximos aos dispositivos IoT de ponta (Yousepfour, et al., 2019). Deste modo, mitigam-se problemas de conexão com servidores centrais mais distantes, que apresentam tempos de resposta muito superiores ao desejado para os dispositivos de ponta, trazendo a inteligência dos dados para perto da ponta (Atlam, et al., 2018).

O projeto proposto neste artigo utilizará do conceito de Edge e *Fog Computing* para descentralizar a inteligência dos dados, evitando, assim, possíveis transtornos na Rede. O projeto busca a implementação de um sistema de Middleware próximo à ponta da rede que por linhas de comando será capaz de orquestrar os dados recebidos pelos dispositivos, processá-los e enviar dados para o servidor de forma mais eficiente, mitigando a necessidade de uma transmissão direta de dados para um ambiente central da nuvem, através do uso de uma rede local.

2. TRABALHOS RELACIONADOS

Em (Carlo et al., 2019), é apresentado diversos aspectos com as vantagens do uso de Fog Computing. No caso de Consumo de Banda, o artigo aborda que por boa parte dos dados ser comunicada a Fog-nodes próximos, uma quantidade reduzida de banda é trocada com um Cloud datacenter. Além disso, os Fog-nodes comportam-se como pontos intermediários entre os dispositivos e a Nuvem, reduzindo ainda mais os dados transmitidos para um Cloud datacenter. Em ambientes hostis, por exemplo, onde se há risco considerável de uma eventual queda de conexão de dados, a utilização de uma rede de Fog Computing é fundamental em casos nos quais o serviço implementado precisa estar disponível constantemente, portanto, devido à ação do orquestrador de maneira independente quando não se é possível estabelecer uma conexão com a nuvem, a manutenção da rede é garantida. Para a proteção e garantia do funcionamento de serviços essenciais a dispositivos conectados em uma rede, este artigo explora o conceito de Fog Computing tendo em vista uma independência da arquitetura quanto a conectividade a nuvem, ajudando a executar serviços que precisam sempre estar em execução, além de que toda arquitetura está implementada de modo a reduzir o consumo de banda geral, ajudando a gerenciar com eficiência o volume de dados na rede visto a implementação do modelo de orquestração por passagem de parâmetros local.

Em, (FU, Kevin et al.2020) é apresentado um cenário com a aplicação de Fog Computing quando associado a diversos dispositivos IoT. No artigo é visto que o número de dispositivos IoT interconectados exige uma maior complexidade para operá-los com segurança e privacidade aumenta. Essa complexidade crescente exige padrões e soluções que nem sempre podem ser atribuídos individualmente a cada dispositivo IoT. Este trabalho considera a análise de segurança e privacidade e a complexidade para a operação de cada dispositivo e de toda arquitetura proposta, pensando nisso, neste artigo é apresentado o modelo de orquestração com passagem de parâmetros localmente, pois desta maneira os dados passam por um gateway onde são tratados antecipadamente ao encaminhamento para a nuvem, visando aprimorar o nível de segurança e privacidade de toda arquitetura proposta.

No Trabalho de (Alrawais, Arwa et al. 2017) é citado acerca da autenticação em IoT, destacando haver vários desafios como a escalabilidade e eficiência para obter um ambiente seguro, escalável, eficiente e fácil de usar com dispositivos IoT com recursos limitados de segurança e autenticação. O artigo destaca que com a implementação de *fog computing*, um algoritmo de criptografia leve pode ser aplicado entre nós de fog e dispositivos IoT para melhorar a eficiência do processo de autenticação. Este artigo não tem o foco na criptografia dos dados, portanto não há um algoritmo de criptografia entre os nós e os dispositivos, diferindo com o artigo citado, onde é desenvolvida a solução de orquestração por passagem de parâmetros onde há regras e padrões para a ativação dos endpoints previamente cadastradas no orquestrador, passando-se a coleta e armazenamento dessas regras para um ambiente local e diminuindo a responsabilidade individual de cada dispositivo em termos de segurança, trazendo-a para os nós intermediários entre a parte externa do sistema e os dispositivos IoT.

Em, (Pereira et al., 2017) foram apresentadas e discutidas características de *Fog Computing* para compensar o modelo convencional de nuvem nas bordas da rede. Dispositivos de borda têm recursos computacionais limitados, e, para contornar essa situação, foi proposto a união das soluções de Fog Computing e computação em nuvem para construir uma infraestrutura de IoT sustentável para cidades inteligentes. Este artigo propõe a utilização de um gateway que executa, dentre outras tarefas, pré-processamento e filtragem de dados, auxiliando o quesito de uma infraestrutura sustentável, tendo em vista os dispositivos de borda usados possuírem limitação de hardware. Logo, o gateway Fog possibilita que somente dados necessários sejam transferidos a nuvem, mantendo o controle e atividades dos sensores e objetos IoT.

A discussão da expansibilidade da aplicação de *Fog Computing* cresce em conjunto com ideias de aplicações em diversos setores. O trabalho de (Varghese et al., 2020) analisa as vantagens do uso de Fog Computing, através da utilização de um modelo que diminui em 20% o tempo médio de resposta de um servidor para um usuário e 90% do tráfego de dados entre a borda e a nuvem, quando se compara a uma solução que utiliza somente computação em nuvem. O tempo médio de resposta para os dispositivos IoT em uma arquitetura com Fog Computing são demonstradas neste artigo, onde é utilizado este modelo através da passagem de parâmetros, simultaneamente com um gateway, que executa diversas operações para que a carga nos dispositivos seja menor, diminuindo assim o uso dos recursos computacionais de dados e hardware.

O artigo de (Subhadeep, Sarkar et al., 2015) apresenta uma novidade ao investigar os aspectos ecológicos para julgar a adequação de *fog computing* para servir o mundo de Dispositivos conectados à Internet. E semelhante a este artigo, foi realizado um estudo para examinar a latência e resposta dos dispositivos em *fog computing* buscando visualizar a eficiência da aplicação de *Fog computing* em sistemas com dispositivos IoT. Neste artigo, há a atuação de um facilitador de processos que, além de fazer requisições a dispositivos e dar autonomia à rede local, possibilita maior resiliência da aplicação, também atuando no quesito de escalabilidade, performance e facilidade de uso.

O trabalho de (Yi, Shanhe et al., 2015) cita dificuldades e problemas que a computação em nuvem apresenta, como latência, falta de suporte para mobilidade e reconhecimento de localização, e, assim como inúmeros artigos no meio científico, discutem as promissoras aplicações de *Fog Computing* no nicho IoT para solucionar estes problemas em projetos, como monitoramento de ambientes e Cidades inteligentes, além do controle remoto de locais físicos. Este artigo apresenta dados de resposta no acionamento de dispositivos para o controle de um ambiente com a implementação de *Fog Computing*, propondo uma arquitetura que busca contornar empecilhos utilizando o modelo de orquestração por passagem de parâmetros em um ambiente com diversos sensores submetidos a um gateway entre a rede externa e estes dispositivos, fazendo com que toda implementação tenha regras pré-definidas e propiciando uma implementação mais precisa e segura dos e dispositivos e do ambiente.

3. ARQUITETURA PROPOSTA

A arquitetura proposta pretende realizar a orquestração utilizando-se de soluções IoT e *Fog/Cloud Computing*. Com base na arquitetura de (M. Aazam, et al., 2014), é possível ver com clareza, em alternativa à computação em nuvem, como o fluxo de dados ocorre de forma descentralizada devido ao processo de transferência e processamento de dados não ocorrer diretamente na nuvem. A computação Fog tem como alvo serviços e aplicativos com implementações amplamente distribuídas.

A proposta visa trazer uma melhoria na autonomia e eficiência dos diversos dispositivos conectados, aumentando o poder computacional entre a nuvem e o dispositivo, além de fornecer resiliência ao sistema a situações adversas, como períodos de indisponibilidade. Finalmente, esta tecnologia também reduz a quantidade de dados enviados para a nuvem, a latência da rede e da Internet e melhora o tempo de resposta do sistema em aplicativos remotos.

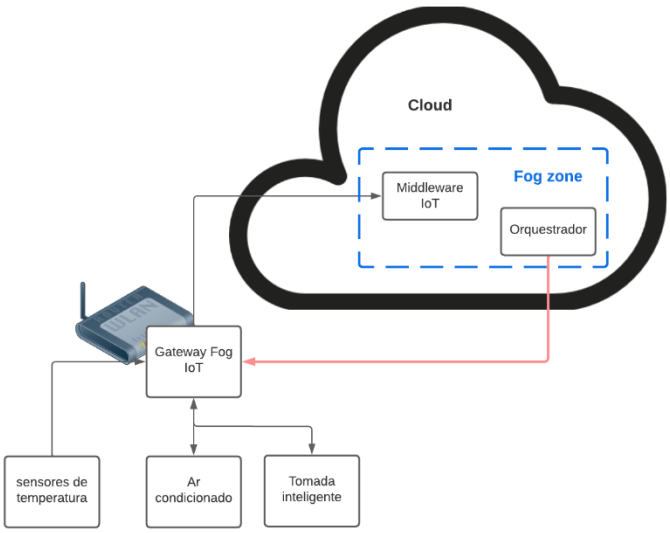

Figura 1. Arquitetura proposta dividida em camadas

Nessa proposta, o g*ateway Fog* IoT possui seus parâmetros pré-estabelecidos pelo orquestrador de parâmetros para transmissão, repasse e armazenamento ao controle de orquestradores.

O g*ateway é* responsável por executar várias tarefas, como coleta de dados e realização de pré-processamento e filtragem dos dados, carregando apenas os dados necessários para a nuvem , bem como a manutenção do controle dos objetos IoT e atividades dos sensores, segurança e privacidade de os dados e monitoramento do serviço. O funcionamento do g*ateway Fog IoT* é detalhado em (D Caldas Filho, et al., 2017) e ele está em contato com a controladora de onde partem as ordens que serão executadas por ele. O Orquestrador é alocado com o *Middleware* usando a arquitetura de *Fog Computing*, desse modo aproveitando os recursos dos sistemas distribuídos. (de Caldas Filho et al, 2019) O sistema é cadastrado com regras de controle que são repassadas para o g*ateway*, verificando-se, portanto, o controle dos atuadores e sensores de forma mais eficiente.

Foi utilizado neste projeto o *Middleware* IoT detalhado em (de Menezes et al, 2019), onde nele é realizado as funções de processamento de dados. O *Middleware é* um facilitador de processos no quesito escalabilidade, performance e facilidade de uso, além de aplicar a arquitetura de Fog *Computing* na rede IoT. Além disso, ele fornece acesso a protocolos HTTP, TCP, MQTT e ZigBee, examina as requisições feitas pelos dispositivos IoT a fim de recolher dados sobre o ambiente, realiza a comunicação com outros *Middlewares* e execução de requisições a dispositivos, bem como dá autonomia à rede local, o que auxilia na maior resiliência da aplicação em ambientes hostis - como manter serviços mesmo com ausência da conexão à Internet. (Menezes, João & Costa et al, 2020).

Na camada física do projeto, é implementado um ambiente de Internet das Coisas (IoT) horizontal, que é composto por diversos tipos de microcontroladores: Arduinos, *nodemcu esp8266 e esp32, Raspberry pi, EMOS,* entre outros. Esses dispositivos possuem um servidor web com *endpoint* responsáveis por receber requisições, onde é possível consultar informações dos sensores e fazer acionamento dos atuadores. A Figura 2 exemplifica a chamada dos atuadores para ligar um ar condicionado em uma casa inteligente, em que foram configurados diversos padrões de uso como controle da temperatura e velocidade na chamada do *endpoint* .

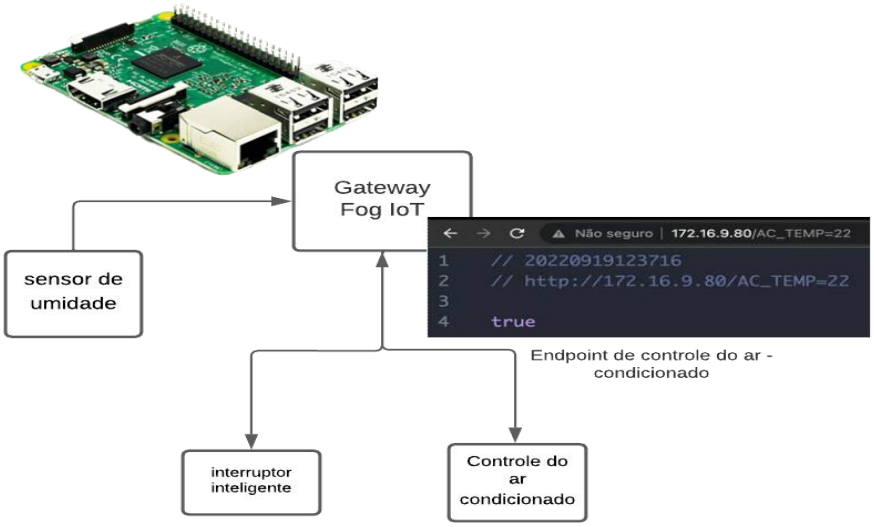

Figura 2. Execução do ar-condicionado via parâmetro

Além do acionamento manual dos *endpoints* em um ambiente local, é possível realizar o acionamento por meio do *gateway Fog* IoT, no qual as regras e padrões para a ativação dos *endpoints* são previamente cadastradas no orquestrador. Assim, o g*ateway Fog IoT* realiza uma coleta e armazenamento dessas regras para um ambiente local e fica responsável pela distribuição e acionamento dos sensores e atuadores de acordo com os parâmetros passados. Isto proporciona maior segurança e escalabilidade para a execução das atividades realizadas pelos dispositivos, contribuindo no processo de automatização de ambientes, tornando-os inteligentes. Por exemplo, no ar-condicionado citado na Figura 2, foram cadastros informações sobre a temperatura e velocidade que o dispositivo deveria operar, assim, é possível acionar, por meio de uma regra cadastrada e combinado com outros sensores em que circunstancias o ar condicionado deve operar em uma faixa de temperatura especifica.

4. RESULTADOS

Para validação da proposta, foram alocados três dispositivos de internet das coisas construídos com Arduinos, *nodemcu esp8266 e esp32* que desempenhavam funções diversas na monitoria e execução de atividades no laboratório como, controle e acionamento de ar condicionado, medição de temperatura do ambiente, monitoramento de humidade e acionamento de interruptores.

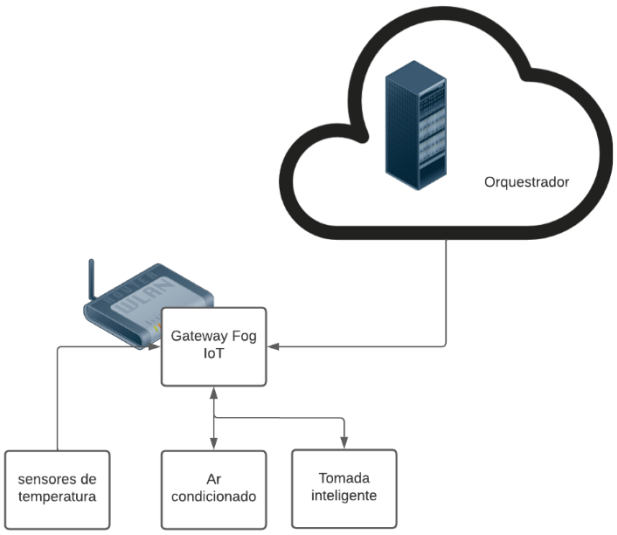

Figura 3. Topologia de comunicação com o orquestrador


```
},
{
  "conditions": [
    "None"
  ],
  "interface": "testes",
  "outputs": [
    " https://172.16.9.83/LEDALL=OFF"
  ],
  "parameters": {
    "meta": {
      "description": "teste",
      "owner": "Anna"
    },
    "service": "1",
    "status": false,
    "ttl": 999
  },
  "serverTime": "2022-10-25T02:23:04.918502+00:00"
},
```


Figura 4. Cadastro de parâmetro no orquestrador

Utilizado um dispositivo presente na Rede Nacional de Ensino e Pesquisa (RNP), que foi responsável por armazenar os parâmetros cadastrados e realizar a comunicação com o Gateway Fog IoT para a execução dos parâmetros, conforme ilustrado na figura 3, e adicionamos um parâmetro para o acionamento do ar condicionado, figura 4.

Com base nesses parâmetros, foram realizados 15 acionamentos com objetivo de comparar a latência para o acionamento do dispositivo, entre um dispositivo em ambiente local em relação ao de resposta do orquestrador conectado ao Gateway Fog IoT. Os dados obtidos pelo experimento, foram obtidos via teste automatizado em Python e expostos na Tabela 1 e 2.

Nas Tabela 1, foram representados os dados coletados de forma consolidada a latência medida da variação entre o tempo de acionamento do *endpoint* e a resposta dos dispositivos de forma local.

Tabela 1. Dados coletados pelos testes em ambiente local

Teste	Dispositivo	Média do tempo de resposta	Primeiro quartil	Segundo quartil
Controle do ar condicionado	*Esp 32*	90,25 ms	83,74 ms	89,02 ms
Sensor de umidade	*Esp 32*	46,97 ms	43,26 ms	46,97 ms
Interruptor inteligente	Esp 8266	19,02 ms	15,69 ms	19,02 ms

Tabela 2. Dados coletados pelo orquestrador

Teste	Dispositivo	Média do tempo de resposta	Primeiro quartil	Segundo quartil
Controle do ar condicionado	*Esp 32*	510,74 ms	217,27 ms	510,74 ms
Sensor de umidade	*Esp 32*	222,53 ms	184,10 ms	240,44 ms
Interruptor inteligente	Esp 8266	127,04 ms	116,69 ms	127,04 ms

Nas Tabela 2, foram representados os dados coletados de forma consolidada a latência medida da variação entre o tempo de acionamento do *endpoint* e a resposta dos dispositivos após a requisição ser feito pelo orquestrador.

A partir da análise destes dados, pode-se inferir que o acionamento dos dispositivos possui um tempo de resposta satisfatório, mesmo que maior em relação ao realizado em ambiente local, o aumento do tempo é justificável devido a necessidade do dado ter de passar por um núcleo de rede até acionar o dispositivo, e a eficiência da adoção de *Fog Computing* em sistemas distribuídos, contribui para a diminuição do tempo de resposta mesmo com outros dispositivos na mesma rede. Com esta arquitetura, o acionamento dos dispositivos é independente do tempo de resposta e da disponibilidade da nuvem, uma vez que as regras são replicadas em um ambiente local, aumentando o tempo de resposta dos dados consultados e dispositivos.

5. CONCLUSÃO E TRABALHOS FUTUROS

A arquitetura desenvolvida, permite uma fácil adaptação e uso da tecnologia em diferentes realidades sendo capaz de processar e executar atividades em múltiplos dispositivos conectados em nuvem e organizados por parâmetros cadastrados e que são executados com auxílio do orquestrador, isso proporciona uma atuação ágil, com menor consumo de energia e tráfego de dados, escalável e resiliente a ambientes hostis.

Por meio de um orquestrador é possível introduzir parâmetros que serão executados pelo Gateway Fog IoT o que permitirá reduzir a necessidade de requisições, gerando dados mais rápidos além de o sistema não ser em apenas um local, ou depender de apenas uma conexão, assim é possível tornar o sistema mais resiliente no caso de falta de energia ou uma intermitência do serviço.

Existem algumas limitações na arquitetura proposta, como a necessidade de se criar diversos parâmetros para atender a necessidade de um ambiente em maior escala para isso como trabalho futuro, será realizado o acionamento de dispositivos através do reconhecimento facial de usuários, através do uso de algoritmos de inteligência artificial combinado com o uso de câmeras, com base em comportamentos identificados, aumento a diversidade de usos que essa tecnologia pode ser utilizada.

Nos testes, foram utilizados dois periféricos, Esp32 e Esp8266, onde o circuito contendo o Esp32 é constituído por um sensor infravermelho e o Esp8266 por dois módulos reles 5v, com isso podemos justificar a demora do tempo da execução do comando de ativação do ar condicionado em relação ao interruptor inteligente, já que, para acionar o sensor infravermelho, é necessário modular o sinal por PWM (Pulse Width Modulation), aumentando o tempo de processamento do Esp32 e ocasionando um aumento no tempo de resposta, alem do aumento do tempo em relação ao teste local.

Os resultados mostram que, mesmo com demais dispositivos conectados, o gateway Fog IoT foi capaz de mitigar um aumento significativo no tempo de acionamento dos dispositivos, através do armazenamento das regras de execução dos atuadores e sensores.

AGRADECIMENTOS

R.T.S.J. agradece o apoio do CNPq outorgas 465741/2014-2 e 312180/2019-5, da Advocacia Geral da União outorga 697.935/2019, do Departamento Nacional de Auditoria do SUS outorga 23106.118410/2020-85, da Procuradoria Geral da Fazenda Nacional outorga 23106.148934/2019-67, do Conselho Administrativo de Defesa Econômica outorga 08700.000047/2019-14 e da Mosaico Tecnologia ao Consumidor.

REFERÊNCIAS

Aazam, M. Et al, 2014. Aazam, mohammad & huh, eui-nam. (2014). Fog computing and smart gateway based C Cmmunication for cloud of things. 464-470. 10.1109/ficloud.2014.83.

Alrawais, arwa et al. Fog computing for the internet of things: security and privacy issues. IEEE internet computing, v. 21, n. 2, p. 34-42, 2017.

Atlam, hany F.; Walters, robert J.; Wills, gary B. Fog computing and the internet of things: A review. Big data and cognitive computing, v. 2, n. 2, p. 10, 2018.

Bellavista, paolo et al. A survey on fog computing for the internet of things. Pervasive and mobile computing, v. 52, p. 71-99, 2019.

Cisco annual internet report (2018–2023). Cisco, 2019. Disponível em: https://www.Cisco.Com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.Pdf. Acesso em: 15/09/2022.

Cisco visual networking index: forecast and trends, 2017–2022. Cisco, 2019. Disponível em: https://twiki.Cern.Ch/twiki/pub/HEPIX/techwatchnetwork/htwnetworkdocuments/white-paper-c11-741490.Pdf

De menezes, J. T. M., Da costa, P. H. L., Da cunha D. F., De caldas filho, F. L., E martins, L. M. C., De mendonça, F. L. L. (2019). Desenvolvimento de modelo hierárquico de middlewares com aplicação de fog computing para redes iot. Atas das conferências ibero-americanas WWW/internet 2019 e computação aplicada , vol. 4128, pp. 155-- 162.(2019).

F. L. D. Caldas filho, L. M. C. E. Martins, I. P. Araújo, F. L. L. D. Mendonça, J. P. C. L. D. Costa, and R. T. De Sousa Junior, “gerenciamento de serviços iot com gateway semântico,” in ˆ atas das conferencias IADIS ibero-americanas WWW/internet 2017 e computação˜ aplicada 2017. Vila moura, algarve, portugal: IADIS press, oct 2017, pp. 199–206.

FU, kevin et al. Safety, security, and privacy threats posed by accelerating trends in the internet of things. Arxiv preprint arxiv:2008.00017, 2020.

M. Muniswamaiah, T. Agerwala and C. C. Tappert, "fog computing and the internet of things (iot): A review," 2021 8th IEEE international conference on cyber security and cloud computing (cscloud)/2021 7th IEEE international conference on edge computing and scalable cloud (edgecom), 2021, pp. 10-12, doi: 10.1109/cscloud-edgecom52276.2021.00012.

Menezes, joão & costa, pedro cunha, dayanne & filho, francisco & martins, lucas & mendonça, fábio lucio. (2020). Desenvolvimento de modelo hierárquico de middlewares com aplicação de fog computing para redes iot.

Pereira charith et al. Fog computing for sustainable smart cities: A survey. ACM computing surveys (CSUR), v. 50, n. 3, p. 1-43, 2017.

Praciano, bruno JG, et al. "Segurança do ambiente usando dispositivo iot com processamento distribuído." Atas das conferências ibero-americanas WWW/internet 2019 e computação aplicada 2019. 2019.

PULIAFITO, carlo et al. Fog computing for the internet of things: A survey. ACM transactions on internet technology (TOIT), v. 19, n. 2, p. 1-41, 2019.

Sarkar, subhadeep; Chatterjee, subarna; Misra, sudip. Assessment of the suitability of fog computing in the context of internet of things. IEEE transactions on cloud computing, v. 6, n. 1, p. 46-59, 2015.

Varghese, blesson et al. Feasibility of fog computing. In: handbook of integration of cloud computing, cyber physical systems and internet of things. Springer, cham, 2020. P. 127-146.

YI, shanhe; LI, cheng; LI, qun. A survey of fog computing: concepts, applications and issues. In: proceedings of the 2015 workshop on mobile big data. 2015. P. 37-42.

Yousepfour, ashkan et al. All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of systems architecture, v. 98, p. 289-330, 2019.