Autenticação e autorização de dispositivos IoT e IIoT em infraestrutura de redes de Identidade Federadas

Fábio Meincheim[1], **Charles C. Miers**[1]

[1]Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Universidade do Estado de Santa Catarina (UDESC)

fabio.meincheim@edu.udesc.br, charles.miers@udesc.br

Resumo. *Realizar a liberação de acesso à Internet para dispositivos IoT nas instituições de ensino é um desafio para a cibersegurança, pois comumente é adotado o compartilhamento de chaves ou utilizadas as credenciais de uma pessoa. Usar uma infraestrutura de autenticação de Federação de Identidades, tal qual a CAFe da RNP, pode facilitar a identificação, autenticação e autorização de dispositivos Internet of Things (IoT) desassociando-o da credencial da pessoa. Este trabalho busca propor uma arquitetura usando Federações de Identidade para realizar o processo de autenticação de dispositivos IoT nas instituições que utilizam a eduroam. Para isto, uma proposta de alteração na arquitetura do ambiente eduroam para registro de dispositivos é o objeto deste estudo.*

1. Introdução e Motivação

O uso de dispositivos *Internet of Things* (IoT) contempla uma considerável variedade de aplicações, coisas ou objetos, como: sensores, atuadores, dispositivos móveis e vários outros. Estes podem interagir e cooperar com os nós vizinhos e mudar de posicionamento [Atzori et al., 2010]. O advento da Indústria 4.0 (I4.0) promoveu a adoção de tecnologias pela indústria, aliando o uso avançado da análise de dados, computadores e pessoas para transformar o negócio, oferecendo serviços internos e entre organizações participantes da cadeia de valor. Surge então o conceito de *Industrial Internet of Things* (IIoT), que traz a adoção de dispositivos IoT, nos equipamentos, processos, cadeia de suprimentos, entre outros, a fim de coletar e analisar dados [Boyes et al., 2018]. A previsão de [Hung, 2017], indica mais da metade dos dispositivos IoT, serão de dispositivos IIoT no futuro próximo. Em 2020, mais de 65% dos negócios irão adotar produtos de IoT, em 2017 este número era 30%. Nas instituições de ensino, nas quais são realizadas pesquisas, desenvolvimento de produtos e atividades de ensino, a necessidade de conectar os dispositivos a Internet, surge como um desafio para as equipes de Tecnologia e Informação (TI). A simples disponibilização de uma conexão WiFi à Internet demanda tempo, tecnologia, segurança e recursos, que muitas vezes a instituição não está preparada para oferecer.

A Rede Nacional de Ensino e Pesquisa (RNP), oferece para as instituições de ensino credenciadas, conexões de Internet, acesso a serviços diversos, e.g., Comunidade Acadêmica Federada (CAFe), e eduroam [RNP, 2020a]. As instituições públicas de ensino, ao utilizarem o acesso à rede CAFe [RNP, 2020b] podem disponibilizar aos docentes e discentes, acesso à Internet usando a rede eduroam para autenticar e autorizar seus usuários na própria instituição, com acesso centralizado por exemplo, sem necessidade

de criar uma Provedor de Serviços (*Service Provider* (SP)) em cada campus. Contudo a CAFe possui credenciais que são essencialmente ligadas às pessoas, e nem sempre dispositivos IoT/IIoT são responsabilidade exclusiva de uma pessoa. Assim, a rede CAFe possui um arcabouço estruturado e com considerável cobertura que pode ser expandida para contemplar dispositivos IoT/IIoT. Desta forma, pode-se utilizar a CAFe, para autenticar e autorizar os dispositivos IIoT, para que os pesquisadores, professores e alunos possam realizar seus estudos e pesquisas. O presente trabalho traz a proposta de utilizar a infraestrutura da RNP, por meio da rede CAFe, para oferecer a autenticação e autorização de dispositivos de IIoT de modo desvinculado às pessoas.

Este artigo está organizado da seguinte forma. A Seção 2 introduz o conceito de IoT e IIoT. A Seção 3 relaciona desafios sobre a autenticação e autorização dos dispositivos. Na Seção 4 o problema é descrito. A Seção 5 apresenta o objetivo do trabalho e por fim, na Seção 6 são apresentadas as considerações e trabalhos futuros.

2. *Industrial Internet of Things* (IIoT)

O termo IoT está relacionado a um considerável número de "coisas" que utilizam tecnologia embarcada e comunicam-se através de infraestruturas de redes de comunicação já existentes, trocando informações e interagindo com o mundo físico (atuadores, comandos e controles) ou provendo informações e análises sobre ambientes (sensores, nós atuadores e outros) [Gubbi et al., 2013]. A IoT possibilitou o desenvolvimento rápido de diversas tecnologias inteligentes, eg., cidades, casas, redes, monitoramento remoto. [Hou et al., 2019]. Para Heng, 2014 e Boyes et al., 2018, na indústria, a adoção da IoT representa uma transformação nos processos de produção, sistemas de armazenamento e logística, e na maneira de integração entre os sistemas ciber-físicos com a adoção e uso da IIoT, tornando os ambientes mais inteligentes. Yaqoob et al., 2017, enumeram os requisitos chaves para o desenvolvimento de arquiteturas de IoT, conforme a Figura 1.

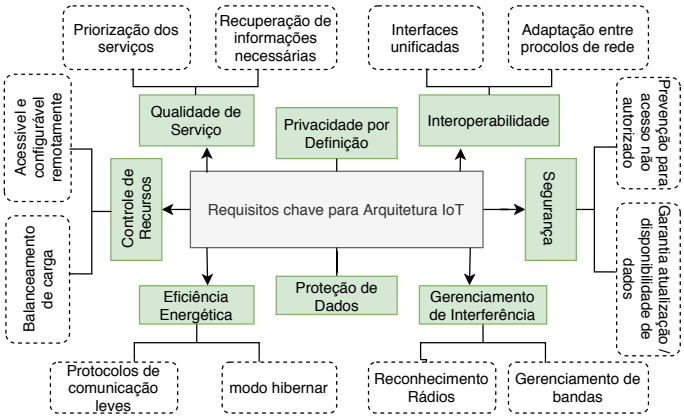

Figura 1. Requisitos de Arquitetura para IoT. Adaptado de: [Yaqoob et al., 2017]

O contexto deste trabalho está no aspecto Segurança de quais dispositivos podem acessar uma rede. A Figura 1 revela a preocupação com o o acesso não autorizado, sendo este item relacionado com autenticação e autorização dos dispositivos IoT / IIoT.

3. Autenticação e Autorização para IoT e IIoT

Problemas de privacidade e segurança em IoT são foco de diversos trabalhos na comunidade de pesquisa e são abordados em diversos níveis. Yang et al., 2017 listam quatro

diferentes visões sobre problemas de segurança: (i) limitação de recurso para aplicar segurança, e.g., poder de processamento, consumo de energia, protocolos básico de criptografia; (ii) classificação de ataques, e.g., físicos, remotos; (iii) foco sobre como mecanismos de autenticação e autorização são implementados; e (iv) análise sobre problemas de segurança nas diferentes camadas de comunicação, e.g., física, rede.

Segundo Neto et al., 2016, a autenticação é uma importante propriedade para IoT e o seu principal objetivo é evitar que dispositivos não autorizados, participem da comunicação e atividades da rede. Basicamente, a autenticação compreende duas propriedades: (i) a autenticação da origem, que garante ao receptor, que a mensagem recebida foi enviada por um remetente confiável; e (ii) a autenticação dos dados, que previne a violação da integridade dos dados na transmissão [Stinson, 2002]. Dispositivos IoT necessitam atender aos requisitos de segurança que garantam rastreabilidade e responsabilidade [Sklyar and Kharchenko, 2019], e os sistemas IIoT precisam garantir requisitos de segurança específicos para o ambiente de Tecnologia Operacional (OT), resultando em diferentes características na operação, descritos na Tabela 1.

Tabela 1. Diferenças: IoT *vs.* IIoT. Adaptado de: [Sklyar and Kharchenko, 2019].

Característica	**IoT**	**IIoT**
Finalidade	Proteção de ativos e dados pessoais	Segurança e prevenção da interrupção do processo
Prioridades	Confidencialidade, integridade, disponibilidade	Disponibilidade, integridade, confidencialidade
Implicações em falhas nos dispositivos	Nenhum consequência critica	Interrupção de processos, impacto na produção, ameaças físicas potenciais
Reação à ameaça	Possível desligamento e remediação	Manutenção da operação, tentativas de prevenção e minimizando a criticidade de efeitos
Atualizações e gerenciamento de correções	Possível durante o tempo de operação, sem razões para atrasos significativos	Precisa ser programado e executado durante o tempo de inatividade, o que pode adiar a atualização por um período de tempo considerável
Ciclo de vida do dispositivo	Atualizações frequentes de dispositivos	Longa vida útil dos dispositivos (mais de 15 anos) e verificação contínua do estado
Ambiente de emprego/uso	Regular	Ambientes severos (temperatura, vibração, etc.)

Sklyar and Kharchenko, 2019, identificam os desafios de segurança da informação para IIoT e a I4.0, baseado no manual de boas práticas para segurança da própria agência e seus pesquisadores. Fagan et al., 2020, descrevem seis atividades básicas que os fabricantes de dispositivos IoT devem adotar para melhorar a segurança no desenvolvimento de produtos e definem uma linha base da capacidade dos recursos de segurança IoT:

- **Identificação do dispositivo**: identificar física e logicamente de forma única;
- **Configuração do dispositivo**: permitir alteração de configurações, mas somente de entidades autorizadas;
- **Proteção de dados**: proteger os dados armazenados e transmitidos, de acesso não autorizado;
- **Acesso lógico às interfaces**: restringir o acesso aos serviços e protocolos das interface apenas para entidades autorizadas;
- **Atualizações do software**: permitir atualizações de software usando mecanismos de segurança apenas para entidades autorizadas; e
- **Relatar estado de segurança**: disponibilizar informações sobre seu *status* de cibersegurança e permitir auditoria por entidades autorizadas.

Os relatórios e recomendações de cibersegurança para dispositivos IoT das agências americana NIST [Fagan et al., 2020], e europeia ENISA, [ENISA, 2019], relacionam di-

versas capacidades de segurança que devem ser implantadas nos dispositivos para garantir a proteção de dados, acessos não autorizados, manutenção segura. A autenticação e autorização de dispositivos podem contribuir para esta garantia.

4. Problema

Os *Identity Provider*s (IdPs) empregam diversas formas de organização para gerenciar as informações de seus usuários. A CAFe implementa o esquema *Lightweight Directory Access Protocol* (LDAP) *brEduPerson*, que armazena informações específicas para a realidade do país, tais como: informações genéricas de identificação para cidadãos que residem no Brasil (CPF, entre outras), informações gerais sobre os membros de uma instituição (e-mail, cargo, etc.), além de informações específicas sobre os funcionário e discentes destas instituições. No esquema *brEduPerson*, a identificação de dispositivos não é contemplada explicitamente, apenas de pessoas [RNP, 2010].

O desafio atual está relacionado às equipes de TI destas instituições, que devem prover este acesso de forma segura, o que inclui: identificar, autenticar e autorizar dispositivos e não somente pessoas. Atualmente, o cenário comum de liberação de acesso à Internet para os dispositivos IoT dentro das instituições é baseado na configuração com chaves de acesso compartilhadas manualmente, em equipamentos que são instalados temporariamente nas salas de ensino.

5. Proposta

As instituições de ensino participantes da CAFe oferecem aos seus usuários a possibilidade de autenticação e autorização de serviços, usando a eduroam em sua rede IEEE 802.11, com cobertura por todo o campus, por meio de uma conta única, cadastrada em sua instituição de origem, adotando o modelo *Single Sign-On* (SSO). Neste sentido propõe-se a utilização desta infraestrutura para realizar a identificação, autenticação e autorização de dispositivos IoT. Para isto, é necessário que na base de dados sejam inseridos campos para armazenar informações sobre os dispositivos. Cada dispositivo IoT, deve possuir um identificador único, que pode ser usado como forma de cadastro na base dados. Além disto, outras informações são necessárias para que a instituição possa confiar neste dispositivo, permitindo desta forma que a autenticação ocorra. Além da identificação e autenticação, as regras de autorização deverão estar presentes para garantir que o dispositivo obtenha acesso controlado.

A proposta de arquitetura, pretende criar um novo esquema LDAP com todos os atributos possíveis que garantam a identificação única do dispositivo, seus recursos e responsáveis. A Figura 2 ilustra a proposta de hierarquia LDAP adaptada a IoT/IIoT.

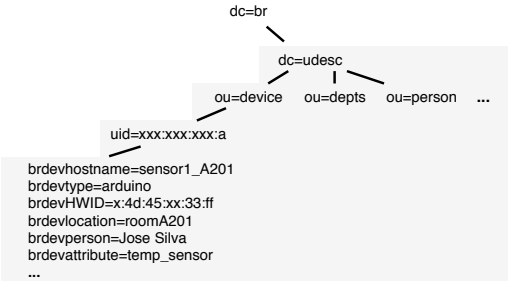

Figura 2. Proposta de novo esquema LDAP.

Este trabalho está em fase inicial de estudos, e os campos que serão propostos ainda não foram avaliados, porém, alguns já podem ser definidos, como: *brdevhostname*, que define o nome de identificação, *brdevperson*, ou seja, pessoa responsável. O identificador único do dispositivo *brdevHWID*, será um dos objetos mais estudados até sua definição final, uma vez que pode-se utilizar o endereço MAC ou outro identificador que possibilite esta diferenciação. Assim, os campos mencionados são uma proposta inicial que será aprimorada nas próximas fases deste estudo. A forma de cadastrado dos dispositivos na instituição de origem e os meios de controle e registro destas informações também fará parte do estudo nas próximas fases.

O processo de autenticação e autorização proposto, é ilustrado na Figura 3. O dispositivo, ao tentar acessar a Internet em sua rede local, é feito a consulta na base CAFe, que redireciona a consulta ao IdP na instituição de origem, na qual ocorre a validação e autenticação, autorizando o acesso.

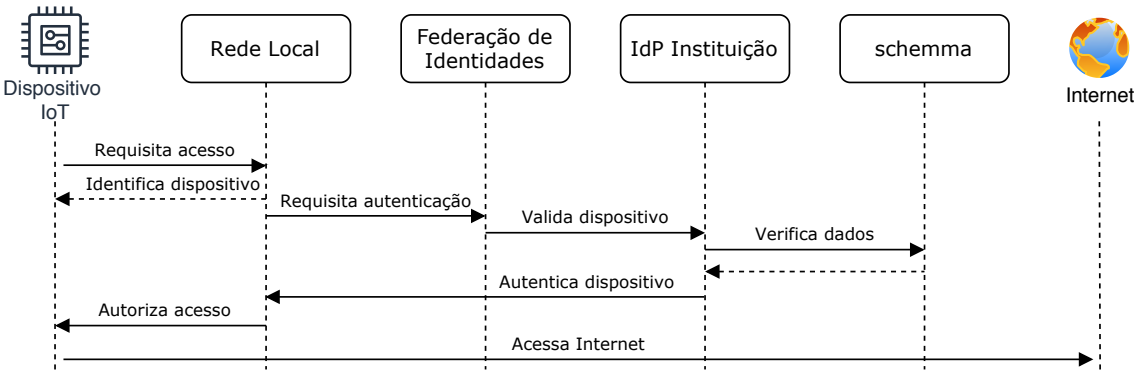

Figura 3. Diagrama de sequência de um dispositivo IoT/IIoT no cenário proposto.

6. Considerações e Trabalhos futuros

Através desta proposta um pesquisador, por exemplo, poderá atuar em outras instituição de ensino, levando seus dispositivos IoT/IIoT, sem a necessidade de reconfigurar o acesso à Internet ou outras configurações de rede, realizar demonstrações ou ainda evoluir sua pesquisa, uma vez que o dispositivo será autenticado e autorizado por sua instituição de origem, usando as credenciais já fornecidas.

Ao implementar este cenário, uma instituição pode oferecer aos seus pesquisadores, um serviço de autenticação e autorização dos seus dispositivos, usados nas pesquisas e projetos de desenvolvimento de novas tecnologias, quando estiver em trânsito, ou seja, quando o pesquisador visitar outra instituição que faça parte das Federações de Identidades, seu dispositivo estará pronto para uso ou demostração, uma vez que não será necessário intervenção de suporte de TI na configuração de acesso, regras de *firewall* ou outras liberações.

Para o processo de desenvolvimento e testes desta proposta pretende-se utilizar a infraestrutura fornecida pela RNP através do GIdLab. [Wangham et al., 2013].

Referências

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805.

Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). The industrial internet of things IIoT: An analysis framework. *Computers in Industry*, volume: 101:1–12.

ENISA (2019). Industry 4.0 - Cybersecurity Challenges and Recommendations. Disponível em: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations. Acesso em: 18/08/2020.

Fagan, M., Megas, K., Scarfone, K., and Smith, M. (2020). Foundational Cybersecurity Activities for IoT Device Manufacturers. Technical Report NIST Internal or Interagency Report (NISTIR) 8259, National Institute of Standards and Technology.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660.

Heng, S. (2014). Industry 4.0: Upgrading of Germany's Industrial Capabilities on the Horizon. SSRN Scholarly Paper ID 2656608, Social Science Research Network, Rochester, NY. Acesso em: 19/08/2020.

Hou, X., Ren, Z., Yang, K., Chen, C., Zhang, H., and Xiao, Y. (2019). IIoT-MEC: A Novel Mobile Edge Computing Framework for 5G-enabled IIoT. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–7. ISSN: 1558-2612.

Hung, M. (2017). Gartner Insights on How to Lead in a Connected World. Disponível em: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. Acesso em:: 19/08/2020.

Neto, A. L. M., Souza, A. L. F., Cunha, I., Nogueira, M., Nunes, I. O., Cotta, L., Gentille, N., Loureiro, A. A. F., Aranha, D. F., Patil, H. K., and Oliveira, L. B. (2016). AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle. In *Proc. ACM SenSys*, Stanford, CA.

RNP (2010). Esquema breduperson - versão 1.0. Disponível em: https://wiki.rnp.br/download/attachments/41190038/BrEduPersonv1_0.pdf. Acesso em:: 08/09/2020.

RNP (2020a). eduroam. Disponível em: https://www.rnp.br/servicos/alunos-e-professores/colaboracao-a-distancia/eduroam. Acesso em:: 17 ago. 2020.

RNP (2020b). Por que eu preciso da cafe? Disponível em: https://www.rnp.br/servicos/gestores-de-ti/hospedagem-e-armazenamento/cafe. Acesso em: 17 ago. 2020.

Sklyar, V. and Kharchenko, V. (2019). ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios. In *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 2, pages 1046–1049.

Stinson, D. (2002). *Cryptography: Theory and Practice,Second Edition*. Chapman and Hall/CRC, 2nd edition.

Wangham, M. S., Mello, E. R., Souza, M. C., and Coelho, H. (2013). Gidlab: Laboratório de experimentação em gestão de identidade. In *Anais do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2013) Workshop de Gestão de Identidade (WGID)*, pages 481–486. Sociedade Brasileira de Computação.

Yang, Y., Wu, L., Yin, G., Li, L., and Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5):1250–1258.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., and Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, 24(3):10–16.