Análise de requisitos de identificação e autorização para dispositivos e gateways de borda em IIoT

Sergio Henrique Silva[1], **Charles C. Miers**[1]

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

sergio.hs@edu.udesc.br, charles.miers@udesc.br

Resumo. *O uso de dispositivos inteligentes para as mais diversas atividades humanas fez emergir o conceito como IoT e também de IIoT quando estes dispositivos são aplicados a indústria. A gestão de identidades e segurança em ambientes IIoT tem limitações e especificidades que resultam em complexidade. O trabalho tem como objetivo identificar e estabelecer critérios que podem mensurar a aplicabilidade de uma abordagem de gestão de identidades em dispositivos aos cenários IIoT. Propõe-se uma análise de requisitos e da arquitetura em IIoT para a identificação de critérios, que posteriormente serão avaliados por experimentos para serem então estabelecidos como válidos.*

1. Introdução e motivação

A *Industrial Internet of Things* (IIoT) pode ser definida como um sistema que conecta e integra sistemas de controle industrial com sistemas empresariais, e também como um conjunto de processos de negócios e análises, usando sistemas de controle industrial que contêm sensores e atuadores [IIC, 2019b]. Estes sistemas também são normalmente de considerável complexidade.

O *Industrial Internet Consortium* (IIC) defende como uma das arquiteturas referenciais em IIoT, a arquitetura de três camadas [IIC, 2019a]: (i) Borda: formada pelos dispositivos físicos, sensores, atuadores e controladores que coletam dados ou executam funções específicas, dispositivos marcados pela pouca disponibilidade de recursos; (ii) Plataforma de Serviço: camada formada pela infraestrutura de comunicação e controle dos dispositivos na rede. A mesma recebe, processa e encaminha comandos de controle da camada corporativa para a camada de borda; e (iii) Corporativa: recebe dados advindos da borda e da camada de plataforma, também emitindo comandos de controle para a camada da plataforma e camada de borda.

Em um cenário de IIoT, no qual existem dispositivos de borda em larga escala com restrições de recursos como processamento e memória os procedimentos de segurança, como a infraestrutura de autenticação devem ser planejados levando em conta as peculiaridades deste cenário [Al-Sharekh and Al-Shqeerat, 2019]. Contudo, a IIoT também necessita de segurança visto que uma falha pode comprometer desde falhas pequenas na operação até riscos a integridade física de seres humanos. Dispositivos não autorizados podem comprometer o controle e a continuidade das operações de uma organização. Diante deste quadro, este trabalho apresenta uma proposta de critérios para análise de abordagens em infraestruturas de autenticação e sua aplicabilidade aos contextos de IIoT.

Na Seção 2 enuncia-se uma introdução a conceitos básicos em identificação e autorização, também sua relação com os cenários de IIoT bem como suas classificações. A Seção 3 introduz os trabalhos relacionados a segurança da informação, com ênfase para autenticação e autorização em dispositivos IIoT. Na Seção 4 propõe-se critérios para análise da aplicabilidade das diversas abordagens de autenticação e autorização.

2. Identificação e autorização em dispositivos

A autorização e autenticação são operações que fornecem o controle de acesso em sistemas distribuídos e usualmente fazem parte de uma infraestrutura de autorização e autenticação (IAA) que faz a gestão de identidades, i.e., *Identity Manager* (IdM). ITU, 2009 afirma que um IdM pode ser definido como um conjunto de tecnologias e processos usados para validar a identidade de uma entidade (um usuário ou um dispositivo) a fim de utilizar um recurso computacional.

Um sistema de IdM é composto pelas entidades: (i) usuário ou dispositivo que utiliza um serviço fornecido por um provedor de serviços; (ii) provedor de identidades *Identity Provider* (IdP), responsável por manter a base de dados dos usuários do domínio e verificar suas credenciais (autenticar usuário ou dispositivo); e (iii) provedor de serviços *Service Provider* (SP), que oferece recursos ou serviços aos usuários [Wangham et al., 2010]. A autenticação é tratada de forma diferente para usuários e para dispositivos em suas operações. Assim, é necessária uma abordagem específica para as abordagens de autenticação em dispositivos. Portanto, neste trabalho, trata-se a autenticação e autorização de dispositivos de maneira transversal em relação a IoT e IIoT.

2.1. Padrões em identificação e autorização em dispositivos

A padronização é um enfoque importante para concretização de ambientes heterodoxos como IIoT. Observa-se um esforço das entidades de padronização de países pelo mundo e de entidades internacionais no intuito de estabelecer padrões. Em relação às abordagens, métodos e boas práticas em segurança, autenticação e autorização relaciona-se padrões advindos das principais instituições de regulação como *International Organization for Standardization* (ISO), *International Telecommunication Union* (ITU) e *National Institute of Standards and Technology* (NIST). A Tabela 1 lista os principais padrões relacionados a segurança de IIoT.

Tabela 1. Padrões relacionados a IIoT: autenticação/autorização de dispositivos.

Orgão	Identificação	Título
IEEE	IEEE P1451-99	Standard for Harmonisation of Internet of Things (IoT) Devices and Systems
IEEE	IEEE 802.15.4	IEEE Standard for Low-Rate Wireless Networks
ISO/IEC JTC	ISO/IEC 27701:2019	Security techniques – Extension to 27001/27002 for Guidelines for privacy information management
ISO/IEC JTC	ISO/IEC 27005:2018	Information technology – Security techniques – Information security risk management
ITU-T	ITU-T X.1361 (09/2018)	Security framework for the Internet of things based on the gateway model environments
NIST	NIST 8259A	IoT Device Cybersecurity Capability Core Baseline

Na Tabela 1 os itens são enquadrados conforme a relação de [Labib et al., 2019] e de acordo com sua aplicabilidade em IIoT, fazendo correlações com a infraestrutura, segurança, autenticação e autorização de dispositivos.

2.2. Taxonomias em identificação e autorização em dispositivos IIoT

Na literatura de taxonomias em autenticação e autorização de dispositivos, observa-se iniciativas em esquematizar as operações e abordagens neste processo. As principais abordagens identificadas que possuem aproximação com o enfoque deste trabalho:

- [El-hajj et al., 2019] : Os autores fornecem uma visão abrangente e atualizada do campo de autenticação em *Internet of Things* (IoT). Disponibilizam um resumo de uma variedade de protocolos de autenticação propostos na literatura revisada no trabalho. Utilizam uma classificação multicritério comparando e avaliando os protocolos de autenticação propostos e mostrando seus pontos fortes e fracos;
- [Lopez et al., 2019]: Elabora-se uma taxonomia de sistemas que fornecem soluções conjuntas para problemas de autenticação e autorização ou soluções para apenas um dos problemas. O trabalho é focado em sistemas já desenvolvidos, em desenvolvimento ou em sua fase experimental, excluindo propostas teóricas.
- [Pulkkis et al., 2006]: Discute e classifica a autenticação de usuários com base em diferentes taxonomias, classificadas em relação a: identificação de usuário, método de autenticação, qualidade da autenticação, complexidade da autenticação e escopo da autenticação.

2.3. Trabalhos relacionados

A segurança da informação é vital para qualquer contexto computacional, mas as especificidades dos contextos de IoT como a escassez de recursos computacionais nos dispositivos faz os desafios na disponibilidade de serviços computacionais tomarem contornos específicos. Em *surveys* relacionando segurança da informação, IoT e IIoT como [Jurcut et al., 2020] e [Sengupta, 2019] faz-se uma relação de alguns trabalhos relevantes em segurança da informação, autenticação e autorização em IoT.

Ammar et al., 2018 pesquisou segurança e privacidade em *frameworks* em IoT, fazendo comparações nos quesitos de autenticação, controle de acesso, comunicação, criptografia de segurança. A pesquisa contribui com critérios de análise de segurança em *frameworks* IoT.

Yang et al., 2017 realizou um estudo sobre soluções de segurança levando em conta as limitações dos dispositivos IoT, fazendo uma classificação de ataques em IoT, autenticação e controle de acesso, mecanismos e análise de segurança em diferentes camadas do modelo OSI.

Lin et al., 2017 apresentou uma visão geral da arquitetura dos sistemas de proteção em IoT, tecnologias habilitadoras, segurança e questões de privacidade na integração da IoT com a *Edge* ou *Fog computing*. Neste trabalho, IoT é apresentada como uma infraestrutura de rede que compreende dispositivos e sistemas para compartilhamento, análise e gerenciamento de recursos. A confidencialidade, integridade, disponibilidade, identificação, autenticação, privacidade e confiabilidade são discutidas como recursos de segurança da IoT.

Nos trabalhos relatados, pode-se observar diversos tipos de experimentos tratando de autenticação e autorização em IoT ou IIoT na literatura. Em conseguinte este trabalho dedica-se a traçar critérios objetivos para análise de arquiteturas ou implementações como as que foram relacionadas de forma que se possa aferir sua aplicabilidade aos cenários IoT ou IIoT.

3. Segurança, autenticação e autorização em dispositivos

Dentre os trabalhos analisados, El-hajj et al., 2019 apresentam uma taxonomia de esquemas de autenticação IoT (aplicável a IIoT) usando diversos critérios selecionados com base nas semelhanças e nas principais características dos esquemas relacionados pelos autores em seu trabalho. Esses critérios são relacionados na Figura 1.

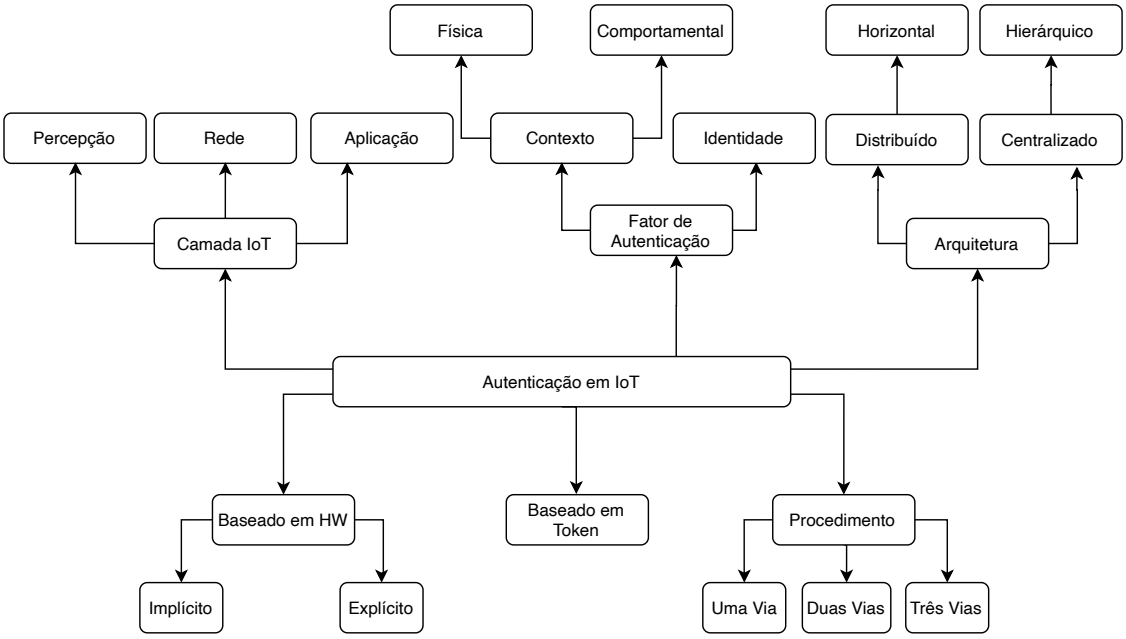

Figura 1. Taxonomia de autenticação IoT. Adaptado de: [El-hajj et al., 2019]

Na classificação (Figura 1) pode-se observar diferentes dimensões relacionadas a autenticação de dispositivos. Este arranjo permite analisar cada implementação ou proposta por múltiplos fatores, relacionando estas implementações aos requisitos de IIoT. Apesar da intrínseca ligação entre a IoT e IIoT, os requisitos de ambas tem alguns pontos de divergência, que tornam abordagens de autenticação aplicáveis ou não aplicáveis aos contextos de IIoT. Partindo-se uma classificação estruturada e dos requisitos dos ambientes IIoT, pode-se traçar os critérios da análise.

4. Critérios para análise da autenticação e autorização em IoT e IIoT

Este trabalho tem como objetivo a análise das abordagens de autenticação de dispositivos inteligentes, especialmente em ambientes IIoT. Neste sentido, analisando os trabalhos listados nas Seções 2.1 e 3, foram definidos quatro critérios iniciais para conduzir esta análise:

1. Adequação aos padrões estabelecidos: As abordagens de gestão de identidades analisadas devem seguir os padrões estabelecidos pelas entidades padronizadoras nacionais e

internacionais. Estas abordagens devem seguir os protocolos derivados destes padrões como o caso do *Wi-Fi Protected Access* (WPA) em referência ao padrão IEEE 802.11. Este critério ainda analisa se a abordagem de utiliza sistemas de autenticação como *openID*, se tem suporte para soluções de autenticação federada com protocolos *ad hoc* como SAML no provimento de identidades.

2. Escalabilidade: Verificar a adequação dos processos de autenticação e autorização à escala industrial, como elaborado em [Consel and Kabac, 2017] que relaciona diversos casos do uso de dispositivos de IoT em larga escala como o gerenciamento de vagas de estacionamento em cidades, monitoramento de sistemas de transporte nas cidades e monitoramento da cadeia de produção de diversos setores industriais. Neste critério serão avaliadas a gestão das identidades pela sua garantia de escalabilidade e disponibilidade para contextos de utilização de dispositivos em grande escala.
3. Uso de técnicas de computação de borda (*Edge Computing*): A computação de borda, também denominada de *Edge Computing* ou *Fog Computing* [Lin et al., 2017]. Neste critério as abordagens de gestão de identidade serão julgadas de acordo com a possibilidade de que o processamento de operações de autenticação e autorização possam ser delegadas a outros dispositivos como um serviço.
4. Comunicação *Machine to Machine* (M2M): Esfahani et al., 2019 relacionam a comunicação M2M como uma das principais características inerentes a IIoT e a Indústria 4.0. Este tipo de comunicação pressupõe que exista a comunicação direta entre os dispositivos e, a partir disso, se torna viável o disparo de ações automáticas entre os equipamentos da camada de borda, e.g., sensores e atuadores. Este critério nivelará as abordagens de autenticação levando em consideração a sua aplicabilidade em cenários de comunicação direta entre dispositivos como M2M.

5. Considerações e trabalhos futuros

Apesar de IoT e IIoT terem como principal característica a disponibilidade de dispositivos inteligentes conectados, a IoT é direcionada ao consumidor final, tem sensores de baixa ou média capacidade e tem baixo risco na utilização. Já a IIoT é empregada em cadeias de suprimentos completas, em larga escala, usando sensores mais precisos em ambientes com riscos potenciais. Neste cenário, a proposta visa atender aos padrões de segurança, além dos requisitos específicos de IIoT

As próximas atividades a serem desenvolvidas nesta pesquisa são: (i) Identificar abordagens estabelecidas ou experimentais em gestão de identidade para os experimentos; (ii) Revisitar e, se necessário, aprimorar a lista de critérios de avaliação; e (iii) Analisar os dados coletados, relaciona-los com os padrões e critérios definidos e, em caso de hipotético sucesso da avaliação, aferir a adequação das abordagens de autenticação e autorização a IIoT.

Agradecimentos: Os autores agradecem o apoio do LabP2D/UDESC e da FAPESC.

Referências

Al-Sharekh, S. I. and Al-Shqeerat, K. H. A. (2019). Security challenges and limitations in iot environments. *IJCSNS International Journal of Computer Science and Network Security*.

Ammar, M., Russello, G., and Crispo, B. (2018). Internet of things: A survey on the security of iot frameworks. *Journal of Information Security and Applications*, 38:8 – 27.

Consel, C. and Kabac, M. (2017). Internet of things: From small- to large-scale orchestration. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 1748–1755.

El-hajj, M., Fadlallah, A., Maroun, C., and Serhrouchni, A. (2019). A survey of internet of things (iot) authentication schemes. *Sensors*, 19.

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M. G., Schmittner, C., and Bastos, J. (2019). A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet of Things Journal*, 6(1):288–296.

IIC, I. I. C. (2019a). The industrial internet of things: Reference architecture.

IIC, I. I. C. (2019b). The industrial internet of things vocabulary technical report.

ITU, I. T. U. (2009). Ngn identity management framework. *Recommendation ITU-T Y.2720*, 01.

Jurcut, A., Niculcea, T., Ranaweera, P., and Le-Khac, N. (2020). Security considerations for internet of things: A survey. *Journal of Network and Computer Applications*, page 19.

Labib, N. S., Brust, M. R., Danoy, G., and Bouvry, P. (2019). Trustworthiness in iot – a standards gap analysis on security, data protection and privacy. *IEEE Conference on Standards for Communications and Networking (CSCN)*.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4:1125–1142.

Lopez, J., Montenegro, J. A., Oppliger, R., and Pernul, G. (2019). On a taxonomy of systems for authentication and/or authorization services. *TERENA Networking Conference*.

Pulkkis, G., Grahn, K., and Karlsson, J. (2006). Taxonomies of user-authentication methods in computer networks.

Sengupta, J. (2019). A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of Network and Computer Applications*.

Wangham, M. S., de Mello, E. R., da Silva Boger, D., Guerios, M., and da Silva Fraga, J. (2010). Gerenciamento de identidades federadas. *GT-STCFed-RNP*, 2010.

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.