

Interoperabilidade entre Dispositivos IoT em Ambientes Industriais Utilizando MQTT, Blockchain Hyperledger Besu e criptografia baseada em atributos: Uma Revisão Sistemática da Literatura

Wesley Novaes Fioreze Costa¹; Arlindo Flávio da Conceição²; Vladimir Emiliano Moreira Rocha³

¹ Universidade Federal de São Paulo – Instituto de Ciência e Tecnologia. (wesley.fioreze@unifesp.br).

² Universidade Federal de São Paulo – Instituto de Ciência e Tecnologia. (arlindo.conceicao@unifesp.br).

³ Universidade Federal do ABC – Centro de Matemática e Computação (vladimir.rocha@ufabc.edu.br).

Resumo: O compartilhamento estratégico de dados entre dispositivos da Internet Industrial das Coisas (IIoT) pertencentes a diferentes organizações é um elemento importante para consolidação de ecossistemas 4.0. Apesar dos avanços tecnológicos, persistem entraves relevantes relacionados à interoperabilidade e, principalmente, ao compartilhamento e controle de dados entre entidades que não mantêm uma relação prévia de confiança. Em particular, observa-se a dificuldade em estabelecer mecanismos que permitam o controle granular de acesso às informações, assegurando simultaneamente privacidade, governança da informação e transparência das regras de compartilhamento. Soluções tradicionais tendem a depender de intermediários centralizados ou de modelos de confiança implícitos, o que limita sua aplicação em ambientes industriais multi-organizacionais. Diante desse cenário, esta pesquisa investigou o estado da arte das soluções de intercâmbio de dados em ambientes IIoT distribuídos, combinando mecanismos de comunicação orientados a mensagens com tecnologias de registro distribuído e técnicas criptográficas. As investigações tiveram foco em propostas com resultados sólidos e testados que utilizaram a tecnologia blockchain para formalizar, gerenciar e tornar auditáveis as permissões de acesso, juntamente com criptografia baseada em atributos (ABE) para garantir que os dados compartilhados sejam acessíveis apenas a entidades que satisfaçam políticas de acesso previamente definidas. Neste panorama, este estudo apresenta uma Revisão Sistemática da Literatura de artigos acadêmicos que aplicam estas tecnologias em projetos de interoperabilidade. Identificou-se que há diferentes abordagens de arquiteturas possíveis para promover interoperabilidade, sendo a privacidade dos dados e o gerenciamento refinado de políticas de acesso os maiores desafios entre elas. Dentre os principais desafios inerentes a arquiteturas de interoperabilidade destaca-se a aderência a regulamentações de segurança ciber-física, compatibilidade com padrões de comunicação industrial e alinhamento com os Objetivos de Desenvolvimento Sustentável (ODS), em especial o ODS 9 (Indústria, Inovação e Infraestrutura). Entre os riscos tecnológicos do projeto, destacam-se a escalabilidade da camada blockchain e a performance computacional em ambientes IIoT. Com o estudado sistemático dos artigos, destaca-se também significativos resultados obtidos e novas possibilidades de modelos de negócio que seriam criados.

Palavras-chave: IoT industrial, Blockchain; Privacidade de dados; Interoperabilidade; Criptografia Baseada em Atributos.

Interoperability between IoT Devices in Industrial Environments Using MQTT, Hyperledger Besu Blockchain, and Attribute-Based Cryptography: A Systematic Literature Review

Wesley Novaes Fioreze Costa¹; Arlindo Flávio da Conceição²; Vladimir Emiliano Moreira Rocha³

¹ Universidade Federal de São Paulo – Instituto de Ciência e Tecnologia. (wesley.fioreze@unifesp.br).

² Universidade Federal de São Paulo – Instituto de Ciência e Tecnologia. (arlindo.conceicao@unifesp.br).

³ Universidade Federal do ABC – Centro de Matemática e Computação (vladimir.rocha@ufabc.edu.br).

Abstract: Strategic data sharing between Industrial Internet of Things (IIoT) devices belonging to different organizations is an important element for consolidating Industry 4.0 ecosystems. Despite technological advances, significant obstacles persist related to interoperability and, especially, to data sharing and control between entities that do not have a prior relationship of trust. In particular, there is difficulty in establishing mechanisms that allow granular control of access to information, while simultaneously ensuring privacy, information governance, and transparency of sharing rules. Traditional solutions tend to depend on centralized intermediaries or implicit trust models, which limits their application in multi-organizational industrial environments. Given this scenario, this research investigated the state of the art of data exchange solutions in distributed IIoT environments, combining message-oriented communication mechanisms with distributed ledger technologies and cryptographic techniques. The investigations focused on proposals with solid and tested results that used blockchain technology to formalize, manage, and audit access permissions, along with attribute-based cryptography (ABE) to ensure that shared data is accessible only to entities that meet predefined access policies. In this context, this study presents a Systematic Literature Review of academic articles that apply these technologies in interoperability projects. It was identified that there are different possible architectural approaches to promote interoperability, with data privacy and refined access policy management being the biggest challenges among them. Among the main challenges inherent to interoperability architectures are adherence to cybersecurity regulations, compatibility with industrial communication standards, and alignment with the Sustainable Development Goals (SDGs), especially SDG 9 (Industry, Innovation and Infrastructure). Among the technological risks of the project, the scalability of the blockchain layer and computational performance in IIoT environments stand out. Through the systematic study of the articles, significant results obtained and new possibilities for business models that could be created are also highlighted.

Keywords: Industrial IoT, Blockchain, Data Privacy, Interoperability, Attribute-Based Encryption.