Métis - Uma Abordagem de Autenticidade Diferenciada para Ambientes IIoT

Mattheus S. Santos[1], **Mario A. R. Dantas**[1], **José M. N. David**[1], **Regina M. M. B. Villela**[1], **Felipe S. Costa**[2]

[1] Departamento de Ciência da Computação
Universidade Federal de Juiz de Fora – Juiz de Fora, MG - Brasil

[2]Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina
Universidade Federal de Santa Catarina – Florianópolis, SC - Brasil

{mattheussantos, mario.dantas}@ice.ufjf.br

{jose.david, regina.braga}@ufjf.edu.br

felipekosta@gmail.com

Abstract. *The security in industrial environments is a growing concern with the integration of Industrial IoT (IIoT).The communication between devices, diverse users and the volume of digital data transferred increase the vulnerability. Aiming to tackle this challenge, we developed studies related to the application of smart contracts with blockchain support to guarantee the integrity of identity authenticity of the digital data that travels within the Industrial IoT (IIoT) environment. Therefore, in this paper, we present the Métis proposal, which represents a differentiated authenticity approach and which was tested through simulations to provide a security landscape to a real industrial 4.0 project.*

Resumo. *A segurança no ambiente industrial é uma preocupação crescente desde a integração dos dispositivos IoT Industriais (IIoT). A comunicação entre esses dispositivos, diferentes usuários e o volume de dados digitais transferidos aumenta a vulnerabilidade. Visando enfrentar este desafio, desenvolvemos estudos relacionados à aplicação de contratos inteligentes com suporte de blockchain para garantir a integridade da autenticidade de identidade dos dados digitais que trafegam no ambiente IoT Industrial (IIoT). Portanto, neste artigo, apresentamos a proposta do Métis, que representa uma abordagem de autenticidade diferenciada e que foi testada por meio de simulações para fornecer um cenário de segurança para um projeto real da Indústria 4.0.*

1. Introdução

A quarta revolução industrial é o novo paradigma no ambiente industrial, definido pela integração dos sistemas ciberfísicos nos ambientes industriais. Esses sistemas são capazes de se comunicar entre si e de tomar decisões autônomas e descentralizadas [Boyes et al. 2018]. Isso possibilitou o desenvolvimento das chamadas fábricas inteligentes, que incluem redes inteligentes, mobilidade, flexibilidade das operações industriais e sua interoperabilidade, integração de clientes e modelos de negócios inovadores. No entanto, essas novas integrações no ambiente industrial trazem novos problemas de segurança, principalmente devido à integração de dispositivos IoT Industriais (IIoT) e

ao grande volume de dados digitais transmitidos dentro deste ambiente da Indústria 4.0 [Pereira et al. 2017].

Uma crescente tecnologia em termos de desenvolvimento e adoção é o blockchain. Dada a natureza de sua arquitetura, o blockchain pode fornecer soluções de confiabilidade e segurança para diferentes domínios além do *e-commerce*. Recentemente, diversas pesquisas têm explorado a implementação do blockchain em ambientes da Indústria 4.0, a fim de garantir a segurança dos dados e recursos destes ambientes. Uma possibilidade de implementar essa segurança por meio do blockchain é fazendo uso de contratos inteligentes. Contratos inteligentes são códigos que executam os termos de um contrato para garantir que certas regras sejam cumpridas. Assim, é possível garantir a segurança dos dados digitais de dispositivos IIoT dentro do ambiente industrial por meio do uso de contratos inteligentes em conjunto com uma rede blockchain [Christidis and Devetsikiotis 2016].

Neste contexto, o projeto Métis foi concebido e desenvolvido como uma abordagem para proporcionar uma autenticidade de identidade diferenciada para requisições no ambiente IIoT. A implementação de uma rede blockchain com contratos inteligentes para realizar validações e verificações garante a integridade e autenticidade de identidade dos dados trafegados, permitindo assim agregar uma abordagem de segurança a um ambiente da Indústria 4.0.

Este artigo está organizado da seguinte forma. Na secção 2 apresentamos alguns trabalhos relacionados ligados às tecnologias que foram utilizadas no desenvolvimento do Métis. Na seção 3 apresentamos a proposta e o processo de desenvolvimento do Métis. Os resultados experimentais são apresentados na seção 4 e, por fim, na seção 5, apresentamos as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Nesta seção, apresentamos trabalhos relacionados usando blockchain e contratos inteligentes, principalmente na área da Indústria 4.0. Essas pesquisas discutem principalmente o uso de blockchain e contratos inteligentes como uma abordagem de segurança e um sistema de gerenciamento de processos.

Em [Hang and Kim 2019], os autores apresentam uma proposta de plataforma IoT integrada usando a tecnologia blockchain, garantindo a integridade dos dados dos sensores IoT, fornecendo uma solução com escalabilidade, alto rendimento, baixo volume de dados e níveis de transparência. O trabalho mostrado em [Garrocho et al. 2019] fornece pesquisa semelhante, mas eles desenvolveram um sistema para apoiar o gerenciamento de processos no ambiente da Indústria 4.0 para avaliar a segurança e o impacto que os contratos inteligentes têm na comunicação entre dispositivos IIoT. Em [Jiang et al. 2019] é apresentado como os contratos inteligentes também podem ser aplicados como uma solução para automatizar transações de pacotes de dados e transações de serviços de análise de dados, trazendo confiança e robustez em uma plataforma descentralizada.

Nossa proposta difere dos trabalhos anteriores trazendo uma camada de segurança inteligente para a Indústria 4.0, verificando não apenas as informações dos dispositivos IIoT, mas também a identidade de quem fez a requisição para realizar a autorização da transação. Desta forma, podemos garantir que apenas aqueles que estão autorizados poderão participar na rede. Isso acontece tanto pela arquitetura proposta pelo Métis, quanto pelas características do blockchain privado.

3. Proposta do Métis

O framework FASTEN [Costa et al. 2020], que foi utilizado como estudo de caso, aborda o problema com a demanda por produtos personalizados da Indústria 4.0, mas carece de uma autenticação de identidade para as requisições feitas para fabricar um produto. A segurança da informação na Indústria 4.0 é uma preocupação crescente, tanto pelos processos quanto pelas tecnologias que a compõe.

Para atacar este problema, concebemos e desenvolvemos o Métis, uma plataforma que integra blockchain e contratos inteligentes com um framework IIoT. Para a plataforma de contratos inteligentes, escolhemos Hyperledger Fabric e utilizamos o FASTEN como framework IIoT. O Métis atua como um protocolo de validação do usuário, garantindo que somente aqueles que foram previamente autorizados poderão solicitar uma operação dentro do framework FASTEN. A arquitetura de nossa proposta pode ser vista na Figura 1. Desenvolvemos a plataforma de segurança dentro da estrutura, atuando como um filtro para todas as requisições antes de serem enviadas para a camada de borda. Com esta rede blockchain, podemos isolar a camada de borda de qualquer acesso direto, e como resultado, evitar qualquer hacking ou acesso indevido a esses dispositivos IIoT.

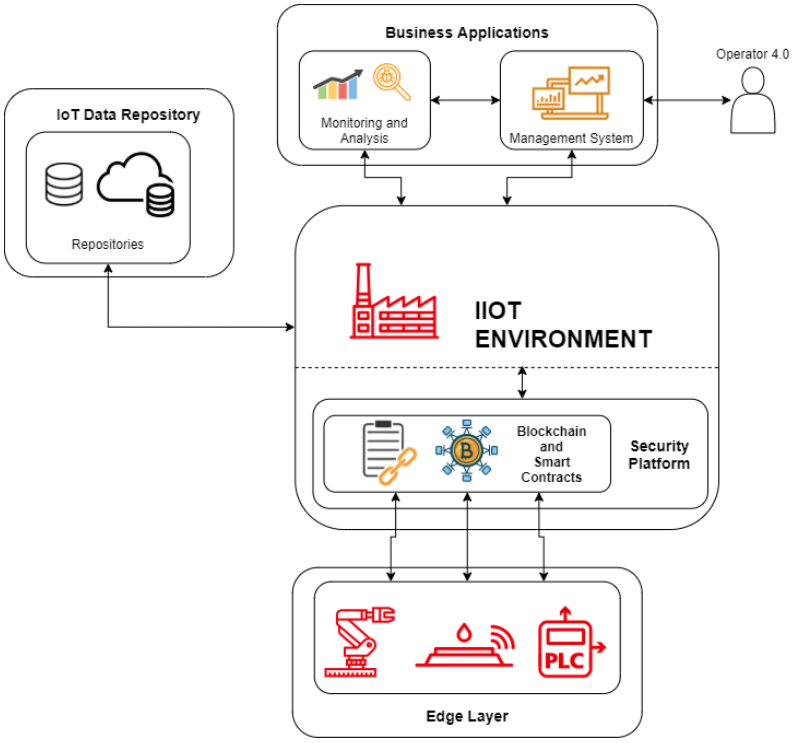

Figura 1. Arquitetura do framework FASTEN com a rede blockchain proposta

Todas as transações emitidas para o framework FASTEN são redirecionadas para nossa rede blockchain, onde Métis pode então validar todas as informações, como quem emitiu a transação, qual dispositivo IIoT e qual operação está sendo solicitada. Então, se a transação for válida, ela será encaminhada ao dispositivo IIoT para executá-la. Também mantemos um registro de todas as transações, válidas ou não, em um banco de dados para que possamos acompanhar todas as transações e tentativas não autorizadas de acesso à plataforma. Este fluxo de trabalho pode ser visto na Figura 2.

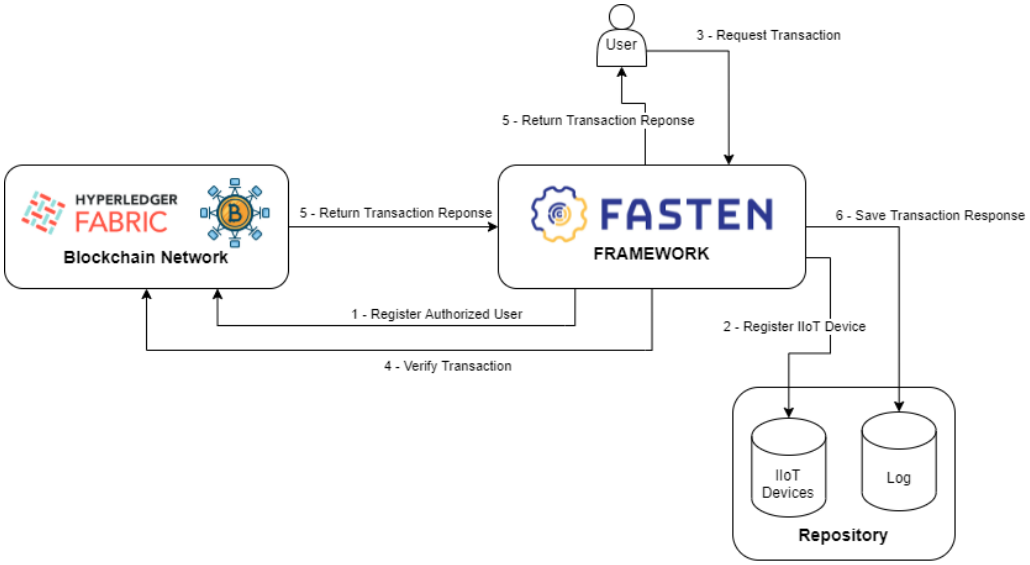

Figura 2. Workflow da rede proposta integrada com o framework FASTEN

3.1. Desenvolvimento

Para testar inicialmente a nossa proposta, desenvolvemos um ambiente simulado, no qual a estrutura de uma requisição recebida do framework FASTEN seria replicada e qual resposta seria devolvida ao framework. O primeiro ambiente simulado foi desenvolvido em um computador pessoal [1]. Este ambiente oferece flexibilidade para nossos desenvolvimentos iniciais, porém, para simulações mais abrangentes, em termos de pesquisa de *data science*, estamos desenvolvendo esforços para execução no NEC Tsubasa, semelhante a uma pesquisa anterior do nosso grupo [do Nascimento et al. 2021].

Com o objetivo de desenvolver o ambiente simulado que manipularia tanto a rede blockchain quanto a requisição e resposta das transações, usamos Node.js [Nodejs 2021] integrado com MongoDB [MongoDB 2021]. Foi desenvolvida uma interface em javascript, na qual foram registrados os usuários autorizados a realizar transações, os dispositivos IIoT e também onde foram preenchidos os dados das requisições que seriam encaminhadas a estes dispositivos.

A primeira etapa neste ambiente é iniciar a rede blockchain, o que é executado automaticamente por scripts fornecidos pelo Hyperledger Fabric, que inicializam imagens no docker contendo os componentes de rede. Em seguida, o administrador é inscrito na rede e após isso, registramos um novo usuário na rede. Utilizamos um UUID (Universally Unique Identifier - Identificador Único Universal) para identificar cada usuário.

Posteriormente, como pode ser visto na Figura 2, registramos as informações de um dispositivo IIoT em nosso repositório, com também um UUID para identificar o dispositivo IIoT, tratando-o como um recurso da plataforma. Neste ponto, Métis está pronto para validar as requisições emitidas por um usuário. Recebemos as informações de uma transação e validamos seu conteúdo. Consideramos uma requisição válida se o usuário estiver registrado em nossa rede blockchain, se o dispositivo IIoT solicitado for válido e

[1] notebook DELL Inspiron 14 3442, 8GB de RAM e processador Core i5-4210U 1.7GHz, com disco rígido de 1TB

se a operação solicitada para este dispositivo também for válida.

Se a requisição for válida, enviamos uma transação para a rede blockchain que é validada com base em nosso contrato inteligente, ou como é chamado pelo Hyperledger Fabric, chaincode. Este chaincode contém os valores que queremos salvar na transação. Optamos por salvar um identificador único para a transação, identificadores de usuário e IIoT, a operação solicitada ao dispositivo e o carimbo de data e hora atuais para rastrear todas as transações realizadas. Independentemente se a transação é válida ou não, nós a salvamos com o seu respectivo resultado em nosso repositório de logs, para que possamos verificar todas as tentativas de acesso à nossa plataforma.

4. Resultados Experimentais

Nesta seção, apresentamos os resultados dos experimentos realizados em nosso ambiente simulado. Testamos possíveis tentativas de requisição que seriam emitidas para a estrutura FASTEN e qual comportamento esperado em cada caso.

Antecipamos quatro casos possíveis, dependendo de quais dados seriam recebidos de uma requisição. O primeiro caso é o que consideramos como um sucesso, no qual os identificadores do usuário e do dispositivo IIoT são válidos e a operação solicitada também é válida. Nesse caso, esperamos obter o usuário da rede blockchain e salvar com êxito a transação na rede. No segundo caso, tratamos como uma requisição inválida se o identificador do usuário não puder ser encontrado na rede. Isso significa que o usuário não tem permissão para realizar uma requisição na plataforma. O terceiro e o quarto casos levam em consideração o identificador do dispositivo IIoT e a operação que este dispositivo pode realizar. Se algum desses valores estiver incorreto, também consideramos a requisição como inválida.

Simulamos algumas requisições, e o comportamento do Métis é mostrado na Figura 3. As transações válidas podem ser vistas nas linhas verdes, e as transações inválidas e respectivos status são representados nas linhas vermelhas. Como afirmado anteriormente, todas as transações apresentadas na Figura 3 foram salvas em nosso banco de dados de log, mas apenas as transações bem-sucedidas foram armazenadas em nossa rede blockchain. Isso garante que tenhamos um histórico de tentativas de transações realizadas e que apenas transações com parâmetros válidos foram realizadas.

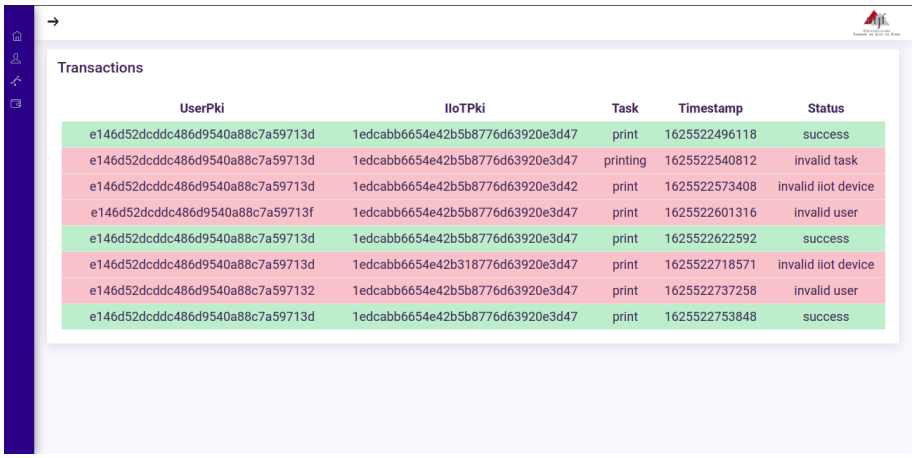

Figura 3. Resultados das Transações Simuladas

5. Conclusões e Trabalhos Futuros

Neste artigo é apresentado uma autenticidade de identidade diferenciada para requisições no ambiente industrial, denominada Métis. Há evidências de que a tecnologia blockchain com contratos inteligentes possui diversos benefícios a oferecer ao ambiente industrial, atuando como uma camada de segurança para proteger recursos, neste caso, dispositivos IIoT, de acessos não autorizados.

Como trabalhos futuros, nosso grupo pretende melhorar as validações e processamento dos dados solicitados, a fim de garantir uma solução de segurança viável para o ambiente da indústria 4.0. Pretendemos também integrar a nossa plataforma com o framework FASTEN, para realizar testes mais elaborados e desenvolver uma solução mais robusta.

Referências

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

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.

Costa, F. S., Nassar, S. M., Gusmeroli, S., Schultz, R., Conceição, A. G. S., Xavier, M., Hessel, F., and Dantas, M. A. R. (2020). Fasten iiot: An open real-time platform for vertical, horizontal and end-to-end integration. *Sensors*, 20(19).

do Nascimento, M. G., Braga, R. M. M., David, J. M. N., Dantas, M. A. R., and Colugnati, F. A. B. (2021). Towards an iot architecture to pervasive environments through design science. In Barolli, L., Woungang, I., and Enokido, T., editors, *Advanced Information Networking and Applications - Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021), Toronto, ON, Canada, 12-14 May, 2021, Volume 2*, volume 226 of *Lecture Notes in Networks and Systems*, pages 28–39. Springer.

Garrocho, C., Ferreira, C. M. S., Junior, A., Cavalcanti, C. F., and Oliveira, R. R. (2019). Industry 4.0: Smart contract-based industrial internet of things process management. In *Anais Estendidos do IX Simpósio Brasileiro de Engenharia de Sistemas Computacionais*, pages 137–142. SBC, Porto Alegre, RS, Brasil.

Hang, L. and Kim, D.-H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity.

Jiang, Y., Zhong, Y., and Ge, X. (2019). Smart contract-based data commodity transactions for industrial internet of things. volume 7.

MongoDB (2021). Mongodb. Available at https://www.mongodb.com/.

Nodejs (2021). Node.js. Available at https://nodejs.org/en/.

Pereira, T., Barreto, L., and Amaral, A. M. (2017). Network and information security challenges within industry 4.0 paradigm.