risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 16/08/2024
Aceitação/Acceptance: 14/10/2024

Segurança no Registro de Dispositivos IoT: Implementação de Autenticação Híbrida

Anna Carolina Ferreira Rosa[1], Vinicius Salgueiro costa[1],
Awatef ali Yousef Rodrigues Fares[1], Francisco De caldas filho[1], Fábio Mendonça[1]

annacarolinafr36@gmail.com; vinicius.salgueiro@uiot.org; francisco.lopes@uiot.org; fabio.mendonca@redes.unb.

[1] Departamento de Engenharia Elétrica, Universidade de Brasília, Campus Universitário Darcy Ribeiro Asa Norte, CEP 70910-900, Brasília/DF, Brasil

Pages: 496-511

Resumo: Com o avanço acelerado da Internet das Coisas, projeta-se que o número de dispositivos ativos chegue a 39,9 bilhões até 2033, demonstrando a necessidade de soluções seguras e eficazes para esse conjunto de tecnologias. Embora técnicas de autenticação tradicionais, como tokens JWT e OAuth2, ofereçam um alto nível de proteção, elas impõem a intervenção humana durante a configuração inicial, limitando a flexibilidade e eficiência do auto-registro de dispositivos IoT em um Middleware IoT. Para enfrentar essas limitações, propõe-se uma abordagem híbrida de autenticação em um Middleware IoT, que combina métodos supervisionados, envolvendo a configuração inicial por um usuário, e não supervisionados, permitindo o registro autônomo dos dispositivos. Essa proposta visa otimizar a segurança e a flexibilidade, garantindo uma integração simples e confiável para a comunicação e gerenciamento de dispositivos IoT.

Palavras-chave: segurança, dispositivo iot, middleware, autenticação híbrida.

Security in IoT Device Registration: Implementing Hybrid Authentication

Abstract: With the accelerated advancement of the Internet of Things (IoT), the number of active devices is projected to reach 39.9 billion by 2033, underscoring the need for secure and effective solutions for this technology ecosystem. Although traditional authentication techniques, such as JWT tokens and OAuth2, offer a high level of protection, they require human intervention during the initial setup, limiting the flexibility and efficiency of self-registration for IoT devices in IoT Middleware. To address these limitations, we propose a hybrid authentication approach within IoT Middleware, combining supervised methods, involving initial configuration by a user, with unsupervised methods, allowing autonomous device registration. This proposal aims to optimize security and flexibility, ensuring a simple and reliable integration for the communication and management of IoT devices.

Keywords: Security, IoT device, middleware, hybrid authentication.

1. Introdução

A tecnologia avança rapidamente, transformando o cotidiano. Em um mundo cada vez mais digital, os dispositivos IoT simplificam tarefas e possibilitam automação e controle. Segundo a Transforma Insights (2023), havia 16,1 bilhões de dispositivos IoT no final de 2023, com previsão de 39,9 bilhões até 2033, crescendo 10% ao ano.

Soluções de interoperabilidades entre dispositivos, resolvem parte dessa integração, entretanto não resolvem as questões relacionadas a seguraça dos registros dos dispositivos (Mendonça, 2024). Os dispositivos IoT, devido ao grande volume de dados que gerenciam e à sua interconexão com outros dispositivos, são frequentemente alvo de ameaças cibernéticas. É crucial adotar medidas de proteção robustas não apenas para os próprios dispositivos, mas também para os dados que eles coletam e transmitem, prevenindo ataques cibernéticos e assegurando a privacidade e a integridade das informações.

Como os dispositivos IoT lidam com grandes volumes de dados, é possível utilizar um *Middleware* IoT (Zhang et al., 2021), que atua como uma camada de software essencial, facilitando a comunicação, o gerenciamento e a integração entre dispositivos IoT e diversas aplicações e serviços. Ele assegura a conectividade entre os dispositivos, coleta e processa dados, e oferece APIs para integrações, promovendo a interoperabilidade e simplificando o desenvolvimento de soluções IoT.

Para realizar a segurança do *Middleware* IoT, frequentemente são utilizadas técnicas de autenticação conhecidas, como *tokens* JWT, OAuth2 (Google Cloud, n.d.), e chaves públicas e privadas (Microsoft, 2024). Essas técnicas requerem o cadastro de um usuário para que ele possa enviar requisições ao *Middleware* IoT. Embora essas abordagens ofereçam um alto nível de segurança, elas limitam a flexibilidade do auto-registro dos dispositivos IoT no *Middleware*, uma vez que o processo de autenticação exige a intervenção de um usuário humano para a configuração inicial.

Dessa forma, com o objetivo de realizar uma abordagem com duas formas autenticações, sendo uma proposta híbrida no *Middleware* IoT. A primeira abordagem é chamada de supervisionada, exigindo que um usuário realize a configuração inicial para o envio de dados e a segunda abordagem é a não supervisionada, permitindo que o próprio dispositivo realize seu cadastro. O objetivo é equilibrar a segurança dos dispositivos e dos dados com a flexibilidade e eficiência no processo de registro, garantindo uma integração simples e segura no *Middleware* IoT.

Além desta introdução, este trabalho também contém o seguinte formato: algumas das obras literárias mais relevantes selecionadas na seção 2. A arquitetura proposta é detalhada na seção 3. A sessão 4 apresenta os dois fluxos para cadastro de dispositivos propostos. A seção 5 apresenta a implementação do Middleware IoT. Os resultados dos testes são apresentados na seção 6. Por fim, a seção 7 contém a conclusão do artigo e sugestões para trabalhos futuros.

2. Trabalhos Relacionados

A segurança em dispositivos IoT (Internet das Coisas) tem sido o foco de inúmeras pesquisas nos últimos anos. Com o aumento do número de dispositivos conectados, a