Janus: A Tool for Managing Identities for IoT Agents Using Verifiable Credentials

Anselmo Lacerda Gomes[1], **Antonio Alex M de Sousa**[1], **Vitor B Estevam**[1],
Elton B Lazzarin[1] **Levi M F de Lima**[1]

[1]LITEC – Laboratório de Inovação Tecnológica e Exploração Científica
Instituto Atlântico – Fortaleza – CE – Brazil

{anselmo_lacerda, alex_sousa, vitor_estevam,
elton_lazzarin, levi_fernandes}@atlantico.com.br

Abstract. *The system proposed in this paper is a solution for monitoring and managing identity issuance processes and access control. This solution uses Verifiable Credentials to add a new security layer over IoT devices and MQTT brokers. Providing a way to deploy and manage Aries agents on IoT Devices through a CLI and ACA-py agents. A credential is issued to the IoT device, specifying the list of sensors it is permitted to use for exporting data. A presentation proof of this credential is required before each sensor data transmission to the broker.*

Resumo. *O sistema proposto neste artigo é uma solução para monitoramento e gerenciamento de processos de emissão de identidade e controle de acesso. Esta solução usa credenciais verificáveis para adicionar uma nova camada de segurança sobre dispositivos IoT e brokers MQTT. Fornecendo uma maneira de implantar e gerenciar agentes Aries em dispositivos IoT através de agentes CLI e ACA-py. Uma credencial é emitida para o dispositivo IoT, especificando a lista de sensores que ele tem permissão para usar na exportação de dados. Uma prova de apresentação dessa credencial é necessária antes de cada transmissão de dados do sensor para o broker.*

1. Introduction

This article delves into Janus, a Proof of Concept (PoC) designed to proficiently handle the intricate processes of issuing identities and managing access control within the realm of decentralized and accredited verifiable identities for IoT devices. Notably, Janus seamlessly integrates with the Dojot platform [de Souza et al. 2020].

Building on the successful implementation of verifiable credentials by the British Columbia government for ensuring user identities, we propose extending the usage of this technology to IoT devices. Just as it enhances trust and security for people, verifiable credentials can play a crucial role in verifying the identities of IoT devices across industries such as healthcare, manufacturing, and logistics. In these sectors, where IoT devices facilitate critical operations like patient monitoring and supply chain optimization, ensuring the integrity of device identities is crucial.

The paper is organized as follows. Section II presents the background of the solution, section III the proposed solution through a Proof of Concept (PoC), section IV demonstrates the performance evaluation of the experiments, also all the tests performed and the results obtained. Section V brings final considerations and future work.

2. Background

2.1. Decentralized Identity

Decentralized Identities are a novel approach to identity management that leverages the principles of self-sovereign identity and blockchain technology. Unlike traditional systems, where identity information is stored and controlled by centralized entities, this new approach empower individuals with the ability to manage their own identity information in a secure, verifiable, and user-centric manner. The credentials are managed through a decentralised application/wallet which allows users to store their credential data privately under their full control and re-use as necessary [Torres 2021].

At the core of the Decentralized Identity framework lies the concept of a Decentralized Identifier (DID). A DID is a unique and persistent identifier that is globally resolvable and does not rely on centralized registries or intermediaries. DIDs are typically registered on blockchain or distributed ledger systems, ensuring immutability and tamper resistance. Furthermore, DIDs are designed to be cryptographically verifiable, enabling secure interactions and data sharing without divulging unnecessary personal information [Torres 2021].

2.2. Verifiable Credentials

Verifiable Credential is a concept that enables the issuance, presentation, and verification of digital attestations in a secure and privacy-preserving manner. At its core, a Verifiable Credential consists of a set of claims about a subject, such as an individual's educational qualifications, professional certifications, or personal attributes. What sets VCs apart is their cryptographically verifiable nature, achieved through the use of digital signatures and decentralized technologies like blockchain [Mukta et al. 2021].

2.3. Zero-Knowledge Proof

In the realm of cryptographic protocols, zero-knowledge proofs (ZKPs) emerge as a mechanism for bolstering security and privacy within communication networks. Zero-Knowledge Proof is a cryptographic protocol exercised to render privacy and data security by securing the identity of users and using services anonymously. This intriguing capability has profound implications in ensuring data integrity, authentication, and privacy preservation [Dieye et al. 2023].

In essence, zero-knowledge proofs enable a prover to convince a verifier that they possess certain knowledge, such as a secret key or a password, without exposing the actual content of that knowledge [Pathak et al. 2023]. The significance of this lies in the fact that sensitive information remains undisclosed, shielding individuals and systems from potential threats such as eavesdropping, unauthorized access, and data breaches [Pathak et al. 2021].

3. Proposed system architecture

This section will present how Janus addresses the challenges associated with IoT device identity management and access control through its unique design and integration with the Dojot platform. The architecture is developed using open-source frameworks and tools, ensuring transparency and collaboration within the technology community.

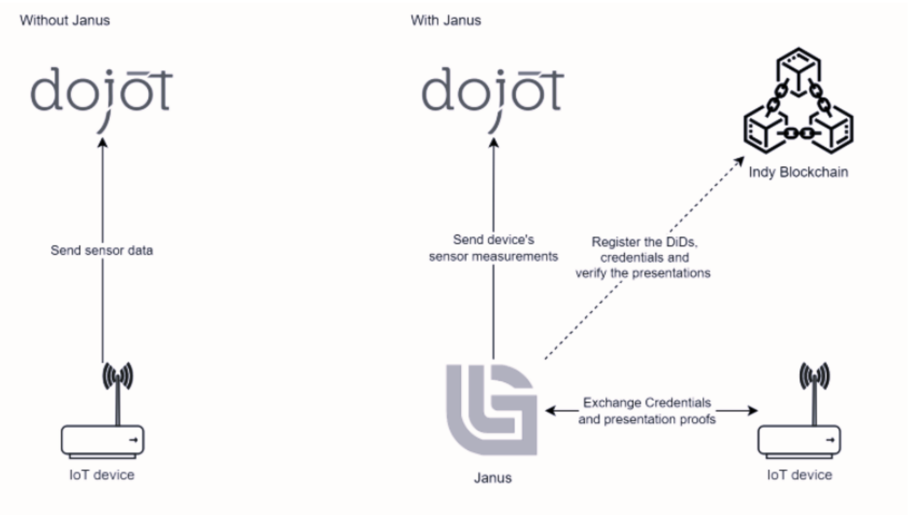
Without Janus
With Janus
dojot
dojot
Send sensor data
Send device's sensor measurements
Register the DiDs, credentials and verify the presentations
Indy Blockchain
Exchange Credentials and presentation proofs
IoT device
Janus
IoT device

Figure 1. Overview of the proposed network using Janus. A Credential is issued to the IoT device with a list of sensors it is allowed to export data and a presentation proof of this credential is required before every sensor data transmission to the broker.

Through the use of Blockchain, Janus uses decentralized identities instead of passwords, makes use of ZKP (Zero-knowledge proof) to increase privacy, access verification and data sharing between devices with verifiable credentials.

3.1. Advantages of Using the Proposed Architecture

1. Mitigation of IoT vulnerabilities: With IoT devices being susceptible to various vulnerabilities, Janus addresses this challenge by incorporating secure identity and access control mechanisms. By eliminating weak passwords and enhancing access management, the architecture directly combats vulnerabilities highlighted in the IoT OWASP Top 10, providing a more robust foundation for IoT deployments.
2. Integration with Dojot platform: Janus seamlessly integrates with the Dojot platform, a significant advantage for IoT ecosystem stakeholders. This integration streamlines the adoption process for organizations already using Dojot, allowing them to benefit from improved security without a complete overhaul of their existing systems.

3.2. Disadvantages of Using the Proposed Architecture

1. Potential performance overheads: The additional layers of identity verification and cryptographic operations introduced by the architecture may lead to potential performance overheads, particularly in resource-constrained IoT environments. Careful optimization is necessary to ensure efficient operation.
2. Limited ecosystem adoption: The adoption of Janus depends on the wider acceptance and integration of decentralized identity concepts within the IoT ecosystem. The architecture's effectiveness might be limited if other platforms and devices do not adopt similar principles.

4. Performance Evaluation

In this section, the experiment and the results obtained by the application will be shown. The experiment carried out will be exemplified and the main characteristics extracted from the metrics will be presented according to the scenarios.

4.1. Simulation Environment

In this section, we present the results of our performance evaluation of the Janus architecture. The experiments were conducted in a controlled environment using Raspberry Pi devices (versions 3 and 4) to deploy agents both locally and remotely. These experiments aimed to assess the efficiency, scalability, and overhead of the Janus architecture in real-world scenario. The experiments were carried out using Raspberry Pi devices due to their popularity in IoT deployments [Zhanying and Yingying 2022]. We utilized Raspberry Pi 3 and 4 models to establish a comprehensive understanding of Janus' performance across different hardware specifications.

4.2. Achieved Results

The comprehensive performance evaluation of the Janus architecture encompassed, as shown in Figure 2, various aspects. We measured the following metrics:

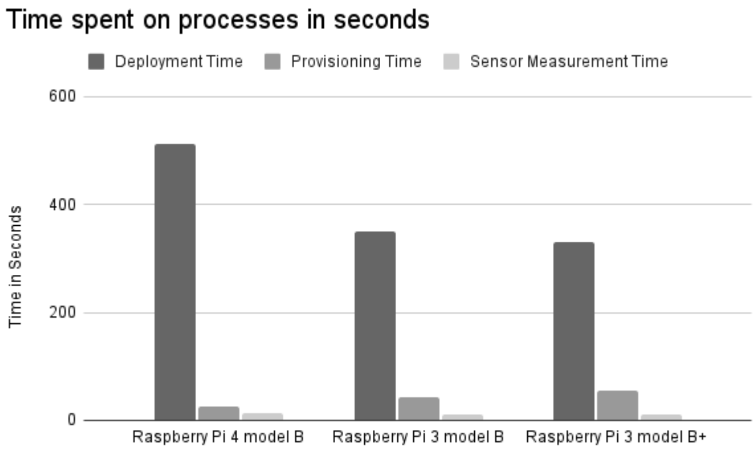

Figure 2. This figure illustrates the time spent on processes within the Janus-enabled IoT networks

1. Deployment Time: It was a critical factor in evaluating the practicality of the system. Our experiments indicated that Janus achieved rapid deployment times, with an average setup duration of 312 seconds. This efficiency ensures swift onboarding of IoT devices without imposing undue delays.
2. Provisioning Time: Referring to the process of issuing verifiable identities to IoT devices was another pivotal metric. Janus demonstrated remarkable efficiency in this regard, with an average provisioning time of 52,5 seconds. The architecture's ability to rapidly provide secure identities contributes to seamless and secure integration of devices into the network.
3. Sensor Measurement Time: it represents the duration between an IoT device generating data and its transmission to the network, and it was also evaluated. Our experiments indicated that Janus facilitated prompt sensor measurement time, with an average duration of 23,75 seconds. This responsiveness is vital for real-time data-driven applications that rely on timely sensor measurements.

In addition to the specific metrics outlined above, we analyzed the resource utilization of the Janus architecture. Monitoring CPU usage and memory consumption provided insights into the architecture's impact on device resources. Notably, as shown in Figures 3 and 4, Janus introduced minimal overhead, with CPU usage averaging 1.0875%. This balanced usage reflects the architecture's ability to accommodate varying workloads without straining device capabilities. Furthermore, memory consumption, consistently below 10%, underscores the architecture's judicious memory allocation and optimal data handling practices.

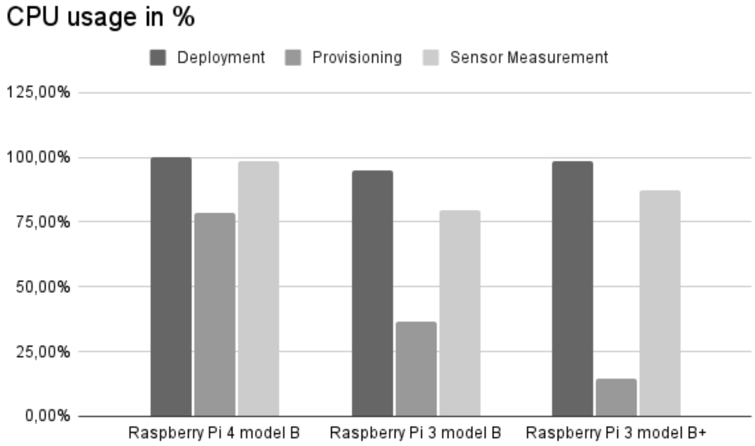

Figure 3. This figure illustrates the resource utilization analysis for CPU within the Janus architecture.

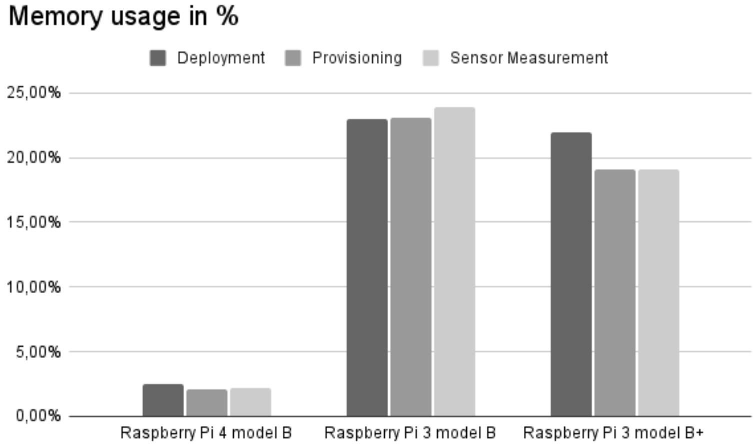

Figure 4. This figure illustrates the resource utilization analysis for memory usage within the Janus architecture.

5. Conclusion and future work

The Janus architecture represents a significant advancement in addressing the complex challenges of identity management and access control within IoT networks. By leveraging decentralized and accredited verifiable identities, Janus enhances security, mitigates vulnerabilities, and streamlines the integration of IoT devices into networks. Our comprehensive performance evaluation demonstrated the architecture's efficiency in deployment, provisioning, and data transmission, further affirming its practicality and effectiveness.

The integration of Janus with the Dojot platform and its reliance on open-source frameworks exemplify a commitment to collaboration and transparency, key factors in building a secure and robust IoT ecosystem. Janus offers a promising solution to the persistent issues of IoT identity and access management, setting the stage for enhanced security and privacy in communication networks. In comparison to the traditional private key/public key method used for IoT devices authentication, Janus offers distinct advantages. Unlike the traditional approach, Janus eliminates the need for password management and key file storage, enhancing security and usability. Also, as each device stores its own verifiable credential, Janus provides a robust authentication mechanism without the risk of key file sharing. This aligns with OWASP IoT Top 10 recommendations, addressing weak passwords and insufficient Privacy Protection.

Overall, Janus offers a more secure and streamlined solution for proving the identity of IoT devices, but requires more computational power than the traditional private key/public key method. By adopting Janus and its robust authentication mechanism based on verifiable credentials, industries can enhance more trust and reliability in IoT ecosystems.

References

de Souza, R. T., dos Santos, G. F., and Zorzo, S. D. (2020). User's privacy management in iot environment using dojot platform. In Latifi, S., editor, *17th International Conference on Information Technology–New Generations (ITNG 2020)*, pages 485–491, Cham. Springer International Publishing.

Dieye, M., Valiorgue, P., Gelas, J.-P., Diallo, E.-H., Ghodous, P., Biennier, F., and Éric Peyrol (2023). A self-sovereign identity based on zero-knowledge proof and blockchain. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/10105959.

Mukta, R., Martens, J., young Paik, H., Lu, Q., and Kanhere, S. S. (2021). Blockchain-based verifiable credential sharing with selective disclosure. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/9343074/.

Pathak, A., Patil, T., Pawar, S., Raut, P., and Khairnar, S. (2021). Secure authentication using zero knowledge proof. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/9544807/.

Pathak, A., Patil, T., Pawar, S., Raut, P., and Khairnar, S. (2023). Efficient smart contract for privacy preserving authentication in blockchain using zero knowledge proof. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/10430710.

Torres, D. A. (2021). Tutorial: Decentralized digital identity with blockchain. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/9530967.

Zhanying, Z. and Yingying, D. (2022). Iot data acquisition terminal based on raspberry pi. *IEEE*. [Online]. Available: https://ieeexplore.ieee.org/document/9723741.