International Journal on Semantic Web and Information Systems
Volume 20 • Issue 1

Blockchain-Based Lightweight Authentication Mechanisms for Industrial Internet of Things and Information Systems

Mingrui Zhao, Shenyang Ligong University, China
Chunjing Shi, Shenyang Ligong University, China*
Yixiao Yuan, Northeastern University, China

ABSTRACT

The industrial internet of things (IIoT) necessitates robust cross-domain authentication to secure sensitive on-site equipment data. This paper presents a refined reputation-based lightweight consensus mechanism (LRBCM) tailored for IIoT's distributed network structures. Leveraging node reputation values, LRBCM streamlines ledger consensus, minimizing communication overhead and complexity. Comparative experiments show LRBCM outperforms competing mechanisms. It maintains higher throughput as the number of participating nodes increases and achieves a throughput approximately 10.78% higher than ReCon. Moreover, runtime analysis demonstrates LRBCM's scalability, surpassing ReCon by approximately 12.79% with equivalent nodes and transactions. In addition, as a combination of LRBCM, the proposed distributed lightweight authentication mechanism (ELAM) is rigorously evaluated against the security of various attacks, and its resilience is confirmed. Experiments show that ELAM has good efficiency while maintaining high security.

KEYWORDS

Blockchain, Identity Authentication, IoT, Lightweight, Reputation

1. INTRODUCTION

The internet of things (IoT) represents the concept of intelligent interaction, seamlessly connecting objects through intercommunication and information exchange. The industrial internet of things (IIoT) applies IoT technology to industrial production, integrating physical devices, sensors, and cloud computing to monitor, control, and optimize industrial processes (Sisinni et al., 2018; Sharma and Sharma, 2022; Yang et al., 2017; Hassija et al., 2019; Yao et al., 2021). In the modern industrial domain, IIoT has become an indispensable part, offering rich opportunities for machine-to-machine communication and automation. However, as devices and sensors become increasingly connected to networks, ensuring the authentication and data integrity of these devices is crucial (Mukherjee and Biswas, 2018; Wang et al., 2022; Nashwan, 2021; Raj and Prakash, 2022; Sengupta et al., 2020;

DOI: 10.4018/IJSWIS.334704 *Corresponding Author

Wang et al., 2019; Feng and Wang, 2022; Danish et al., 2020; Gupta et al., 2021). In the realm of IIoT security and authentication mechanisms, robust authentication mechanisms are urgently needed to protect industrial systems from malicious attacks and unauthorized access.

In recent years, numerous studies have focused on addressing security and authentication challenges in industrial IoT (Chen et al., 2021; Zhuang et al., 2019; Yuan et al., 2021; Yang et al., 2018; Pan et al., 2022; Shen et al., 2020; Esfahani et al., 2017; Xiong et al., 2020; Sadhukhan et al., 2021; Khalid et al., 2020; Stergiou et al., 2021; Wang et al., 2022; Mishra et al., 2022; Wang et al., 2019; Mohammadipanah and Sajedi, 2021; Fu et al., 2022). For example, research in machine-to-machine (M2M) communication has demonstrated outstanding performance compared to traditional methods (Nguyen et al., 2021). The rise of artificial intelligence and machine learning has also led to the proposal of various methods for detecting and preventing malicious software attacks (Zhang et al., 2023; Ling and Hao, 2022; Tembhurne et al., 2022; Xu et al., 2021; Gaurav et al., 2023; Lu et al., 2021; Ling and Hao, 2022; Sharma and Sharma, 2022; Devi and Bharti, 2022; Singh and Gupta, 2022).

Despite significant progress in recent years, device authentication in industrial IoT still faces many challenges. Existing authentication methods may not meet the growing needs of industrial IoT networks, especially in cases with a large number of devices, extensive network scale, and strict requirements for data integrity and confidentiality. Blockchain technology is widely considered a potential solution to address these challenges (Stergiou et al., 2021; Wang et al., 2022; Mishra et al., 2022; Wang et al., 2019; Mohammadipanah and Sajedi, 2021; Fu et al., 2022). Blockchain, as a scalable, distributed, and tamper-resistant ledger, exhibits unique advantages in maintaining consistent information records across different locations. Among these, the Reputation Proof-of-Work (PoR) blockchain proposed by Zhang et al. (2021) stands out for its security, resource efficiency, and decentralization. Additionally, ReCon (Reputation Consensus), incorporating a reputation module, is compatible with other consensus protocols. However, with the increasing interconnection of industrial devices, security threats correspondingly rise, necessitating a multi-layered security strategy to address challenges such as high resource consumption and low efficiency in cases with numerous devices.

This study aims to fill the research gap in the field of industrial IoT device authentication, addressing challenges such as a large number of devices, extensive network scale, and high requirements for data integrity and confidentiality. To tackle these issues, we introduce a lightweight reputation-based consensus algorithm, LRBCM, to achieve efficient consistency of authentication transaction data. The algorithm enhances the throughput and real-time capabilities of industrial IoT devices by reducing computational complexity and communication overhead. Subsequently, we propose a lightweight cross-domain authentication mechanism, ELAM, to ensure the security and efficiency of device authentication. The mechanism improves performance by reducing energy consumption and optimizing interoperability between devices.

The contributions of this paper include:

- Proposing the lightweight reputation-based consensus mechanism (LRBCM) to enhance authentication efficiency.
- Designing the distributed lightweight identity authentication mechanism (ELAM) for cross-domain trustworthy authentication.
- Conducting experiments and comparative analysis to evaluate the proposed consensus algorithm and identity authentication mechanism.

The paper is organized as follows: Section 2 summarizes related research, Section 3 presents the proposed lightweight consensus mechanism and the lightweight identity authentication mechanism, Section 4 presents experimental results and security analysis, and Section 5 provides the conclusion.

The data used to support the findings of this study are included within the article.