TYPE Editorial
PUBLISHED 25 February 2025
DOI 10.3389/fcomp.2025.1566353

Check for updates

OPEN ACCESS

EDITED AND REVIEWED BY
Chintha Tellambura,
University of Alberta, Canada

*CORRESPONDENCE
Arslan Musaddiq
✉ arslan.musaddiq@lnu.se

RECEIVED 24 January 2025
ACCEPTED 03 February 2025
PUBLISHED 25 February 2025

CITATION
Musaddiq A, Azam I, Olsson T and Ahlgren F (2025) Editorial: Machine learning for resource management in industrial Internet of Things. *Front. Comput. Sci.* 7:1566353.
doi: 10.3389/fcomp.2025.1566353

# Editorial: Machine learning for resource management in industrial Internet of Things

Arslan Musaddiq[1]*, Irfan Azam[2], Tobias Olsson[1] and Fredrik Ahlgren[1]

[1] Department of Computer Science and Media Technology, Linnaeus University, Kalmar, Sweden,
[2] Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC, Canada

KEYWORDS

**Internet of Things, resource management, machine learning, IoT applications, industrial IoT**

Editorial on the Research Topic
Machine learning for resource management in industrial Internet of Things

Recent advances in the Industrial Internet of Things (IIoT) field have seen significant growth in recent years. IoT is revolutionizing manufacturing, transportation, oil and gas, and logistics sectors. However, developing IIoT applications poses several challenges, including the limited computational, memory, and energy resources of Internet of Things (IoT) devices. These devices generate large amounts of data at the network edge, making cloud-based processing impractical due to bandwidth constraints, latency, and security risks. Edge computing, which brings data processing closer to the source, offers a viable solution to these challenges. Despite its promise, edge computing faces significant hurdles. One of the primary challenges lies in the diversity of sensor types deployed across different environments, which adds complexity to the system architecture. Furthermore, the large-scale deployment of edge devices and the inherent resource constraints of these devices complicate the task of optimizing performance. Machine learning has emerged as a powerful tool to address these issues, particularly in domains like robotics and natural language processing, where it helps optimize task allocation, improve decision-making processes, and increase the overall efficiency of edge systems. This Research Topic features four articles that explore diverse and cutting-edge applications within the IIoT, including resource management and enhancing security in IoT systems.

The first article, "*An enhanced whale optimization algorithm for task scheduling in edge computing environments*" by Han et al., focused on addressing the challenges of real-time execution due to limited resources in edge computing environments. The authors proposed an enhanced whale optimization algorithm (WOA) incorporating a multi-objective model that considers CPU, memory, time, and resource utilization to optimize task scheduling in edge computing. By leveraging chaotic mapping and a nonlinear convergence factor, the algorithm balances local and global search, significantly reducing cost (by 29.22%), completion time (by 17.04%), and improving resource utilization (by 9.5%). This work significantly addresses the increasing demand for real-time processing capabilities in resource-constrained edge environments.

The second contribution is a comprehensive review entitled "*Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies*" by Kaur et al., which examined the security challenges posed by the increasing complexity of IoT environments. The authors identified key security threats, such as spoofing, distributed denial of service, and man-in-the-middle attacks. This article reviewed various mitigation strategies such as machine learning, deep learning, lightweight encryption, intrusion detection systems, and advanced security protocols. The evaluation of IoT technology, the accompanying security progress, and the need for continued development were discussed. The article also identified IoT application areas, such as healthcare, smart cities, smart homes, and industrial IoT, highlighting the specific security challenges each faces. This review provides valuable insights into current vulnerabilities and presents strategies that could significantly improve the resilience and security of IIoT systems.

In the third article, "*'Below 58 BPM,' involving real-time monitoring and self-medication practices in music performance through IoT technology*" by Merendino et al., the authors explored the development of an Internet of Musical Things system designed to assist an opera singer with a carotid aneurysm during performances. This system monitors the singer's heart rate in real-time and promotes self-healing by providing non-intrusive feedback. The project combined healthcare and the performing arts to help the singer manage stress. The system is an example of "inclusive design," presenting a model for integrating assistive technology into the arts. The project focuses on accessibility and environmental sustainability, and the results showed that it could potentially reduce heart rate peaks during performances.

Finally, the fourth article, "*GPS-free synchronized pseudo-random number generators for internet-of-things*" by Rahman and Chakrabartty introduces a security solution for wireless communication of IoT devices without relying on GPS. The conventional random number generator (RNG) based approach was found to be unsuitable for resource-constrained IoT devices due to their limited power and computational capabilities. The authors proposed a synchronized pseudo-random number generator (SPRNG) architecture that combines a fast linear-feedback-shift-register (LFSR)-based PRNG with a secure seed generator using self-powered timers. These timers operate on the basis of quantum-mechanical tunneling, making them tamper-resistant and capable of providing dynamic seeds that increase the randomness of the output. The SPRNG system facilitates the secure exchange of encryption keys between IoT devices using synchronized timers. The National Institute of Standards and Technology conducted the random number tests and validated this approach. This approach is suitable for use in resource-constrained and adversarial environments, with potential applications ranging from healthcare to military-grade IoT systems.

The research presented in this topic is driving advancements in the IIoT across various industries. From task scheduling and security to real-time monitoring and secure communications, the articles exemplify the breadth of research addressing critical challenges in the field. By providing solutions that improve efficiency, enhance security, and address domain-specific needs, this Research Topic lays the groundwork for future innovations that will further transform IIoT systems.

## Author contributions

AM: Conceptualization, Writing – original draft, Writing – review & editing. IA: Writing – original draft, Writing – review & editing. TO: Writing – original draft, Writing – review & editing. FA: Writing – original draft, Writing – review & editing.

## Acknowledgments

The guest editors would like to thank all authors and reviewers who contributed to this Research Topic. We also thank the editors and staff of Frontiers for their help in navigating the publication process and tools.

## Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.