

Enhancing AI-powered IoT systems: A lightweight edge-based framework for adaptive AI and interoperability

Problem Statement:

In the field of AI-integrated Internet of Things (AIoT), this study is a cornerstone for advanced systems in sectors such as industry, healthcare, and public services.

These systems contribute to increased efficiency and effectiveness in improving and accelerating decision-making through comprehensive advocacy power. However, these electronic devices face a fundamental and significant challenge: multi-performance practices and resource availability. In Industrial IoT (IIoT) environments, AI algorithms achieve up to 99.2% accuracy in object and location identification. However, this puts a strain on the processors and batteries of these edge devices, which are already resource-constrained.

This situation is exacerbated by a lack of standardized compatibility between devices, leading to system failures, sudden outages, and difficulties in data transfer between different platforms. This hinders the realization of a comprehensive internet vision in smart cities. These persistent outages lead to increased latency and data transfer times, a recurring problem in both the healthcare and industrial IoT sectors, requiring immediate and continuous action.

Existing solutions, as research has shown, include "edge computing" in agriculture, which relies on reduced storage and cloud processing. Another approach involves using artificial intelligence (AI) to minimize carbon emissions, as also discussed in research.

After examining all of this, a clear gap emerges: the lack of a lightweight AI framework. Therefore, there is a pressing need for a successful system or model that balances high security with low resource consumption, ensures compatibility across different device manufacturers, and guarantees the sustainability and efficiency of AI-powered IoT systems in complex real-world environments.

Research Objectives:

Main Objective: This research aims to develop a robust AI-based technical framework specifically designed for edge computing. This framework aims to enhance the operational efficiency and security of industrial and service-oriented IoT systems, taking into account the limited resources, processing power, and energy consumption of edge computing devices.

Specific Objectives:

To Evaluation: Identify weaknesses in traditional models when used in dynamic environments and conduct a comprehensive comparative analysis to assess the impact of modern AI algorithms (such as deep learning and reinforcement learning) on energy consumption and response times in resource-constrained IoT devices.

To Design: Create a lightweight AI model that uses adaptive learning or model compression to identify complex cyber threats and predict mechanical problems in real time with minimal strain on edge computing devices.

To Proposal: Develop and propose an intelligent communication protocol that facilitates interoperability, aiming to remove software barriers between different platforms. This will enable secure and seamless data exchange between devices manufactured by different companies within an AI-powered IoT network.

To verification: Using a working model or advanced simulation platforms for realistic scenarios in the healthcare and industrial production sectors, the effectiveness of the proposed framework was tested and verified, and its ability to balance device lifespan under challenging conditions with the accuracy of its results was assessed.

To recommendations: To ensure a secure and sustainable digital transformation, developers and decision-makers should be provided with a set of useful suggestions and technical guidance on how to integrate this framework into existing infrastructures.

Literatures Review:

The Internet of Things (IoT) has changed big time lately. It used to be just about simple data monitoring. Now, it's all about smart IoT systems powered by AI. They build machine learning right into our virtual devices. Some recent studies suggest this shift is behind the latest Industrial Revolution. It's bumped industrial efficiency way up, like 99.8%. That means less wasted resources and fewer people needed.

But honestly, the "black box" thing is a major hurdle. It stops us from using it everywhere. That's especially true in sensitive fields like healthcare. People just don't trust AI conclusions if they can't understand how they got there. It makes them hesitate.

Resource constraints really come up when you look at the research. Those super complex algorithms They chew through an insane amount of processing power, That's what drains the battery and makes sending data to the cloud take forever. Cybersecurity work mostly went into R&D on encryption.

AI apps, like systems that spot intrusions, were a big deal too. Those efforts actually worked out really well. They managed to catch emerging threats 99.2% of the time. Honestly, analyses show AI's key for boosting those small smart energy grids in farming.

It might even cut the world's carbon footprint by 12%. That'd be something. We've gotta ditch these clunky, centralized communication systems. It's clear we need to move towards privacy-focused "light edge" models. They really cut down on how long it takes to get things done. Plus, they sort out those annoying compatibility headaches between different gadgets. Honestly, we probably need more digging into this stuff within a specific setup.

References:

- * Al Rawajbeh, M., et al. (2025). Trustworthy Adaptive AI for Real-Time Intrusion Detection in Industrial IoT Security. Future Internet, 18(2), 82. <https://doi.org/10.3390/iot6030053>
- * Azmat, H. (2024). Artificial Intelligence and the Internet of Things: Transforming Connectivity and Smart Systems. ResearchGate Publication. https://www.researchgate.net/publication/398284167_Artificial_Intelligence_and_the_Internet_of_Things_Transforming_Connectivity_and_Smart_Systems
- * Hasan, M. M., et al. (2025). AI-Driven Quality Control in Manufacturing and Construction: Enhancing Precision and Reducing Human Error. Engineering Informatics, 31, 10270. <https://doi.org/10.25163/engineering.3110270>
- * Kasereka, S. K., et al. (2026). From IoT to AIoT: Evolving Agricultural Systems Through Intelligent Connectivity in Low-Income Countries. IoT Journal, 6(3), 53. <https://doi.org/10.3390/fi18020082>
- * Mustafa, A. (2025). AI-Powered IoT: Transforming Healthcare, Industry, and Smart Infrastructure. ResearchGate Publication. https://www.researchgate.net/publication/39828413_AI-Powered_IoT_Transforming_Healthcare_Industry_and_Smart_Infrastructure
- * Wang, Q., et al. (2024). Ecological footprints, carbon emissions, and energy transitions: the impact of artificial intelligence. Humanities and Social Sciences Communications, 11, 35205. <https://doi.org/10.1057/s41599-024-03520-5>