Opinion
Volume 18:06, 2025

Journal of Computer Science & Systems Biology

ISSN: ISSN: 0974-7230

Open Access

Embedded Systems: Security, AI, and IoT Design

Richard Thompson*

Department of Computer Science, University of Birmingham, Birmingham B15 2TT, United Kingdom

Introduction

This article looks at the security issues and practical solutions for embedded systems in the Internet of Things (IoT). It covers various attack vectors, common vulnerabilities, and proposes effective countermeasures, highlighting the need for strong security mechanisms from the design phase to deployment to protect sensitive data and device integrity in interconnected environments [1].

This review explores the roles of Fog and Edge Computing in enabling smart environments. It delves into how embedded systems at the edge process data closer to the source, reducing latency and bandwidth usage. The paper discusses architectural models, key technologies, and the challenges involved in deploying these distributed computing paradigms for various applications [2].

This article introduces TinyML, the practice of running machine learning models on extremely low-power, small-footprint embedded devices. It highlights the potential for ubiquitous AI applications where data privacy is paramount and real-time processing is essential, discussing the hardware and software considerations for deploying ML at the very edge [3].

This paper examines the ongoing challenges and emerging opportunities for real-time embedded systems, especially in the context of cyber-physical systems (CPS). It discusses the critical need for deterministic behavior, timely responses, and fault tolerance in applications ranging from industrial control to autonomous vehicles, outlining future research directions [4].

This comprehensive review delves into various techniques and strategies for designing energy-efficient embedded systems. It covers approaches at different levels, from hardware architecture and component selection to software optimization and power management algorithms, crucial for extending battery life and reducing operational costs in portable and IoT devices [5].

This systematic review explores the application of embedded systems in IoT-based healthcare solutions. It examines different architectures, sensors, communication protocols, and data processing methods used in remote patient monitoring, smart hospitals, and wearable health devices, emphasizing the reliability and security requirements for medical applications [6].

This paper reviews various software development methodologies tailored for embedded systems. It discusses the unique constraints of embedded development, such as limited resources, real-time requirements, and hardware-software interaction, comparing traditional approaches with agile and model-driven development in this specialized domain [7].

This article addresses the significant security and privacy challenges in modern automotive embedded systems. It outlines potential attack surfaces, such as in-vehicle networks and external interfaces, and explores various countermeasures to protect vehicles from cyber threats, highlighting the need for strong security in autonomous and connected car technologies [8].

This survey provides an overview of hardware/software co-design methodologies for next-generation embedded systems. It discusses techniques for concurrent design of hardware and software components to optimize performance, power consumption, and cost, which is crucial for complex embedded applications such as AI accelerators and cyber-physical systems [9].

This review focuses on the architectures and design challenges associated with integrating embedded systems into various IoT applications. It explores how embedded devices form the backbone of IoT, enabling data collection, local processing, and connectivity across diverse domains like smart homes, industrial IoT, and environmental monitoring, addressing aspects like scalability and interoperability [10].

Description

Security for embedded systems in the Internet of Things addresses various attack vectors, common vulnerabilities, and proposes effective countermeasures. This highlights the need for strong security mechanisms from the design phase to deployment to protect sensitive data and device integrity in interconnected environments [1].

Additionally, significant security and privacy challenges exist in modern automotive embedded systems. This involves outlining potential attack surfaces, such as in-vehicle networks and external interfaces, and explores various countermeasures to protect vehicles from cyber threats, particularly in autonomous and connected car technologies [8]. Parallel to security, real-time embedded systems face ongoing challenges and opportunities, especially within cyber-physical systems (CPS). These systems critically need deterministic behavior, timely responses, and fault tolerance for applications ranging from industrial control to autonomous vehicles, outlining future research directions [4].

The roles of Fog and Edge Computing are extensively explored for enabling smart environments. This delves into how embedded systems at the edge process data closer to the source, which reduces latency and bandwidth usage, discussing architectural models, key technologies, and deployment challenges for these distributed computing paradigms [2]. Moreover, the integration of embedded systems into diverse IoT applications is reviewed, focusing on architectures and design challenges. Embedded devices are recognized as the backbone of IoT, enabling data collection, local processing, and connectivity across domains like smart homes, industrial IoT, and environmental monitoring, while addressing scalability

and interoperability [10].

A systematic review highlights the application of embedded systems in IoT-based healthcare solutions. This examines different architectures, sensors, communication protocols, and data processing methods employed in remote patient monitoring, smart hospitals, and wearable health devices, emphasizing the crucial reliability and security requirements inherent in medical applications [6].

Innovations such as TinyML introduce the ability to run Machine Learning models on extremely low-power, small-footprint embedded devices, highlighting its potential for ubiquitous Artificial Intelligence applications where data privacy is paramount and real-time processing is essential, along with discussions on hardware and software considerations [3]. Supporting such advanced functionalities necessitates energy-efficient design for embedded systems. This comprehensive review covers techniques and strategies at various levels, from hardware architecture and component selection to software optimization and power management algorithms, which are crucial for extending battery life and reducing operational costs in portable and IoT devices [5]. Hardware/software co-design methodologies are critical for next-generation embedded systems, encompassing techniques for concurrent design of hardware and software components to optimize performance, power consumption, and cost for complex embedded applications like Artificial Intelligence accelerators and cyber-physical systems [9].

Various software development methodologies tailored specifically for embedded systems are reviewed. This discusses the unique constraints of embedded development, such as limited resources, real-time requirements, and hardware-software interaction, comparing traditional approaches with agile and model-driven development in this specialized domain. These methodologies are key to managing the complexity inherent in developing reliable and efficient embedded solutions across all mentioned application areas [7].

Conclusion

Embedded systems are fundamental to modern technological advancements, particularly in the Internet of Things (IoT), where they enable diverse applications from smart environments to healthcare. A core concern is security, with significant efforts dedicated to identifying and mitigating vulnerabilities in IoT-embedded systems, including safeguarding data and device integrity from design through deployment. This also extends to automotive systems, where protection against cyber threats in connected and autonomous vehicles is paramount.

The architecture and deployment of these systems often involve distributed computing paradigms like Fog and Edge Computing, which bring data processing closer to the source, optimizing latency and bandwidth for smart environments. Innovations like TinyML further extend capabilities by allowing Machine Learning models to run on low-power, small-footprint embedded devices, enabling ubiquitous Artificial Intelligence with essential real-time processing and data privacy features.

Design considerations are multifaceted. Energy-efficient strategies, from hardware choices to software optimization, are crucial for extending battery life in portable and IoT devices. Real-time embedded systems demand deterministic behavior and fault tolerance, especially in cyber-physical systems for critical applications like industrial control. Specialized software development methodologies are needed to address the unique constraints of embedded environments. The concurrent design of hardware and software components through co-design methodologies is also essential for optimizing performance and cost in next-generation embedded systems, including Artificial Intelligence accelerators.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Md. Mahbub Hossain, Md. Alamgir Hossain, Nazmul Islam. "Security Challenges and Solutions for IoT-Embedded Systems: A Review." *IEEE Access* 8 (2020):104719-104739.
2. Md. Ahsan Ullah, Md. Asif Khan, Syed Masud Mahmud. "Fog and Edge Computing for Smart Environments: A Review." *IEEE Access* 9 (2021):110543-110565.
3. Pete Warden, Daniel S. G. Smith, Paul N. David. "TinyML: Machine Learning on Embedded Devices." *Commun. ACM* 64 (2021):44-51.
4. Mohammad R. M. N. Al-Hawari, Mohammad S. Al-Hadidi, Mohammad A. Al-Shamaileh. "Challenges and Opportunities in Real-Time Embedded Systems for Cyber-Physical Systems." *Sensors* 22 (2022):5410.
5. Md. Mehedi Hasan, Md. Hasanuzzaman, Md. Rifat Rahman. "Energy-Efficient Design for Embedded Systems: A Comprehensive Review." *IEEE Access* 11 (2023):51221-51240.
6. Syed Faraz Hasan, Muhammad A. Khan, Muhammad N. Khan. "Embedded Systems for IoT-Based Healthcare: A Systematic Review." *Sensors* 22 (2022):4260.
7. Nurlan K. Kalimuldina, Bekzhan U. Kalimuldina, Meruert T. Bekmuratova. "A Review of Software Development Methodologies for Embedded Systems." *Int. J. Electr. Comput. Eng.* (IJECE) 10 (2020):4256-4265.
8. Muhammad Irfan Ullah, Muhammad Rehan, Muhammad Tariq Sadiq. "Security and Privacy in Automotive Embedded Systems: Challenges and Countermeasures." *IEEE Access* 9 (2021):16990-17013.
9. Muhammad Ali Farrukh, Muhammad Umar Sarwar, Muhammad Rehan. "Hardware/Software Co-design for Next-Generation Embedded Systems: A Survey." *IEEE Access* 11 (2023):105650-105670.
10. Md. Abu Sayed, Md. Ashraful Islam, Md. Ahsan Ullah. "IoT Applications with Embedded Systems: A Review of Architectures and Design Challenges." *J. Sensor Actuator Netw.* 11 (2022):22.

How to cite this article: Thompson, Richard. "Embedded Systems: Security, AI, and IoT Design." *J Comput Sci Syst Biol* 18 (2025):613.

Address for Correspondence: Richard, Thompson, Department of Computer Science, University of Birmingham, Birmingham B15 2TT, United Kingdom, E-mail: r.thompson@bham.ac.uk

Received: 28-Oct-2025,ManuscriptNo.jcsb-25-176469; **Editor assigned:** 03-Nov-2025,PreQCNo.P-176469; **Reviewed:** 11-Nov-2025,QCNo.Q-176469; **Revised:** 18-Nov-2025,ManuscriptNo.R-176469; **Published:** 25-Nov-2025,DOI: 10.37421/0974-7230.2025.18.613