Chapter 6
Security, Privacy, and Trust of AI–IoT Convergent Smart System

Taye Iyinoluwa Adeyinka
https://orcid.org/0009-0006-4357-6319
University of Science and Technology, Beijing, China

Kehinde Iyioluwa Adeyinka
https://orcid.org/0009-0009-7685-6693
University of Science and Technology, Beijing, China

Ayoade Abolade Emmanuel
https://orcid.org/0009-0007-9846-0927
Harbin Institute of Technology, Shenzhen, China

ABSTRACT

Combining AI with IoT transforms conventional systems into highly adaptive, data-driven, and networked intelligent ecosystems. In fact, most of the modernization drives carried out in smart cities, healthcare, manufacturing, and environmental monitoring industries are based on these very AI-IoT systems. AI-IoT integration will hit the future of technology-driven settings pretty fast through improved user experience, efficient management of resources, and real-time decision-making. This chapter covers all security, privacy, and other issues of trust that develop from the convergence of AI with IoT. It provides detailed insights into recent trends and events in privacy-enhancing technologies, such as differential privacy and federated learning. Secure protocol development and trust management schemes cannot be neglected in a trusted AI-IoT ecosystem. .he theoretical and applied approaches, hence opening up ways to some robust and reliable intelligent ecosystems that shall adapt to evolving security and privacy challenges.

DOI: 10.4018/979-8-3693-8332-2.ch006

1. INTRODUCTION

The convergence of AI with IoT is revolutionizing modern technologies. It enables the implementation of intelligent and networked ecosystems, with broad applications ranging from industrial automation and environment monitoring to healthcare and smart cities. With the help of this AI-IoT integration, the huge sensor networks of the Internet of Things can gather enormous volumes of data, which AI algorithms may then evaluate to produce insights and support real-time decision-making. As these systems spread, they provide previously unheard-of chances for automation and efficiency in various industries, greatly improving the calibre and personalization of services. On the other hand, despite all these benefits of AI-IoT ecosystems, several important disadvantages are brought into wide usage, especially in security, privacy, and trust.

AI-IoT system security is complex and multi-dimensional. Since IoT devices are interconnected, even a single device's smallest weakness can potentially compromise an entire network, exposing important information and functions to bad actors. Cyber threats such as device spoofing, data manipulation, and Distributed Denial of Service (DDoS) assaults pose serious hazards and potentially seriously compromise user privacy and system integrity (Khatun et al., 2023). According to Lu et al. (2023), the Mirai botnet attack is a well-known example of how hijacked IoT devices could be used to overwhelm network infrastructure and cause widespread service outages. This incident shows the need for better security protocols in the AI-IoT ecosystem. These should involve multilayer strategies comprising encryption, secure boot mechanisms, and intrusion detection systems capable of immediately recognizing and eliminating the threat (Schmidt, Biessmann, & Teubner, 2020). Additionally, by providing decentralized, tamper-resistant data management frameworks that improve authentication and data integrity across devices, blockchain technology has emerged as a promising way to enhance AI-IoT security (Commey et al., 2024).

Also, one of the most pressing concerns over AI-IoT systems is the issue of privacy. They are deploying IoT devices in private, mostly houses, cars, and personal wearables-results in the continuous gathering of data. There are serious concerns over data ownership and privacy because this data frequently contains extremely sensitive information about users' routines, habits, and health (Mohanta et al., 2020). These problems are made worse by the incorporation of AI into these systems, which enables the analysis and deduction of extremely private information that users might not even be aware is being taken. For example, data concerning mobility patterns, device usage, and energy consumption can provide personal details about a person's daily routine in smart home settings, raising worries about privacy violations and surveillance (Saied et al., 2013). Privacy-preserving strategies like differential privacy and federated learning are increasingly being used to mitigate these dangers. For instance, federated learning enables training AI models across distributed devices without raw data centralization, protecting users' privacy while model optimization is still enabled (Baniecki & Biecek, 2024). Meanwhile, adding differential privacy into a dataset by inserting controlled noise complicates drawing any inferences about individual data points, given that it balances the requirements of performing an accurate analysis with preserving user privacy. By showing that technical innovation can align with ethical data practices, these strategies are essential for building trust in AI-IoT systems.

Trust is one of the difficult things to protect, but it forms the core tenet for the uptake and acceptability of AI-IoT ecosystems. Besides their data protection, users have to be secured in the fairness and transparency of the operation of such systems. Prejudice, justice, and accountability concerns arise when consumers of these AI-IoT systems find it difficult to comprehend the inner decision-making workings of many AI algorithms because of their intricacy and opacity. Explainable AI, which allows users to see and