Chapter 7
Securing Web Data and Privacy in AIoT Systems

Marius Iulian Mihailescu
https://orcid.org/0000-0001-9655-9666
Universitatea Spiru Haret Bucureşti, Romania

Stefania Loredana Nita
Military Technical Academy "Ferdinand I", Romania

ABSTRACT

The exponential growth of Artificial Intelligence of Things (AIoT) has resulted in an unparalleled fusion of AI with IoT technologies, giving rise to intricate systems that present vast opportunities for automation, productivity, and data-centric decision-making. Nevertheless, this amalgamation also poses substantial obstacles regarding safeguarding online information and upholding confidentiality. The chapter extensively examines the difficulties associated with these issues and the tactics employed to surmount them. The chapter commences by delineating the distinctive susceptibilities inherent in AIoT systems, with a particular emphasis on how the interconnection of AI and IoT technologies gives rise to novel avenues for data breaches and privacy infringements. It then explores the most recent approaches and technologies used to protect data sent over AIoT networks. These include improved encryption methods, secure data transfer protocols, and solutions based on blockchain technology. A substantial chunk of the chapter focuses on privacy-preserving strategies in AIoT. The text examines the equilibrium between data usefulness and privacy protection. It delves into techniques like anonymization, differential privacy, and federated learning as means to safeguard user data while ensuring the effectiveness of AIoT systems. The chapter also examines regulatory and ethical factors, thoroughly examining current and developing legislation and regulations that oversee data security and privacy in AIoT. The content incorporates case studies and real-world examples to demonstrate the pragmatic implementation of theoretical principles. Ultimately, the chapter predicts forthcoming patterns and difficulties in this swiftly progressing domain, providing valuable perspectives on possible AIoT security and privacy protocol advancements. This resource is vital for professionals, researchers, and students engaged in AIoT, cybersecurity, and data privacy. It provides them with the necessary information and tools to protect against the ever-changing threats in this dynamic field.

DOI: 10.4018/979-8-3693-1487-6.ch007

1. INTRODUCTION TO AIOT AND WEB SECURITY

The combination of Artificial Intelligence (AI) and the Internet of Things (IoT), referred to as the Artificial Intelligence of Things (AIoT), is a significant transformation in the technological field. Integrating AI technology into IoT systems enhances their capabilities, facilitating more efficient, autonomous, and intelligent decision-making processes. Nevertheless, as these systems grow more intricate and interconnected, primarily through web technologies, they become more susceptible to cyber dangers. This requires a robust and comprehensive approach to security, namely in protecting web data and preserving user privacy.

AIoT systems can efficiently handle substantial amounts of data (Ramos et al., 2022), frequently in real-time, to extract essential insights and execute automated actions. These systems are utilized in diverse domains like healthcare, smart cities, industrial, and home automation. The widespread management of data presents the difficulty of guaranteeing data integrity, confidentiality, and availability. Furthermore, because of the frequent interconnection of AIoT devices via the internet, they are susceptible to the inherent weaknesses of web technologies. This encompasses potential hazards such as unlawful data breaches, data tampering, and diverse cyber assaults.

This chapter delves into the complexities of protecting web data and preserving privacy in AIoT systems. We want to equip readers with the essential knowledge and skills to manage cybersecurity challenges in this quickly evolving sector successfully. This book offers a comprehensive guide for anyone looking to improve the security of AIoT systems. This course encompasses the fundamental principles of Artificial Intelligence of Things (AIoT) and internet security, sophisticated defense tactics, and adherence to regulatory standards. At the outset of our voyage, we will analyze the field's current state and estimate the future challenges and opportunities in this rapidly evolving subject.

Web security in the context of AIoT encompasses more than just protecting data from unwanted access. It also involves preventing any manipulation of the AI components. Manipulation of AI models might result in erroneous judgments, potentially resulting in substantial damage, particularly in vital domains such as healthcare or self-driving vehicles. Furthermore, ensuring the privacy of users is of utmost importance. AIoT systems frequently manage sensitive personal information, and it is essential to guarantee the anonymity and privacy of this data. This is important to preserve user confidence and adhere to increasingly strict global data protection standards.

The convergence of Artificial Intelligence of Things (AIoT) and web technologies gives rise to a dynamic and intricate cybersecurity landscape. Conventional security measures are frequently insufficient to tackle the distinct problems presented by these linked systems. Hence, it is crucial to possess knowledge of AIoT designs and online security concepts. This encompasses expertise in network security, application security, data encryption, access control, and the ethical and legal aspects of data privacy.

Comprehending AIoT can be exciting, contingent upon the specific case study and practical circumstances. To address this obstacle, let us consider a hypothetical scenario where our residential thermostat can acquire knowledge about our tastes and autonomously regulate the temperature accordingly. Similarly, envision a scenario where factory equipment can anticipate and avert future malfunctions. The power of AIoT lies in the ability of physical devices to gather data, connect, and utilize AI algorithms to carry out intelligent actions. Nevertheless, the extensive array of interconnected gadgets, frequently equipped with restricted computational capabilities and security attributes, generates a substantial vulnerability for malevolent individuals.