RADemics

AI Powered Smart Buildings with Automated Energy Optimization and Adaptive Facility Management Systems

Ganesh Babu Oorkavalan, Kundan Baddur,
Varsha Rahul Dange
Anna University Regional Campus Madurai,
Teegala Krishna Reddy Engineering College,
Vishwakarma Institute of technology

AI Powered Smart Buildings with Automated Energy Optimization and Adaptive Facility Management Systems

[1]Ganesh Babu Oorkavalan, Assistant Professor (Sl. Gr), Civil Engineering, Anna University Regional Campus Madurai, Madurai 625019. oganeshbabu@auttvl.ac.in

[2]Kundan Baddur, Assistant Professor Computer Science & Design, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Hyderabad, Telangana-500097. kundanb83@gmail.com

[3]Varsha Rahul Dange, Assistant Professor, Department of Information technology, Vishwakarma Institute of technology, Bibwewadi, Pune, Maharashtra. dange.varshar@gmail.com

Abstract

The integration of Artificial Intelligence (AI) in smart building systems has led to significant advancements in automated energy optimization, adaptive facility management, and enhanced operational efficiency. However, these innovations have introduced complex challenges surrounding data privacy, security, and system integrity. This book chapter explores the critical aspects of AI-powered smart building systems, emphasizing the importance of robust security frameworks and privacy-preserving technologies. Key focus areas include the vulnerabilities inherent in Internet of Things (IoT) devices, data transmission protocols, and the role of Trusted Execution Environments (TEEs) in safeguarding sensitive information. Furthermore, the chapter discusses the implementation of incident response and recovery strategies to address data breaches, highlighting the necessity for effective policies and real-time monitoring systems. It also delves into the regulatory landscape surrounding smart building data, presenting best practices for ensuring compliance with data protection laws. The growing dependence on AI and IoT in building management underscores the need for continuous innovation in security measures and privacy solutions, aiming to foster a secure, efficient, and privacy-conscious environment for occupants and administrators alike.

Keywords: AI-powered smart buildings, data privacy, IoT security, Trusted Execution Environments (TEEs), incident response, regulatory compliance.

Introduction

The advent of Artificial Intelligence (AI) and Internet of Things (IoT) technologies has significantly reshaped the architecture and operation of modern buildings, giving rise to the concept of "smart buildings [1]." These structures leverage AI algorithms and IoT devices to optimize energy consumption, enhance operational efficiencies, and improve the overall experience of occupants [2]. The integration of AI facilitates automated building systems, allowing for real-time adjustments in heating, ventilation, air conditioning (HVAC), lighting, security, and other facility management aspects [3]. IoT-enabled devices, such as sensors, cameras, and actuators, continuously monitor building performance and occupant behavior, providing a wealth of data that can be used to improve decision-making processes [4]. Together, AI and IoT contribute to the creation of highly adaptive environments that can respond dynamically to changing conditions, offering enhanced energy efficiency, cost savings, and comfort for building users [5].

While these advancements offer considerable benefits, they also introduce a host of challenges related to security, privacy, and data management [6]. As smart buildings become more reliant on interconnected systems, the risk of cyberattacks and data breaches grows exponentially [7]. The continuous exchange of data between IoT devices and central control systems raises concerns about the privacy of sensitive information, such as occupancy patterns, usage behaviors, and energy consumption [8]. This data, if intercepted or misused, could be exploited for malicious purposes, potentially compromising both the privacy of occupants and the operational integrity of the building [9]. Therefore, ensuring the security and privacy of smart building systems is critical to their continued success and widespread adoption [10].

To address these concerns, a robust security framework is essential for protecting the vast amounts of data generated and transmitted within smart buildings [11]. Traditional security measures, such as firewalls and antivirus software, are no longer sufficient to address the complexities introduced by IoT and AI technologies [12]. New approaches are needed that account for the unique characteristics of smart buildings, including their decentralized nature, real-time data exchange, and continuous connectivity [13]. The deployment of advanced security technologies, such as encryption, secure data storage, and access control systems, is necessary to safeguard sensitive information [14]. Furthermore, the integration of Trusted Execution Environments (TEEs) can enhance data privacy by enabling secure computation and ensuring that sensitive data is processed without exposure to unauthorized parties [15].

In security measures, privacy-preserving techniques must be incorporated into the design and operation of smart building systems [16]. These techniques aim to minimize the amount of personal data collected, limit its retention, and ensure that data is used only for its intended purposes [17]. Privacy-enhancing technologies (PETs), such as anonymization, pseudonymization, and differential privacy, are critical in safeguarding occupant privacy while still allowing for the collection of valuable data to improve building performance [18]. Smart building systems should be designed with privacy by default, ensuring that occupants' personal information is protected throughout the entire lifecycle of the system [19]. Regulatory compliance with data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, must be ensured to provide legal safeguards for individuals' data [20].