RADemics

Smart Locker Systems with IoT and Biometrics for Secure Access in Campus Facilities

Sanjeev Kumar Sharma, Madanu Thambi Joseph
Technocrats Institute of Technology (Excellence),
Hyderabad Institute of Technology and Management

Smart Locker Systems with IoT and Biometrics for Secure Access in Campus Facilities

[1]Sanjeev Kumar Sharma, Professor, Department of Computer Science and Engineering, Technocrats Institute of Technology (Excellence), Bhopal, Madhya Pradesh, India. spd50020@gmail.com

[2]Tunga Venkanna Babu, Assistant professor, Electronics and Communication Engineering, Hyderabad Institute of Technology and Management, Gowdavally, Medchal Malkajgiri, Hyderabad, Telangana, India. venkannat.ece@hitam.org

Abstract

This book chapter explores the integration of Internet of Things (IoT) and biometric authentication technologies in the development of smart locker systems for secure access within campus environments. With the increasing demand for efficient, secure, and automated solutions, smart locker systems are emerging as a transformative solution in educational institutions, offering enhanced security, real-time monitoring, and improved user experience. The chapter delves into the architecture and design of these systems, focusing on key components such as IoT sensors, biometric devices, and data encryption protocols. It addresses the challenges faced in securing communication, data transmission, and user privacy, providing best practices for ensuring the integrity and confidentiality of sensitive data. The performance and reliability of system components are critically evaluated, emphasizing the importance of scalability, responsiveness, and integration with existing campus infrastructure. The chapter further examines future trends, including the adoption of 5G connectivity, artificial intelligence, and blockchain technologies, which promise to elevate the capabilities of smart locker systems. With a focus on practical applications, this work serves as a comprehensive guide for the deployment of secure, efficient, and adaptable smart locker solutions in modern campus facilities.

Keywords: Smart Locker Systems, Internet of Things (IoT), Biometric Authentication, Campus Security, Data Encryption, System Performance.

Introduction

The rapid adoption of digital technologies in educational environments has prompted a fundamental shift in how campus facilities are managed, particularly with regard to securing and storing personal belongings [1]. Traditional locker systems, reliant on physical keys or PIN codes, have become increasingly inadequate to meet the demands of modern campuses, where security, efficiency, and accessibility are paramount [2]. With an increasing focus on enhancing user experiences and ensuring the safety of personal items, campuses are turning to more advanced, secure alternatives, such as smart locker systems powered by the Internet of Things (IoT) and biometric authentication technologies [3]. These systems offer significant advantages over traditional lockers [4], including real-time monitoring, increased security, and seamless access through biometric identification methods such as fingerprint scanning, facial recognition, and iris scanning [5].

The integration of IoT technology plays a pivotal role in transforming traditional locker systems into smarter, more efficient solutions [6]. IoT-enabled lockers are equipped with sensors that communicate with central management systems to provide real-time updates on locker occupancy, usage patterns, and maintenance needs [7]. This connectivity allows campus administrators to remotely manage locker assignments, track usage statistics, and optimize resource allocation without needing physical intervention [8]. The ability to monitor locker status in real time also reduces the likelihood of maintenance issues, ensuring that lockers remain operational and accessible to users at all times [9]. Moreover, IoT-powered systems enable easy scalability, allowing campuses to expand their locker infrastructure in response to growing student populations or increased demand [10].

Biometric authentication technologies offer another transformative aspect of smart lockers, addressing the limitations of traditional security methods such as keys and codes [11]. By utilizing unique biometric identifiers such as fingerprints or facial features, smart locker systems provide a higher level of security that is difficult to bypass or replicate [12]. This reduces the risks of unauthorized access, ensuring that only the designated user can access their personal storage [13]. Biometrics also eliminate the need for physical keys or access cards, which can be lost, stolen, or forgotten [14]. The seamless, contactless nature of biometric verification enhances user convenience and ensures that locker access is swift, secure, and straightforward [15].