RADemics

IoT Based E Governance Platforms for Seamless Public Administration Smart Citizen Engagement and Service Automation

Suganyadevi M, karthika G, Srikanta Kumar Sahoo
PPG Institute of Technology, Bhubaneswar Engineering College

IoT Based E Governance Platforms for Seamless Public Administration Smart Citizen Engagement and Service Automation

[1]Suganyadevi M, Assistant professor, ECE, PPG Institute of Technology, Coimbatore. suganyamurugesan3@gmail.com

[2]karthika G, Assistant professor, ECE, PPG Institute of Technology, Coimbatore.

[3]Srikanta Kumar Sahoo, Assistant Professor, CSE, Bhubaneswar Engineering College, Bhubaneswar, Odisha, India. sks.nita@gmail.com

Abstract

The integration of Internet of Things (IoT) technologies into public administration offers transformative opportunities for enhancing governance, improving citizen engagement, and automating government services. However, the seamless incorporation of IoT into existing government infrastructures presents significant challenges, including issues of interoperability, data security, and cost-effective deployment. This chapter explores the strategic approaches required to overcome these barriers, with a focus on the integration of IoT with legacy systems, ensuring data compatibility, and addressing privacy concerns. It highlights the need for standardized APIs, middleware solutions, and economic models that support sustainable IoT deployment in government settings. Furthermore, the chapter delves into the legal and compliance challenges that arise when managing IoT data within established regulatory frameworks, proposing methodologies to ensure adherence to privacy and data protection laws. Finally, it discusses innovative strategies for optimizing IoT integration in public administration, with an emphasis on building scalable, secure, and efficient infrastructures. This research contributes valuable insights into the practicalities of IoT adoption in government, offering a comprehensive roadmap for future smart governance initiatives.

Keywords: Internet of Things, Smart Governance, Public Administration, IoT Integration, Legacy Systems, Data Privacy.

Introduction

The Internet of Things (IoT) is rapidly reshaping the landscape of public administration, offering transformative opportunities for enhancing government services, improving operational efficiency [1], and fostering greater citizen engagement. As cities and countries move toward becoming "smart" through digital transformation, IoT technologies play a pivotal role in automating administrative functions, optimizing resource allocation, and enabling real-time decision-making [2]. From smart traffic management to environmental monitoring and public health surveillance, IoT systems promise to create more responsive, transparent, and sustainable governance frameworks [3]. The integration of IoT into public administration is expected to not

only streamline operational processes but also make public services more accessible and tailored to citizens' needs [4].

The adoption of IoT in public administration faces substantial challenges, particularly when integrating IoT technologies with legacy government systems [5]. Many governmental infrastructures were originally built with outdated technologies that were not designed to accommodate the scale, complexity, and variety of data generated by modern IoT devices [6]. These legacy systems were often isolated from each other, creating silos that hinder efficient data exchange and interoperability [7]. Integrating new IoT-based solutions into these existing frameworks requires overcoming compatibility issues between old and new technologies, necessitating the development of specialized tools and middleware that can bridge these gaps [8].

A significant concern when deploying IoT solutions within public administration is data compatibility and interoperability [9]. As IoT devices collect vast amounts of real-time data from various sources, ensuring seamless communication between devices, platforms, and legacy systems is crucial for effective service delivery [10]. Data collected by IoT sensors must be compatible with existing databases, management tools, and reporting systems used by governments [11]. For IoT-enabled services to operate smoothly, these systems need to work in harmony, sharing data and making decisions based on shared information [12]. This requirement for interoperability can be especially challenging for governments with fragmented digital infrastructures and varying degrees of technological maturity across departments [13].

Security and privacy concerns are paramount when implementing IoT technologies in public administration [14]. Governments are custodians of sensitive data, including citizens’ personal information, health data, and financial records [15]. As IoT devices generate massive volumes of real-time data, ensuring robust security measures to protect this information becomes a significant challenge [16]. Inadequate security can lead to breaches that expose vulnerable citizens to identity theft, surveillance, and other forms of exploitation [17]. Integrating IoT technologies requires adherence to privacy laws and compliance with regulatory frameworks such as the General Data Protection Regulation (GDPR) in Europe, which imposes strict requirements on data handling and citizen consent. Balancing the need for efficient service delivery with the responsibility to protect individual privacy is one of the most complex aspects of IoT integration in the public sector [18].