IoT Security Challenges and Solutions in Smart Cities

Taylor Rodriguez
PhD
Delft University of Technology
Mekelweg 5, 2628 CD Delft, Netherlands

Casey Campbell
Dr.
University of São Paulo
Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010, Brazil

Robin Gonzalez
Prof.
KTH Royal Institute of Technology
Brinellvägen 8, 114 28 Stockholm, Sweden

Abstract. This article examines the security challenges associated with the Internet of Things (IoT) in the context of smart cities. As IoT devices proliferate, ensuring their security becomes critical to protect sensitive data and maintain public safety. The paper discusses various threats such as unauthorized access and data breaches, and explores solutions including encryption techniques and secure communication protocols. The role of policy and regulation in enhancing IoT security is also highlighted.

Keywords: IoT security, Smart cities, Data encryption, Communication protocols, Regulatory measures

Introduction

The rapid development of the Internet of Things (IoT) is transforming urban environments into smart cities, enhancing efficiency, sustainability, and quality of life. However, this transformation also introduces significant security challenges. This article delves into the various security threats facing IoT systems in smart cities, including unauthorized access, data breaches, and the potential for malicious attacks. It explores a range of solutions designed to mitigate these risks, such as advanced encryption techniques, secure communication protocols, and robust policy frameworks. The importance of regulatory measures in ensuring the security and reliability of IoT infrastructures is underscored.

References

1. Stall, K., & Kruk, G. (2023). The impact of technological innovation on employee retention in enterprises: a case study of quality control. Zarządzanie Innowacyjne w Gospodarce i Biznesie, 37(2), 57-77.