



# IoT and Smart City Security: Future Security of Urban Life

*The concept of smart cities is changing the life of the city by using connected devices, yet with this innovation comes severe security threats. What can we do to secure billions of devices in a connected world*

By **Maryam Jabeen** | University of Agriculture, Faisalabad | Published: August 2026

✉ mahjabeen984888@gmail.com | Position: Software Engineer

## Introduction

Smart cities are being rapidly developed in modern cities with the help of the Internet of Things. IoT gadgets are enhancing efficiency and living standards, whether in the form of intelligent traffic lights or intelligent surveillance systems.

Yet, with this cybersecurity change comes new cybersecurity problems. With the increasing number of devices getting hooked to the web, there is a high risk of cyber attacks and hence security is one of the biggest concerns to governments and citizens.

***"It is as weak as its weakest connected gadget that a smart city can be made"***

## Technology Overview

Internet of Things (IoT) is a network of physical devices like cameras, sensors, smart appliances, and other devices that gather and exchange information. IoT is applied in traffic management, healthcare, energy systems, and in the public safety of smart cities.

To illustrate, traffic systems are smart and they ease congestion, whereas smart meters are used to regulate electricity consumption. Pakistan Cities such as Lahore and Islamabad are gradually embracing smart technologies to enhance urban management.

Nevertheless, most IoT devices are not well secured, and can be easily compromised by hackers. Poor passwords, software that is out of date, and the absence of encryption make them more vulnerable.



*Figure 1: Smart city IoT architecture showing interconnected devices such as traffic systems, surveillance cameras, and smart infrastructure protected by cybersecurity mechanisms.*

## Key Findings & Impact

One of the major security issues in smart cities is unauthorized access to IoT devices. In case security is poor, hackers may control the systems like traffic lights, surveillance cameras, or power grids.

Research demonstrates that poor security design of IoT devices has exposed a high proportion of such devices to cyber attacks. This may result in data breach, privacy invasion and even interference of city services.

In the case of the tech industry of Pakistan, the enhanced security of IoT can open new prospects to startups, cybersecurity specialists, and developers of software. It also can assist in the establishment of trust among users and aid digital development.

## What's Next?

Acceptable cybersecurity is needed to make smart cities safe. This contains encrypted data, frequent software updates, and safe authentication processes. Policies and standards on the security of IoT should also be developed by governments.

The future of smart cities is a reality, but with the absence of the security, it can be targeted as a victim of cyberattacks. We need to act and create a safe online space to all.

### About the Author

Author Maryam is a BS Information technology student in Pakistan who is passionate about cybersecurity and new technologies. She concentrates on issues related to IoT, data protection, and digital innovation. She can be reached at [mahjabeen984888@gmail.com](mailto:mahjabeen984888@gmail.com)

**Keywords:** Smart Cities; Internet of Things; Cybersecurity; Data Protection; Pakistan Tech.

## References

- [1] Ahmed, R. (2025) *IoT Security Challenges in Smart Cities*, *Journal of Cyber Technology*, 8(1), pp. 45–60. [2] International Telecommunication Union (2025) *Global Cybersecurity Outlook for Smart Cities*.