


# Chapter 1

# Introduction to Smart City Infrastructure Overview and Its Evolution From Web 2.0 to Web 3.0

**Usman Khalil**

 <https://orcid.org/0000-0001-8550-1557>

*Universiti Brunei Darussalam, Brunei*

**Mueen Uddin**

*University of Doha for Science and Technology, Qatar*

**Owais Ahmed Malik**

 <https://orcid.org/0000-0002-4888-5448>

*Universiti Brunei Darussalam, Brunei*

## **ABSTRACT**

*This chapter provides a comprehensive overview of the evolution of smart cities, tracing their roots from the Web2.0 era to the emerging Web3.0 ecosystem. It delves into the historical development of IoT-enabled smart devices and the enabling communication technologies that underpin their functionality. The chapter explores the layered architecture of smart cities, comprising application, transmission, and sensing layers, and identifies the associated security challenges at each level. A particular focus is placed on IoT-enabled smart device authentication, examining the state-of-the-art authentication models, including single-factor, two-factor, and multi-factor authentication. The chapter delves into the specifics of multi-factor*

DOI: 10.4018/979-8-3693-8876-1.ch001

*authentication, discussing biometrics, token-based, certificate-based, hardware security module, and trusted platform module approaches. By understanding these concepts, readers will gain insights into the intricate workings of smart cities and the critical role of security in ensuring their resilience and reliability.*

## **INTRODUCTION**

In the context of Web3, a decentralized smart city is an innovative urban concept that utilizes blockchain technology to enhance city operations and improve the quality of life for its residents. By leveraging decentralized technologies such as blockchain, smart contracts, and decentralized applications (dApps), a decentralized smart city can offer greater transparency, security, and efficiency in managing urban resources such as energy, water, and waste. An exponential number of smart devices connecting to the internet with every passing day results in a network of low-powered devices that communicate with each other. For the smart city, it is inevitable to refer to a ubiquitous computing system, as it develops a system where all the connecting devices can communicate with each other through the miner, making it possible to create a device-to-device (D2D) or a machine-to-machine (M2M) network (Cisco, 2020). One of the key benefits of a decentralized smart city in the context of Web3 is the ability to create a more decentralized and democratized system of governance. By utilizing decentralized voting systems, residents can have a greater say in how their city is run, ensuring a more equitable and democratic approach to urban development. Another important aspect of a decentralized smart city in the context of Web3 is the increased security and privacy of citizen data. By utilizing decentralized data storage and management systems, residents can have greater control over their data, ensuring that it is not exploited or misused by government or private entities. Here Internet-of-Things (IoT referred to as a network of low-powered smart devices that communicate with each other through mining machines or servers, etc.) has an important role in realizing the smart city concept as these devices play an important role in every domain. They make the edge of the network where real-time data collection is carried out in cyber and physical space. It can also be defined as a system in which things, people, processes, and data connect to the internet and each other (Cisco, 2020). It requires merging other technologies to make a ubiquitous computing system. Due to the ease of carrying out day-to-day activities, IoT-enabled smart devices have become an integral part of cyber-physical systems (CPS/s) in which they operate such as energy management, medical, retail, transport, manufacturing, etc. (Hussain et al., 2020). These CPSs may eventually be operating in a smart city realizing the concept of a smart plant. Furthermore, a decentralized smart city in the context of Web3 can enable greater innovation and

34 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/introduction-to-smart-city-infrastructure-overview-and-its-evolution-from-web-20-to-web-30/386798](http://www.igi-global.com/chapter/introduction-to-smart-city-infrastructure-overview-and-its-evolution-from-web-20-to-web-30/386798)

## Related Content

---

### Internet of Things (IoT) in Urban Development: Applications, Challenges, and Future Research Directions

B. Maheswari, S. Subha and T. Thilagam (2026). *Post-Quantum Cryptography and IoT Communications for Sustainable Urban Development* (pp. 281-308).

[www.irma-international.org/chapter/internet-of-things-iot-in-urban-development/391694](http://www.irma-international.org/chapter/internet-of-things-iot-in-urban-development/391694)

### Randomized Round Crypto Security Encryption Standard for Secure Cloud Storage

Anitha K., Anto Arockia Rosaline R., Devipriya A., Nancy P. and Vijaya K. (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 315-331).

[www.irma-international.org/chapter/randomized-round-crypto-security-encryption-standard-for-secure-cloud-storage/348616](http://www.irma-international.org/chapter/randomized-round-crypto-security-encryption-standard-for-secure-cloud-storage/348616)

### Homomorphic Encryption and Machine Learning in the Encrypted Domain

Neethu Krishna, Kommisetti Murthy Raju, V. Dankan Gowda, G. Arun and Sampathirao Suneetha (2024). *Innovative Machine Learning Applications for Cryptography* (pp. 173-190).

[www.irma-international.org/chapter/homomorphic-encryption-and-machine-learning-in-the-encrypted-domain/340979](http://www.irma-international.org/chapter/homomorphic-encryption-and-machine-learning-in-the-encrypted-domain/340979)

### Intrusion Detection System in Mobile Networks

P. Ramkumar, E. Saravanakumar, R. Uma, V. Mareeswari and Naveen H. S. (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 364-374).

[www.irma-international.org/chapter/intrusion-detection-system-in-mobile-networks/348619](http://www.irma-international.org/chapter/intrusion-detection-system-in-mobile-networks/348619)

### ICA and PCA-Based Cryptology

Sattar B. Sadkhan Al Maliky and Nidaa A. Abbas (2014). *Multidisciplinary Perspectives in Cryptology and Information Security* (pp. 200-217).

[www.irma-international.org/chapter/ica-and-pca-based-cryptology/108031](http://www.irma-international.org/chapter/ica-and-pca-based-cryptology/108031)