Chapter 8
NFT Security in Smart Cities:
An Exploration of Challenges, Countermeasures, and Emerging Trends

Kassim Kalinaki
https://orcid.org/0000-0001-8630-9110
Islamic University in Uganda, Uganda

Owais Ahmed Malik
https://orcid.org/0000-0002-4888-5448
Universiti Brunei Darussalam, Brunei

Gusti Ahmad Fanshuri Alfarisy
https://orcid.org/0000-0002-0689-7002
Institut Teknologi Kalimantan, Indonesia

Jalia Nassanga
Islamic University in Uganda, Uganda

ABSTRACT

The fusion of blockchain technologies and non-fungible tokens (NFTs) into smart city ecosystems presents new security challenges, impeding the widespread adoption of NFT in urban settings. Accordingly, this study comprehensively reviews the cybersecurity aspects surrounding NFTs within smart city environments. Firstly, a discussion of the various applications of NFTs in smart cities is provided. This is followed by an exploration of the unique cybersecurity vulnerabilities emanating from implementing NFTs in smart city ecosystems, including data privacy issues,

DOI: 10.4018/979-8-3693-8876-1.ch008

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

smart contract vulnerabilities, token theft, and the potential for market manipulation, etc. Moreover, various countermeasures and best practices to negate NFTs' cybersecurity concerns and vulnerabilities have been detailed. Finally, emerging trends in NFT security are equally also analyzed. This review study provide urban planners, policymakers, technologists, students, and researchers with a refined understanding of the cybersecurity concerns of NFT in smart cities.

INTRODUCTION

By definition, NFTs are unique digital assets representing ownership or proof of authenticity of a specific item or piece of content using blockchain technology (S. Yang et al., 2023). NFTs, whose structure is decocted in Figure 1, gained mainstream attention in 2021 with high-profile sales like Beeple's "Everydays: The First 5000 Days" artwork selling for $69 million[1] (Jenkins, 2024). While the initial hype has settled, NFTs continue to be used for digital ownership, community building, access passes, and various Web3 applications. However, integrating NFTs with smart city frameworks marks the point of intersection at which technological advancement meets smart city planning, presenting a lot of opportunities while also introducing complex security issues (Musamih et al., 2024; Razi et al., 2024). NFTs seem to present viable instruments for managing digital assets, property ownership, and public participation in the environment of a smart city within the context of Smart City initiatives globally adopting digital transformation. However, this integration presents many security concerns that need to be deeply analyzed and supported by innovative solutions (Ali et al., 2023). Smart cities, characterized by integrated systems and data-driven functions, are increasingly researching the applicability of NFTs in various domains, such as digital identity management, property tokenization, public services, and cultural heritage preservation (Kalinaki et al., 2023; Kuznetsov et al., 2024). These unique digital tokens, verified using blockchain technology, provide tamper-proof proof of ownership and authenticity and are thus highly sought after for application in governance and service provision in smart city settings (Kalinaki, 2024; Khalil et al., 2022; Shafik et al., 2024). Incorporating NFTs into smart city systems, nonetheless, brings with it a complicated security environment that intersects with critical infrastructure, safeguarding of personal information, and public safety concerns (Ali et al., 2023).

The security considerations that accompany the utilization of NFTs in smart cities extend outside the conventional cybersecurity frameworks. Although blockchain technology inherently delivers security advantages due to its decentralization and cryptography, the broader ecosystem facilitating NFTs, such as marketplaces, wallet frameworks, and smart contracts, is fraught with numerous potential weaknesses that

32 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/nft-security-in-smart-cities/386805

Related Content

Secure Text Extraction From Complex Degraded Images by Applying Steganography and Deep Learning
Binay Kumar Pandey, Deepak Mane, Vinay Kumar Kumar Nassa, Digvijay Pandey, Shawni Dutta, Randy Joy Magno Ventayen, Gaurav Agarwaland Rahul Rastogi (2021). *Multidisciplinary Approach to Modern Digital Steganography (pp. 146-163).*
www.irma-international.org/chapter/secure-text-extraction-from-complex-degraded-images-by-applying-steganography-and-deep-learning/280001

H0NEY4LOG: A Comprehensive Tool for SSH Honeypot and Log4j Vulnerability Scanner
Sujatha Gurunathan (2025). *Cryptography, Biometrics, and Anonymity in Cybersecurity Management (pp. 317-342).*
www.irma-international.org/chapter/h0ney4log/378756

Homomorphic Encryption Enabling Computation on Encrypted Data for Secure Cloud Computing
Ali Al Maqousi, Mohammad Alauthmanand Ammar Almomani (2024). *Innovations in Modern Cryptography (pp. 219-244).*
www.irma-international.org/chapter/homomorphic-encryption-enabling-computation-on-encrypted-data-for-secure-cloud-computing/354041

Security in Context of the Internet of Things: A Study
Mohammad Tariq Banday (2019). *Cryptographic Security Solutions for the Internet of Things (pp. 1-40).*
www.irma-international.org/chapter/security-in-context-of-the-internet-of-things/222268

An Integration of Keyless Encryption, Steganography, and Artificial Intelligence for the Secure Transmission of Stego Images
Digvijay Pandey, Vinay Kumar Nassa, Ayushi Jhamb, Dashrath Mahto, Binay Kumar Pandey, A. S. Hovan George, A. Shaji Georgeand Samir Kumar Bandyopadhyay (2021). *Multidisciplinary Approach to Modern Digital Steganography (pp. 211-234).*
www.irma-international.org/chapter/an-integration-of-keyless-encryption-steganography-and-artificial-intelligence-for-the-secure-transmission-of-stego-images/280004