


# Chapter 7


## Securing IoT Devices Using Generative AI Techniques

**Azeem Khan**

 <https://orcid.org/0000-0003-2742-8034>

*University Islam Sultan Sharif Ali,  
Brunei*

**Noor Jhanjhi**

 <https://orcid.org/0000-0001-8116-4733>

*TUSB, Malaysia*

**Ghassan Ahmed Ali Abdulhabeab**

*University Islam Sultan Sharif Ali,  
Brunei*

**Sayan Kumar Ray**

*TUSB, Malaysia*

**Mustansar Ali Ghazanfar**

*University of East London, UK*

**Mamoona Humayun**

*Independent Researcher, UK*

### ABSTRACT

*Generative artificial intelligence (GenAI) is a part of artificial intelligence which has the ability to generate content in various formats ranging from text to videos and images to audio formats. GenAI has the ability to inherently learn from large datasets and can produce results that can be of optimal use in case of cybersecurity. In the current digital landscape, we see a plethora of electronic gadgets connected to this seamless network of devices connected online. These seamless network of devices which were earlier unable to connect due to lack of ip addresses are now able to connect and are improving the quality of human life ranging from home appliances to health domain. From here we see emergence of smart networks which at one side is a boon but at the same time they have the risk of exploitation with unexpected cyberattacks. Hence, this chapter is an effort to highlight the issues concerning*

DOI: 10.4018/979-8-3693-5415-5.ch007

Copyright © 2025, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

*cyberthreats and advice on how GenAI can be utilized to mitigate these risks. This chapter focused on applying generative AI to secured IoT devices. By discussing the core concepts of IoT security, such as device authentication and access control, the chapter demonstrated how the next-generation generative AI models, including GANs and VAEs, can boost anomaly detection for device security. The chapter also provided examples of real-life use cases to illustrate how generative AI can be used to optimize the energy grid, protect data privacy, and strengthen cybersecurity efforts. Additionally, this chapter presented the key issues related to ethical considerations pertaining to privacy, bias, and accountability in the development and deployment of responsible AI. Moreover, it introduced the legal aspects of privacy legislation, data protection, and cybersecurity compliance. Finally, the chapter outlined some of the future trends in generative AI for IoT security to name a few are enhanced threat detection, privacy-preserving multimedia processing, and secure communications. The chapter then encourages organizations to start using generative AI to enable systems to become proactive about IoT security and reduce the massive onslaught of cyber threats while navigating an ever-evolving digital landscape.*

## **1. INTRODUCTION**

The Internet of Things has brought exponential growth and transformation to our daily lives. Smart homes, connected cities, and everywhere in-between these ever-present devices drive data and, with it, innovation, and convenience (Khan, Jhanjhi, Haji, & Omar, 2024; Mughal, Ullah, Cheema, Yu, & Jhanjhi, 2024). However, due to the widespread and accessible devices, a large critical problem has been created: how to secure and protect an ever-growing number of devices. Because today's security tools are traditional and slow to react, these devices are opportunities for attackers. This chapter is an effort to investigate on how generative AI can change the levers of IoT security and elucidates generative AI by examining how GenAI models can aid in the development of responsive security measures. This developing model, possibly including responsive threat recognition, mitigation and creating synthetic data to secure development, validation, and holds promise for the future of IoT security (Marjani, Jhanjhi, Hashem, & Hajibeigy, 2021).

IoT digital landscape though comprises numerous advantages for improving quality of life but at the same time there is an inherent concern that these devices (Sayan K Ray, Pawlikowski, & Sirisena, 2009) are not devoid of challenges. The sections below enlighten on those intricacies with which the whole IoT digital landscape can be protected and put on sustainable development path (Khan, Jhanjhi, Humayun, & Ahmad, 2020; Ponnusamy, Humayun, Jhanjhi, Yichiet, & Almufareh, 2022).

44 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/securing-iot-devices-using-generative-ai-techniques/356775](http://www.igi-global.com/chapter/securing-iot-devices-using-generative-ai-techniques/356775)

## Related Content

---

### Evaluation of Fault Tolerant Mobile Agents in Distributed Systems

Hojatollah Hamidiand Abbas Vafaei (2009). *International Journal of Intelligent Information Technologies* (pp. 43-60).

[www.irma-international.org/article/evaluation-fault-tolerant-mobile-agents/2446](http://www.irma-international.org/article/evaluation-fault-tolerant-mobile-agents/2446)

### Financial and Economic Analysis of Sustainable Practices for Green Computing

M. Nandhakumar, C. Kavitha, Rajimol K. P., R Ramya Sri, S. Anandakumarand S. Boopathi (2024). *Cases on AI Ethics in Business* (pp. 175-203).

[www.irma-international.org/chapter/financial-and-economic-analysis-of-sustainable-practices-for-green-computing/347534](http://www.irma-international.org/chapter/financial-and-economic-analysis-of-sustainable-practices-for-green-computing/347534)

### The Role of Artificial Intelligence in Transforming Supply Chain Management

P. Suganya, Subramanian R. Siva, S. N. Ananthi, T. Thilagam, J. Elavarasi, Gracious L. A. Antoand P. Girija (2026). *Transformative Impact of AI in Supply Chain Management* (pp. 271-294).

[www.irma-international.org/chapter/the-role-of-artificial-intelligence-in-transforming-supply-chain-management/387702](http://www.irma-international.org/chapter/the-role-of-artificial-intelligence-in-transforming-supply-chain-management/387702)

### An Agent-Based Approach for Sourcing Business Rules in Supply Chain Management

Sudha Ramand Jun Liu (2005). *International Journal of Intelligent Information Technologies* (pp. 1-16).

[www.irma-international.org/article/agent-based-approach-sourcing-business/2376](http://www.irma-international.org/article/agent-based-approach-sourcing-business/2376)

### Integrating Digital Humanities in Teaching Research Methodologies for Postgraduate Students in Arabic and Islamic Studies

Tawffeek Mohammed, Mohamed Faraj Saleh Raheeland Muhammad Ashraf Ebrahim Dockrat (2026). *Human-AI Collaboration and the Evolving Role of Educators* (pp. 271-302).

[www.irma-international.org/chapter/integrating-digital-humanities-in-teaching-research-methodologies-for-postgraduate-students-in-arabic-and-islamic-studies/405326](http://www.irma-international.org/chapter/integrating-digital-humanities-in-teaching-research-methodologies-for-postgraduate-students-in-arabic-and-islamic-studies/405326)