

Chapter 3

Case Studies and Applications of Generative AI in Real-World Cybersecurity Scenarios

Azeem Khan

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

University Islam Sultan Sharif Ali, Brunei

Noor Jhanjhi

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

Taylor's University, Malaysia

Ghassan Ahmed Ali

Universiti Islam Sultan Sharif Ali, Brunei

Sayan Kumar Ray

Taylor's University, Malaysia

Sobia Wassan

Vocational College, China

ABSTRACT

This chapter elucidates what the major effects of generative artificial intelligence are: It changes things a lot. It first discusses the overall of what generative AI can do using one kind of generative AI, then it considers what generative AI does to make

DOI: 10.4018/979-8-3693-8939-3.ch003

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

our defences against new things that can go wrong much more effective, and then it reflects on the major effects of generative AI on detecting malware and things that are subtly making our networks vulnerable. It emphasizes generative AI's ability to detect malware that was created to be hard to see with many examples of real things that attempt led to infection. Then it continues to discuss how generative AI interacts with threat intelligence feeds. It brings up that it is a way we can find out about cyber-attacks before they try to intrude. It goes on to relate to meaning how generative AI helps us with behavioural analysis and user authentication. It explains how we can protect privacy when learning about things that can go wrong using networks and threats. It focuses on collaborative learning and differential privacy. The next is to do with how well generative AI systems can handle 'attacks' – what professionals call adversarial attacks. It wonders if they are scalable for cybersecurity, and lastly it stretches discussion on ethical and legal concerns. In conclusion this chapter suggests Generative AI has potential benefits which can be tapped for better security and privacy of the seamless digital devices connected online apart from it the chapter suggests collaboration among all the stakeholders connected to this network for good using better defense mechanisms which Gen AI can provide against intrusions and anomalies that can infect our networks. At the end this chapter wind up the discussion concluding that this chapter is aimed at specialists working in cybersecurity, researchers, and policymakers.

1. INTRODUCTION TO CASE STUDIES

There is always a need to comprehend state of the art technologies comprehensively with an intent to grab insights to the crux of issues pertaining to specific concept, event, or a phenomenon, for the sake of updating and enhancing the knowledge pertaining to them. Hence, here comes case studies (Gill et al.) to address these sought of issues. In essence, case studies, aim to understand these sought of things of intricate details and come up with profound insights and solutions to existing or prevalent problems in academia or industrial arena (Julie, Nayahi, & Jhanjhi, 2021). They comprise and involve thorough investigations to get the crux of the matter. This chapter entitled case studies and applications of Generative AI in Real world cybersecurity scenarios is an effort to understand Generative AI and its application to optimize and improve the efficiency of cyber defense systems (A. Khan, Jhanjhi, & Sujatha, 2022).

38 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/case-studies-and-applications-of-generative-ai-in-real-world-cybersecurity-scenarios/357977

Related Content

Navigating Emerging Threats: Strategies for Cybersecurity in AI-Driven Healthcare Diagnostics and FDA Compliance

Sreekanth Yalavarthi and Rambabu Inaganti (2025). *AI-Driven Healthcare Cybersecurity and Privacy* (pp. 327-342).

www.irma-international.org/chapter/navigating-emerging-threats/376828

SEC-CMAC A New Message Authentication Code Based on the Symmetrical Evolutionist Ciphering Algorithm

Bouchra Echandouri, Fouzia Omary, Fatima Ezzahra Ziani and Anas Sadak (2018). *International Journal of Information Security and Privacy* (pp. 16-26).

www.irma-international.org/article/sec-cmac-a-new-message-authentication-code-based-on-the-symmetrical-evolutionist-ciphering-algorithm/208124

Exploring the Potential of Blockchain-Embedded Smart Grids in Quantum Era: Blockchain Embedded Smart Grids

Bannishikha Banerjee, Sreejita Sikdar, Pratyay Khastagir, Arshiya Dutta, Shumaila A. Rahim and Indraneel Mukhopadhyay (2025). *Convergence of Blockchain, Internet of Everything, and Federated Learning for Security* (pp. 345-376).

www.irma-international.org/chapter/exploring-the-potential-of-blockchain-embedded-smart-grids-in-quantum-era/380173

The Compliance of IT Control and Governance: A Case of Macao Gaming Industry

Colin Lai, Hung-Lian Tang, J. Michael Tarn and Sock Chung (2016). *International Journal of Information Security and Privacy* (pp. 28-44).

www.irma-international.org/article/the-compliance-of-it-control-and-governance/155103

A New Feature Selection Method Based on Dragonfly Algorithm for Android Malware Detection Using Machine Learning Techniques

Mohamed Guendouz and Abdelmalek Amine (2023). *International Journal of Information Security and Privacy* (pp. 1-18).

www.irma-international.org/article/a-new-feature-selection-method-based-on-dragonfly-algorithm-for-android-malware-detection-using-machine-learning-techniques/319018