



Chapter 3

Dynamic Defense Strategies With Generative AI


Khizar Hameed

 <https://orcid.org/0000-0003-1203-2010>
University of Tasmania, Australia


Muhammad Tayyab

 <https://orcid.org/0000-0001-5580-9163>
Taylor's University, Malaysia

Noor Zaman Jhanjhi

 <https://orcid.org/0000-0001-8116-4733>
Taylor's University, Malaysia

Syeda Mariam Muzammal

 <https://orcid.org/0000-0003-2960-1814>
Taylor's University, Malaysia

Majid Mumtaz

Independent Researcher, UK

ABSTRACT

This chapter examines the issues that traditional cyber defense tactics confront and investigates the limitations of static defense measures and the necessity for dynamic and adaptable alternatives. Furthermore, the chapter discusses the principles of GenAI for cyber defense and its approaches, as well as an overview of how GenAI allows synthetic data to be developed to train robust defense models and recognize emerging threats. A separate part discusses how GenAI can be applied to dynamic

DOI: 10.4018/979-8-3693-8944-7.ch003

threat detection and response in real-time cyber defense operations. This chapter emphasizes the importance of dynamic threat detection and response in real-time cyber defense operations and adaptive security policies based on GenAI. A full treatment of predictive analytics and forecasting, as well as threat intelligence fusion using GenAI techniques, is included in the book chapter. Finally, the chapter finishes with real-world examples and use cases demonstrating the efficacy of dynamic defense strategies utilizing GenAI, ethical and legal considerations, future directions, and new trends.

INTRODUCTION

Owing to the ongoing advancements in network-based systems, including cloud computing, the Internet of Things (IoT), and other nascent technologies, many Cyber-Physical Systems (CPS) have been implemented across domains, facilitating the simultaneous sharing and utilization of information resources. While promoting the efficient functioning of critical and influential sectors such as energy, transport, economics, and grid power, these resources have emerged as essential strategic infrastructures for all nations and organizations (Keshk et al., 2021; Mukherjee & De, 2021; Patwary et al., 2020). As a result, a new norm of social operations emerges, profoundly altered by these resources regarding human production and way of life. Alongside this advancement and their interconnected structured operations and processes, the digital world is expanding and permeating every part of our lives, and with it comes the undercurrent of cybersecurity concerns. Furthermore, as cyberspace gains access to more extensive data assets and amenities, security threats also assume novel forms. Diverse cyber security incidents transpire regularly, concomitant with the global proliferation of novel cyber threats (Tayyab & Marjani, 2021). Constantly occurring major security incidents and the array of attacks have demonstrated that cyber security confronts formidable obstacles over the years (He et al., 2021; Zafar et al., 2017).

The constant and ever-changing nature of cybersecurity threats is a formidable obstacle for organizations in today's interconnected digital world. A dual strategy is necessary to protect a company's assets in an age of ever-increasing need for more robust cybersecurity. First, there is an immediate necessity for companies to increase their cybersecurity resources, which must be acknowledged. Second, to put these system protections into place and keep an eye on them, organizations must actively seek out, hire, and collaborate with top-tier cybersecurity experts (Hameed et al., 2018; Lone et al., 2023). With the emergence of diversification attacks, conventional cyber defense technologies—including data security and device security, access management, authentication, data encryption, privacy protection, and intrusion

52 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/dynamic-defense-strategies-with-generative-ai/356579

Related Content

Convergence Between Criminology and Artificial Intelligence

Enrique Ismael Meléndez Ruíz, Mayra Elizabeth Brosig Rodríguez and Fernando Ortiz-Rodríguez (2026). *Reshaping Criminology with AI* (pp. 1-18).

www.irma-international.org/chapter/convergence-between-criminology-and-artificial-intelligence/384065

From Classroom to Clinic: The Impact of AI on Medical Education

Faisal A. Nawaz, Elisa Opriessnig, Firdous M. Usman, Jhalak Agrohi, Zara Arshad, Rahul Kashyap and Siddiq Anwar (2025). *Precision Health in the Digital Age: Harnessing AI for Personalized Care* (pp. 63-90).

www.irma-international.org/chapter/from-classroom-to-clinic/364453

Classifying Consumer Comparison Opinions to Uncover Product Strengths and Weaknesses

Kaiquan S. J. Xu, Wei Wang, Jimmy Ren, Jin S. Y. Xu, Long Liu and Stephen Liao (2011). *International Journal of Intelligent Information Technologies* (pp. 1-14).

www.irma-international.org/article/classifying-consumer-comparison-opinions-uncover/50482

Group Process Losses in Agile Software Development Decision Making

Sharon Coyle, Kieran Conboy and Thomas Acton (2013). *International Journal of Intelligent Information Technologies* (pp. 38-53).

www.irma-international.org/article/group-process-losses-agile-software/77873

Inside the Presidential Speechwriting Process: Using Content Analysis to Study Changes to Speech Drafts

Ken Collier (2016). *International Journal of Signs and Semiotic Systems* (pp. 35-57).

www.irma-international.org/article/inside-the-presidential-speechwriting-process/153599