Chapter 10
Case Studies and Real-World Application of Generative AI

Shikha Khullar
http://orcid.org/0009-0000-5598-3145
Poornima University, India

Chirra Baburao
http://orcid.org/0000-0003-4881-3708
Sir C.R. Reddy Educational Institutions, India

Nikhil Kumar Goyal
http://orcid.org/0009-0007-4532-8033
Noida International University, Greater Noida, India

Vaishali Sonwane
http://orcid.org/0000-0002-5823-4868
Poornima University, India

Shikha Sharma
http://orcid.org/0000-0001-6339-9731
Poornima University, India

Rakesh Kumar Saxena
http://orcid.org/0000-0002-6453-6053
Poornima University, India

ABSTRACT

The rapid adoption of digital technologies has intensified cyber threats, making effective risk management crucial for organizations. Traditional AI supports anomaly detection and intrusion prevention but struggles with novel attacks. Generative AI, leveraging GANs, VAEs, and LLMs, introduces a transformative edge by simulating realistic attack scenarios, generating synthetic datasets, and automating adaptive responses. This chapter examines real-world applications of Generative AI in cyber risk management, outlining its use in threat modeling, anomaly detection, incident response, and risk assessment. Case studies include phishing detection, ransomware simulation, and synthetic data generation across finance and healthcare sectors. A comparative analysis highlights key benefits and challenges, followed by discussions on ethical and adversarial risks and future directions such as integration with

DOI: 10.4018/979-8-3693-8397-1.ch010

Copyright © 2027, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

blockchain, explainable AI, and human–AI collaboration. This chapter provides researchers and practitioners a holistic view of how Generative AI is redefining cyber risk management.

1. INTRODUCTION

Digital revolution has presented global connection, collaboration and innovation opportunities never before seen before. Nevertheless, the cyber threat has also been on an increase proportional to this change. Since phishing attacks attack millions of users every day and advanced ransomware brings down healthcare organizations and financial institutions, the cyber risk industry is constantly developing in size and complexity. The old-fashioned security systems though effective against the familiar threats commonly collapse when faced with unfamiliar attackers, zero-day attacks, or highly dynamic attackers. Every company engaged in manufacturing, operations, or related services must adhere to the best practices in information technology flows and procurement management; therefore, the results across all companies will remain consistent and uniform at minimal levels. (Symantec, 2023) (IBM Security, 2023; ENISA, 2023) (Steinel, 2025)

This loophole has led to implementation of artificial intelligence (AI) on cybersecurity. The first AI systems were predominantly rule-based or prediction based and provided some form of incremental data improvement in detection and response. However, when the attackers started to utilize AI themselves the defense side had to have a strategy not merely predictive but also generative and adaptable. (Brundage et al., 2018; Chenna, 2022). This next frontier in AI is Generative Artificial Intelligence (Generative AI). Using generative AI in the form of architectures like Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and large language models (LLMs), generative AI does not merely analyze the existing data - it generates new and realistic data and scenarios. It enables defenders to both simulate cyberattacks and predict threats and enhance resilience in unknown directions (Goodfellow et al., 2014; Cai et al., 2021) (Kingma & Welling, 2013; Yan et al., 2025).

There are traditional AI classifiers available that could find known malicious email templates, but a generative AI one could present thousands of synthesized phishing emails, which could replicate evolving phishing tactics. This will allow the employees as well as the automated defense systems to be trained on future, unknown threats. In the same manner, simulating attack chains in ransomware preparedness so that organizations can be able to test their defenses against any actual incidents, this is what generative models can do.

22 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-real-world-application-of-generative-ai/413294

Related Content

Security Fortifying Critical Infrastructure: AI-Based Identity and Access Management (IAM) for Industrial Automation
Sandhya Samant, Pawan Kumar Goel, Himanshu Tyagiand Aafia Hussain (2025). *AI-Enhanced Cybersecurity for Industrial Automation (pp. 439-470).*
www.irma-international.org/chapter/security-fortifying-critical-infrastructure/379637

An Analysis of Device-Free and Device-Based WiFi-Localization Systems
Heba Alyand Moustafa Youssef (2014). *International Journal of Ambient Computing and Intelligence (pp. 1-19).*
www.irma-international.org/article/an-analysis-of-device-free-and-device-based-wifi-localization-systems/109625

Unstructured Road Detection Method Based on RGB Maximum Two-Dimensional Entropy and Fuzzy Entropy
Huayue Wu, Tao Xue, Xiangmo Zhaoand Kai Wu (2022). *International Journal of Ambient Computing and Intelligence (pp. 1-18).*
www.irma-international.org/article/unstructured-road-detection-method-based-on-rgb-maximum-two-dimensional-entropy-and-fuzzy-entropy/300801

Building Intelligent Recruitment Pipelines: Strategic Integration of AI and Big Data for Future-Ready Talent Acquisition
Ramadevi Vitthal Salunkhe (2026). *Strategies for AI and Big Data in Recruitment (pp. 97-138).*
www.irma-international.org/chapter/building-intelligent-recruitment-pipelines/388405

Teaching the Human-AI Balance: Enhancing Technical and Interpersonal Skills in Front Office Education Through AI-Powered Simulation
Zaid Roubyand Christopher Dutt (2026). *The Impact of Artificial Intelligence on Hospitality Education (pp. 331-350).*
www.irma-international.org/chapter/teaching-the-human-ai-balance/411859