Chapter 14
Future Trends and Challenges in Cybersecurity and Generative AI

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

Dayang H. T. B. A. Haji Hamid
University Islam Sultan Sharif Ali, Brunei

Haji Abdul Hafidz B. Haji Omar
University Islam Sultan Sharif Ali, Brunei

Fathi Amsaad
Wright State University, USA

Sobia Wassan
Jiangsu University, China

ABSTRACT

The chapter presents a comprehensive exploration of the changing dynamics at the intersection between the rapidly growing landscape of the interconnectivity of various devices—the internet of things—and the innovations piloted by advancements in generative artificial intelligence. In the following background-focused analysis, the significance of the enactment of new levels of security details in this fast-growing and virulently expansive landscape is emphasized, with generative AI ultimately serving as the highlight. The conversation consequently shifts to threats. This includes a detailed depiction of new cybersecurity threats rooted in advancements in

DOI: 10.4018/979-8-3693-5415-5.ch014

AI, featuring AI malicious actors and incidents, such as the increasingly popular phenomenon of ransomware-as-a-service as mirror illustrations of the dynamic and multifaceted character of these threats. The class further proceeds to more in-depth detail about the most contemporary generative AI platforms such as generative adversarial networks, variational autoencoders, and reinforcement learning—all relevant in identifying emerging solutions to advance strategies in cybersecurity. The conversation simultaneously conducts an opportunity and threat analysis of the merger between these platforms and cybersecurity with regard to ethics, regulations, and overall adversarial touchpoints and tactics. The chapter concludes with a call for unity in discourse and action between the relevant industry, academia, and government stakeholders as a summary of the essential cross-disciplinary aspect that must drive the narrative in confronting and overcoming the threats to and from generative AI research. Having presented the narrative structure, this chapter has allowed a comprehensive coverage of the major issues and opportunities at the heart of the cybersecurity-generative AI combination. Additionally, it has provided a forum to call for collaborative and fortified efforts regarding the securing and defending of the uncertainties that the rapidly changing and more unpredictable digital landscape has in store for the world.

1. INTRODUCTION

As depicted in Fig 1.0, with the advent of 21st century we see many technologies emerging, among those one of them which is the buzzword and hyped extensively is Artificial Intelligence acronymized as AI, this technology has brought numerous advantages, apart from challenges as well that are associated with it (I. A. Shah, N. Jhanjhi, & S. K. Ray, 2024). AI is classified into two broad categories namely Narrow AI or Weak AI and the second one is General AI. Weak or Narrow AI has specialised applications to name a few are classifying spam emails, chatbots, etc. (David & Eldon, 2022). Generative AI also falls under this category, as it is a subfield of AI that has the ability to create new content based on multi modal inputs which can be either text, image, audio or video by taking any of those inputs Gen AI with the help of machine learning algorithms such as supervised or unsupervised can create outputs of varied types which can be text, image, video, audio or 3D outputs as well (Al Naqbi, Bahroun, & Ahmed, 2024). Large datasets are required to train these models and they have enormous applications among those applications are the one associated with cybersecurity where GenAI has the ability to predict, analyse, suggest, and develop defensive mechanisms with which the entire digital landscape can be secured (N. Z. Jhanjhi & Shah, 2024).

Introduction to Quantum Computing and Its Integration Applications

Alex Khang, Vugar Abdullayev, Abuzarova Vusala Alyar, Matlab Khalilov, Nazila Ali Ragimovaand Yitong Niu (2024). *Applications and Principles of Quantum Computing (pp. 25-45).*

www.irma-international.org/chapter/introduction-to-quantum-computing-and-its-integration-applications/338281