Chapter 13
Future Trends and Trials in Cybersecurity and Generative AI

Venkat Narayana Rao T.
Sreenidhi Institute of Science and Technology, India

Harsh Vardhan G.
Sreenidhi Institute of Science and Technology, India

Krishna Sai A. N.
Sreenidhi Institute of Science and Technology, India

Bhavana Sangers
https://orcid.org/0009-0005-6134-1081
Sreenidhi Institute of Science and Technology, India

ABSTRACT

The relationship between the fields of generative (AI) and cybersecurity offers both opportunity and danger as technology continues to grow at an unimaginable rate. The emergence of 5G networks and the spread of internet of things (IoT)-connected devices are changing the challenging landscape in the field of cybersecurity. The predictions point to an increase in complex cyberattacks using AI-driven strategies like adversarial machine learning and deepfake methods. Simultaneously, content manipulation are being revolutionized by the rise of generative AI technologies such as deep learning and GANs (generative adversarial networks). The AI-generated synthetic media contributes to existing problems with digital trust and authenticity by posing moral questions about identity theft and disinformation. In conclusion, managing the intersection of cybersecurity and generative AI requires proactive

DOI: 10.4018/979-8-3693-5415-5.ch013

steps to fully utilize AI's potential while minimizing its inherent risks. This chapter includes solutions like anomaly detection systems and AI-powered threat intelligence.

1. INTRODUCTION

It is quite an important branch of the digital reality that has had great impact both during the operational process and during active defence in the last years is the combination of cybersecurity and generative AIs. We find one subcategory of AI applications called "generative AI" which is capable of creating original content (writing, visual, audio, or even computer code) using knowledge gathered from data that has already been collected. Cybersecurity as compared to information security, covers the protection of computer networks, operating systems and data from being misused, damaged or stolen by someone else.

1.1 Rapid Technological Advancements

Cybersecurity and generative AI technologies are developing at a rate never seen before, powered by a number of important factors(Gupta et.al,2023):

A. Machine Learning Breakthroughs

The abilities of the generative artificial intelligence models have been developed significantly by the achievement and advancement made in the field of machine learning, specifically in the area of deep learning. AI technologies capable of generating sophisticated and completely real data like image and speech recognition have become attainable through methodologies such as transformers, variational autoencoders (VAEs) and generative adversarial networks (GANs).

B. Data Quality and Availability

Data for generative AI models have been made in sufficient quantity because of the growth of digital data as well as its collection and storage methods. Because there is a plenty of data, AI systems can complete the process of learning the complex patterns even the nuances, which makes them productive in the correctness and sophistication of their outputs.