The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

Architecting A Secure Future: Cybersecurity in the Era of Generative AI

Vijayasarathi Balasubramanian (vijayasarathib@gmail.com)
: https://orcid.org/0009-0002-5002-1814 Georgia, USA

 Crossref/DOI: https://doi.org/10.55454/rcsas.3.09.2023.001

Abstract: *Generative AI is a sensational technology, but with cybersecurity challenges it actively needs attention. Data security and privacy is the top concern as over 120 zettabytes of data are available over the internet. Generative AIs can access all of this data due to the lack of comprehensive legislation policies to regulate it (Pooyandeh et al., 2022). People's private data and business data are both vulnerable to risk. In the current scenario, where we have incorporated AI technology into our daily lives seamlessly, our personal lives become an open book. Enhanced AI tools have access to our personal information. The remarkable evolution of AI with its cybersecurity implications needs immediate attention and research for a safe future. With the rise of Generative AI tools, an average computer user could potentially become a cyberattacker without much in-depth technical knowledge like in the previous era. Undoubtedly, Generative AI holds springs of a bright future, yet it also introduces challenges in cybersecurity.*

Keywords: AI in Cybersecurity, Cyberattacks, Cybersecurity, Future of Cybersecurity, Generative AI

Article History: **Received: 19 Sept- 2023;** **Accepted: 27 Sept- 2023;** **Published/Available Online: 30 Sept- 2023;**

1. Introduction

In today's digital era, we have witnessed a remarkable evolution of Artificial Intelligence to Generative AI. Generative AI has become a predominant area of the AI industry. With these innovations, human life is blessed with wide connectivity and convenience. On the other hand, it exposes new vulnerabilities. With Generative AI cyber-crimes have reached another level which shocks industries and nations. These days top companies reach out to heads of government to put robust regulations to control Generative AIs. Even some organizations have paused all usage of Generative AI technology in their companies till the time a certain level of cybersecurity is achieved with it.

Figure 1

Cybersecurity needs to be in balance, and should not over-regulate and not under-regulate. A lot of regulations are implemented by different countries using Cybersecurity Framework. For instance, NIST (National Institute of Standards and Technology) in the US has implemented an 'AI Risk Management Framework', 'Cyber Essentials' is the primary framework, established by the NCSC (National Cyber Security Centre) for the UK. In India, 'The NIST Cyber Security Framework, 'The Center for Internet Security Critical Security Controls (CIS)', and 'The International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002' frameworks are for public and private organizations. These organizations are working towards reaching a particular level of protection from Generative AI cyberattacks.

Generative AI

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

Generative AI is the hottest buzzword these days. It is a type of Artificial intelligence capable of generating highly realistic content in various domains, such as text, images, audio, and videos. Generative AI models are based on two neural networks, one is used as a generator and the other is used as a Discriminator. Generators learn the patterns and structure from input training data and then generate new data that has similar characteristics. It does not make predictions like traditional AI systems. Discriminator is used to discriminate between real and fake generated images. Both networks work simultaneously to achieve great results.

Some of the famous Generative AI tools are GPT-4, Jasper, ChatGPT, Alpha Code, Bard, Dall-E2, Synthesia, Speechify, StyleGAN and Chat.ai.

Cybersecurity

Cybersecurity is the strategic measure of protecting networks, electronic data, critical systems, and sensitive information from unauthorized access and digital attacks. Cybersecurity measures are designed to combat threats against a wide spectrum of interconnected networked systems, cloud networks, laptops, and mobile and software applications. Cybercriminals attack through various mediums, including malware software, emails, social media, pop-up ads, internet-of-things, online meeting platforms, and redirection to unintended websites. By employing an array of defense mechanisms, cybersecurity seeks to ensure the confidentiality, integrity, and security of critical information and services, thereby mitigating the potential risks posed by cyber intrusions and breaches.

Generative AI attracts the whole world's eye with its positive applications of generating art, faces, music, videos, virtual assistants, content synthesis, etc. But, it also gets significant attention from cyber attackers because of the ease of application without any in-depth technical knowledge. Generating fake emails, deep fake videos, audio, fake facial recognition, authentic-looking social media posts, and spreading misinformation adds a new set of challenges and risks of cybersecurity.

History of Generative AI

The evolution of Generative AI has been very interesting and can be marked by some important breakthroughs. Generative AI is based on LLM and the number of LLMs has continued increasing since 2018 with this accelerated timeline at the beginning of the year 2023 (Legous et al., 2023) as shown in Figure 2.

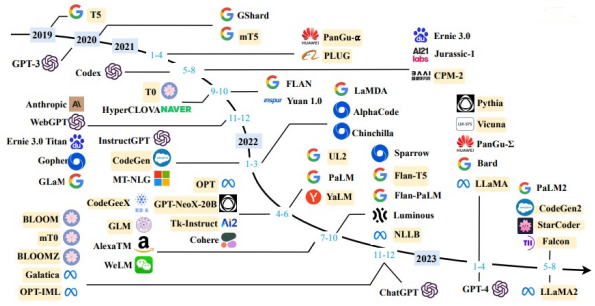

Figure 2: Evolution of Generative AI over the years. Source: (Zhao et al., 2023)

Some important milestones that have reshaped the landscape of Generative AI are:

- **WaveNet (2016):** DeepMind's WaveNet has made advanced marked audio generative models. WaveNet opens the door for AI assistants with its highly accurate text-to-speech synthesis.
- **Progressive GANs (2017):** NVIDIA Progressive GANs achieved the milestone in producing high-resolution realistic photo images.
- **GPT-2 and GPT-3 (2019, 2020):** OpenAI's generative pre-trained transformer (GPT) models marked a significant leap in the field of GenAI for textual data. They introduce the world with an AI-powered chatbot.

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

- **DALL-E (2022):** OpenAI DALL-E is a deep learning model that can generate digital images from natural language prompts.
- **ChatGPT (2022):** The most sensational evolution of GenAI is ChatGPT with record-breaking users. It is a conversational chatbot based on GPT, and the platform reached one million users within five days.
- **GPT-4 (2023):** The latest GPT model GPT-4 is more accurate and has advanced reasoning capabilities. It is an advanced version of ChatGPT.

Each of these milestones has played an important role in the evolution of Generative AI and in making it reach a remarkable level of computational power and intelligence.

2. Materials and Methods

This article employs a systematic review approach to synthesize existing literature on the benefits of Cybersecurity in the Era of Generative AI. A comprehensive search was conducted across reputable databases, including PubMed, IEEE Xplore, and Google Scholar, using keywords such as "Cybersecurity," "Generative AI," "Future of Cybersecurity," "AI in Cybersecurity," and "Cyberattacks". Peer-reviewed articles, conference proceedings, and reports published within the last five years were considered to provide an up-to-date perspective on the topic.

Architecting a Secure Future- Cybersecurity in the Era of Generative AI is a two-way process. To architect a secure cyber future either we look for solutions to provide cybersecurity from Generative AI or Generative AI can be used to provide Cybersecurity.

Methodology 1

The first methodology is to provide a solution for the cybersecurity issues created by Generative AI. Sometimes, 3rd party software is automatically downloaded and installed backend with some pop-up ads, email phishing (Zhang et al., 2023), or any other malware software. Some open-source libraries and add-on plugins increase the risk of data leakage. Malware Code Generation is also one of the major threats that can intrude into our systems. These smart Generative AI codes create biometric spoofing by password guessing, and creating fake images, videos, or voices. The fake facial recognition or voice authentication is used to fool the biometric security systems. Generative AI may be used to create convincing but false or misleading news and misinformation that can influence an organization's employees, spread propaganda and create untrusted situations among them.

For security assurance and software validation, it is important to run a rigorous code-scanning process in every system from time to time. This scanning process involves a thorough analysis of the software's source code to identify any potential vulnerabilities, especially within the open-source libraries, emails, plug-ins, and software it relies on. This proactive measure empowers organizations by identifying vulnerabilities, and suspicious malicious code segments at an early stage. It helps in rectifying issues, ensures data privacy and security, and minimizes the risks associated with cybersecurity vulnerabilities within the organization.

Methodology 2

The second methodology uses Generative AI itself for cyber security. Generative AI has many evolved applications that can be implemented for cyber security to safeguard the system from malicious intruders. It will reduce the manual work and enhance the threat detection process with speed-up responses to cyber-attacks. With Generative AI cyber experts and non-experts, others can provide real-time assessment and quantification. Generative AI tools are used by cyber attackers to intrude, similarly, cyber defenders can use Generative AI tools to enhance their threat intelligence capability by leveraging the information from huge data. Secured code generation and producing test cases to confirm the security of written code is one of its implementations. Defense mechanisms against cyberattacks can also speed up using GenAI.

Generative AI-powered cyber defense system includes Cyber Defense Automation, Threat Intelligence, Secure Code Generation and detection, identifying of cyber-attacks and self-healing capabilities, Real-time risk assessment and quantification, Developing ethical guidelines, and Incidence Response.

3. Results

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

In this section, we will elaborate on Cybersecurity issues from Generative AI and the Mitigation Plan for Cyber Security Issues Using Generative AI in detail.

Cybersecurity issues from Generative AI

Security issues from Generative AI in cyberspaces are-

1) Data Privacy: Generative AI may collect private data from their users like IP addresses, browsing data, and saved data on their system, and might use that as input for new data generation.

2) Malware and Phishing: Many cyber attackers use Generative AI to create new malware and phishing activities which might lead to financial losses and reputation damage.

3) Malware Code Generation: Generative AI can be used by cyber attackers to create malware code that might harm your software, attack your system, and leak information.

4) Biometric Spoofing: Generative AI is used for fake image generation and fake password guesses which lead to breaches in biometric security solutions.

5) Fake news and information: Generative AI can be used to create fake news and information which will e spread to achieve some negative propaganda, reach trust, and mislead people. Fake social media posts are creating havoc among users.

6) Generate Malicious Domains: Generating Malicious domains will lead users to some fake sites. Like bank sites or eCommerce sites, malicious domains might lead to financial losses and private data loss.

7) Fake Document Generation: Counterfeit government official documents can be created using GenAI which can harm the government bodies and can corrupt the nation's economic system.

8) Fake Voice and Video: Generative AI features to generate fake voices and videos can be used for illegal purposes which is a great threat to human mankind.

Generative AI Helps in Cybersecurity

Major areas where Generative AI can contribute to Cybersecurity are-

1) Cyber Defense Automation: Generative AI can reduce the load of security systems by automating the whole cyber defense mechanism. Defense automation reduces response time, and human efforts and improves security systems performance (Gupta et al., 2023).

2) Threat Intelligence: Generative AI models train with a huge amount of data, that improves intelligence to identify potential threats and generate actionable intelligence to protect organizations beforehand.

3) Malware Detection: Generative AI models trained with large data of malware samples and capable of creating synthetic malware variants. By training GenAI model, a more robust and advanced malware detection system can be made which can identify and predict any new malware in the system. (Dhoni et al., 2023)

4) Phishing Detection: A more trained and effective phishing detection system can be made using Generative AI by training it on generated phishing emails. Thus, phishing detection systems will be more effective in email filtering and identifying its threats.

5) Secure Code Generation and Detection: Generative Tools can easily detect security vulnerabilities in software code. Detecting security bugs in software plays a crucial part in the software development cycle. Generative AI makes it less labor-intensive, and more accurate security bug-free code.

6) Identifying cyber-attacks and self-healing capabilities: Generative AI can help enhance security and performance by automatically identifying and repairing cyber vulnerabilities, anomalies, and misconfigurations.

7) Real-time Risk Assessment and Quantification: Generative AI has the potential to assess the cyber threats on organizations in real-time, their likelihood and severity. It can easily help in prioritizing the threats so that preventive actions can be taken accordingly.

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

8) Developing Ethical Guidelines: Using NLP, Generative AI can develop ethical guidelines based on ethical principles written by various cybersecurity agencies. Guidelines and recommendations can be implemented in AI systems using GenAI.

Mitigation Plan for Cyber Security Issues

We have three plans to mitigate cyber security issues.

1) Auditing and Monitoring of Organizations: Regular auditing and monitoring of organizations are necessary to review systems to detect security and privacy issues. The security teams should run a rigorous code-scanning process in every system regularly to identify vulnerabilities, malware, phishing threats, any fake data or code generation, or any biometric spoofing. Security scanning should be included during the software development cycle to monitor the inputs and outputs of generative AI systems to detect anomalies and use threat intelligence to anticipate attacks.

2) Use Generative AI tools for Cyber security: By harnessing human talent and cutting-edge innovations and technology, Generative AI tools can be widely used for cybersecurity. Cyber defense mechanisms can be automated with intelligent systems. GenAI acts if any unauthorized person tries to intrude into the system using a fake password, fake voice, or face identification. Generative AI discriminators are designed to distinguish between real and fake data. This will detect and prevent fake code from entering our software, malware installation, or any phishing activity, assess the intensity of the attack, and implement self-healing capabilities. Intelligent systems can quick threat identification and quick response action.

3) Government Role: The government plays an important role in protecting the nation from cyber-attacks. AI is spread in diverse domains like public and private industries, healthcare, education, manufacturing, finance, retail, and many others. The government needs to form rigorous policies to prevent cyberattacks which should do justice to all. In the USA Cybersecurity & Infrastructure Security Agency (CISA) plays a vital role in protecting the nation against cyberattacks and malicious activities. North Atlantic Treaty Organization (NATO) making strategies to protect member countries from enhanced cyber crimes in the era of advanced Generative AI. Other countries' government is also actively working towards cyberattack security on the international level.

4. Conclusion

In conclusion, as we explore Generative AI in the era of cybersecurity, it seems to be a multi-faceted technology. Every individual, technology, organization, and government has a role to play in preventing cybercrime. It is unfair to judge a new technology until it is fully developed to its capabilities. It is an early stage of Generative AI implementation and it causes some cybersecurity issues. But, as we enhance and evolve with Generative AI tools, it seems to boom for Cybersecurity as well. Currently, it might seem like a hole in cybersecurity, but with more features, it will work as a more enhanced version of Cybersecurity systems.

In this article, we have discussed solutions to prevent cybercrime created by Generative AI and using Generative AI to provide cybersecurity. In the era of fast-growing technology, the future of Generative AI seems promising as well as challenging. If it grows with a holistic approach of mankind and an intrusive approach to cyber security along with government, it will strengthen our defenses against cybercrime and pave the way towards a safer, more secure digital future for all.

References

CAO, Y., LI, S., Liu, Y., Yan, Z., Dai, Y., YU, P.S. and Sun, L. (2023). A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from GAN to ChatGPT. Cornell University. https://arxiv.org/abs/2303.04226.

Dhoni, P. and Kumar, R. (2023). Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity. ResearchGate. https://www.researchgate.net/publication/373222263_Synergizing_Generative_AI_and_Cybersecurity_Roles_of_Generative_AI_Entities_Companies_Agencies_and_Government_in_Enhancing_Cybersecurity.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Science Direct. https://www.sciencedirect.com/science/article/pii/S1566253523001136.

ISSN: 2583-1380 Vol. 3 | Issue No. 9 | September 2023 Impact Factor: 4.736 (SJIF)

Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. Cornell University. https://arxiv.org/abs/2307.00691.

Legous, G. (2023, April 17). History of the Generative AI. Medium. https://medium.com/@glegoux/history-of-the-generative-ai-aa1aa7c63f3c.

Pooyandeh, M., HanORCID, K. and Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. MDPI - Publisher of Open Access Journals. https://www.mdpi.com/2076-3417/12/24/12993.

Shen, C. (2023, May 30). Generative AI: A Blessing or a Curse for Cybersecurity?. inweb3. https://www.inweb3.com/generative-ai-a-blessing-or-a-curse-for-cybersecurity/.

Zhang, C. Y. (2023, July 1). Cybersecurity and Generative AI. Linkedin. https://www.linkedin.com/pulse/cybersecurity-generative-ai-dr-christina-yan-zhang/?trk=pulse-article_more-articles_related-content-card.

Zhang, Z., Hamadi, H.A., Damiani, E., Yeun, C.Y. and Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Explore. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9875264.

Zhao, W. X., Zhou, K., Li, J., Tang, Y., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z., Du, Y., Yang, C., Chen, Y., Chen, Z., Jiang, J., Ren, R., Li, Y., Tang, X., Liu, Z., Liu, P., Nie, J. and Wen, J. (2023). A Survey of Large Language Models. Cornell University. https://arxiv.org/abs/2303.18223.

Conflicts of Interest: The author declares no conflict of interest.