Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0015

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

The Rise Of Artificial intelligence In Cyber Security

Dr. Jayashri P. Barai
Asst. Professor
Purushottam Thote college of Social work Nagpur.
giradkarjayashri@gmail.com

Abstract

Cyber security has become a major concern in the digital era. Data breaches, ID theft, cracking the catch, and other such stories abound, affecting millions of individuals as well as organizations. The challenges have always been endless in inventing right controls and procedures and implementing them with acute perfection for tackling with cyber attacks and crimes. The ever-increasing risk of cyber attacks and crimes grew exponentially with recent advancements in artificial intelligence. It has been applied in almost every field of sciences and engineering. From healthcare to robotics, AI has created a revolution. This ball of fire couldn't be kept away from cyber criminals, and thus, the "usual" cyber attacks have now become "intelligent" cyber attacks. In this chapter, the authors discuss specific techniques in artificial intelligence that are promising. They cover the applications of those techniques in cyber security. They end the discussion talking about the future scope of artificial intelligence and cyber security.

Keywords : Cyber Security ,artificial intelligence, attacks, revolution Control Distribution, Human Senses Mimicry, Vulnerability Management

Introduction

As we navigate the digital era of the 21st century, cyber security has grown into a pressing societal issue that requires innovative, cutting-edge solutions. In response to this pressing need, Artificial Intelligence (AI) has emerged as a revolutionary instrument, causing a paradigm shift in cyber security. AI's prowess resides in its capacity to process and analyze immense quantities of heterogeneous cyber security data, thereby facilitating the efficient completion of crucial tasks. These duties, which include threat detection, asset prioritization, and vulnerability management, are performed with a level of speed and accuracy that far exceeds human capabilities, thereby transforming our approach to cyber security. These documents provide a comprehensive dissection of AI's profound impact on cyber security, as well as an in-depth analysis of how AI tools not only augment, but in many cases transcend human-mediated processes. By delving into the complexities of AI implementation within the realm of cyber security, we demonstrate the potential for AI to effectively anticipate, identify, and preempt cyber threats, empowering organizations to take a proactive stance towards digital safety. Despite these advancements, it is essential to consider the inherent limitations of AI. We emphasize the need for sustained human oversight and intervention to ensure that cyber security measures are proportionate and effective. Importantly, we address potential ethical concerns and emphasize the significance of robust governance structures for the responsible and transparent use of artificial intelligence in cyber security. This paper clarifies the transformative role of AI in reshaping cyber security strategies, thereby contributing to a safer, more secure digital future. In doing so, it sets the groundwork for

further exploration and discussion on the use of AI in cyber security, a discussion that is becoming increasingly important as we continue to move deeper into the digital age.

Meaning of Artificial intelligence in Cyber security

AI in cyber security integrates artificial intelligence technologies, such as machine learning and neural networks, into security frameworks. These technologies enable cyber security systems to analyze vast amounts of data, recognize patterns, and adapt to new and evolving threats with minimal human intervention. Unlike traditional cyber security tools, which rely on predefined rules to detect threats, AI-driven systems learn from experience, allowing them to predict, detect, and respond more effectively to known and unknown threats. By doing so, AI empowers organizations to enhance their cyber security posture and reduce the likelihood of breaches. AI in cyber security involves technologies that can understand, learn, and act based on data. AI is evolving in three main stages:

1. **Assisted intelligence:** Enhances what people and organizations already do today.
2. **Augmented intelligence:** Enables new capabilities, allowing people to perform tasks they couldn't do before
3. **Autonomous intelligence:** Future technology where machines will act independently, like self-driving cars.

Important of Artificial intelligence in Cyber security

The importance of AI in cyber security cannot be overstated. As cybercriminals adopt more sophisticated methods, conventional security systems need help to keep pace. The sheer volume of data generated by modern networks further complicates the detection of threats, leaving many organizations vulnerable to attacks. AI offers a solution to these challenges by:

Enhancing the speed and accuracy of threat detection: AI can quickly sift through massive amounts of data to detect anomalies and identify potential risks, reducing the time it takes to respond to threats.

Automating routine tasks: AI frees security teams to focus on more strategic efforts by automating time-consuming processes such as log analysis and vulnerability scanning.

Predicting future attacks: AI can identify patterns in past attacks and anticipate new threats, helping organizations stay one step ahead of cyber criminals.

Benefits of AI in Cyber security

1. Improved Threat Intelligence

AI enhances threat intelligence by analyzing large datasets in real time and providing predictive insights. This capability allows cyber security teams to anticipate attacks before they occur and take proactive measures to defend against them.

2. Faster Incident Response Times

Speed is crucial during a cyber attack, and AI enhances incident response by automating threat detection, analysis, and mitigation. Thus, the time from detection to action is reduced, and potential breach impacts are minimized. AI-powered systems provide improved context for prioritizing security alerts, enable rapid incident response, and identify root causes to mitigate vulnerabilities and prevent future issues.

3. Better Vulnerability Management

AI's ability to identify vulnerabilities in networks and systems is another significant advantage. AI-powered vulnerability scanners can prioritize risks based on reach ability, exploitability, and business criticality, helping organizations address the most pressing issues first. This reduces false positives and ensures that security teams are working efficiently.

4. More Accurate Breach Risk Predictions

Accounting for IT asset inventory, threat exposure, and security controls effectiveness, AI-based systems can predict how and where you are most likely to be breached so that you can plan for resource and tool allocation toward areas of weakness. Prescriptive insights derived from AI analysis can help you configure and enhance controls and processes to improve your organization's cyber resilience most effectively.

5. Automated Recommendations

Another key to harnessing AI to augment human infuse teams is the explain ability of recommendations and analysis. This is important in getting buy-in from stakeholders across the organization, understanding the impact of various infuse programs, and reporting relevant information to all stakeholders, including end users, security operations, CISO, auditors, CIO, CEO and board of directors.

Conclusion

As AI technology advances, its role in cyber security will continue to expand. Innovations such as Quantum AI and more advanced language models hold the potential to enhance threat detection and response capabilities further. However, cybercriminals are also adapting as AI becomes more prevalent in cyber security. We can expect AI to be used in more sophisticated cyber attacks, requiring organizations to stay vigilant and continuously update their defenses. The role of AI in cyber security has become essential in bolstering human efforts in information security. As the enterprise attack surface expands, AI aids in identifying and analyzing threats, reducing breach risk, and enhancing security posture. It excels in risk prioritization, malware detection, incident response guidance, and intrusion detection. AI drives cyber security beyond individual capabilities by forming powerful partnerships between humans and machines.

Reference

Abuali, K., L. Nissirat, and A. Al-Samawi. 2023. Advancing network security with AI: SVM-Based deep learning for intrusion detection. Sensors (Switzerland) 23 (21):8959. doi: 10.3390/s23218959.

Aflalo, A., S. Bagon, T. Kashti, and Y. Eldar. 2023. Deepcut: Unsupervised segmentation using graph neural networks clustering. In Proceedings of the IEEssE/CVF International Conference on Computer Vision, Paris, France, 32–46. IEEE. doi:

Albhirat, M., A. Rashid, R. Rasheed, S. Rasool, S. Zulkiffli, and H. Muhammad Zia-Ul-Haq. 2024. The PRISMA statement in enviropreneurship study: A systematic literature and a research agenda. Cleaner Engineering and Technology 18 (February):100721. Elsevier. doi: 10.1016/j.clet.2024.100721.

Alharbi, Y., A. Alferaidi, K. Yadav, G. Dhiman, S. Kautish, and J. Xia. 2021. Denial-of-service attack detection over IPv6 network based on KNN algorithm. Wireless Communications and Mobile Computing 2021 (1):1–6. doi: 10.1155/2021/8000869.

Anupam, S., and A. Kumar Kar. 2021. Phishing website detection using support vector machines and nature-inspired optimization algorithms. Telecommunication Systems 76 (1):17–32. doi: 10.1007/s11235-020-00739-w.