From Safeguard to Threat: The Dichotomy of AI's Influence on Privacy and Cybercrime

Mr. Nitin Soni, Research Scholar, Department of Computer Applications, Government Engineering College, Bikaner, Rajasthan, India, nsoni6789@gmail.com
Dr. Rakesh Poonia, Assistant professor, Department of Computer Applications, Government Engineering College, Bikaner, Rajasthan, India, rakesh.ecb98@gmail.com

Abstract

According to data as of October 2023, Artificial Intelligence (AI) is a powerful disruptive force in cybersecurity and privacy, providing both extraordinary opportunities and serious challenges. This paper examines this duality of AI as a protector and a potential threat; an agent of strong protection and at the same time a new danger for privacy and cybersecurity. AI & Cyber Security AI plays a vital role in both defense and offensive in terms of cyber security.AI in Cyber Security enables Security Infrastructure to Defense Against Cyber Attacks - Cyber security AI enhances Security infrastructure in terms of Threat Detection Systems, Anomaly Detection, Predictive Analytics, and Automated Incident Response mechanisms, a combination that gives a stronghold to the defense against cyber threats. On the other hand, cybercriminals are leveraging the power of AI to conduct more complex cyber-attacks, such as AI-enhanced attacks, automated hacking, identity theft using deepfakes, and mass privacy violations.

By stripping down and analyzing existing AI, we unravel how the very technology which helps reinforce and strengthen security infrastructures, can be subverted and bent to subvert them, creating a paradoxical situation. The paper further references case studies to show where AI has operated as a guardian or a threat, summarizing a balanced perspective of its impact. In addition, the research tackles regulatory and ethical issues, calling for broad strategies to regulate the use of use AI in cybersecurity.

By the end of the paper, the author recommends a multi-pronged approach to the challenges posed by AI, including strong oversight, ethical development of AI, and international cooperation. It highlights the critical need to strike a balance between harnessing the potential of AI to improve privacy and security, while ensuring protections against its potential misuse in the always-evolving cyber threat environment.