IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 5, March 2025

# Artificial Intelligence in Cyber Security: Review on Challenges and Opportunities

**Gauri Bare[1], Prerana Bhadane[2], Sakshi Charaskar[3], Kalyani Adhav[4], Kunal Avhad[5], Gayatri Rakesh Jagtap[6]**
Computer Engineering Department
Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India

**Abstract:** *Artificial intelligence (AI) presents significant opportunities to enhance cybersecurity by automating threat detection, rapidly responding to incidents, and identifying emerging attack patterns, but its implementation also comes with challenges like data quality issues, model interpretability, and the potential for adversarial attacks, requiring careful consideration of both benefits and risks to effectively leverage AI for robust cyber defense strategies. AI can analyze vast amounts of data to detect anomalies, predict potential threats, and proactively respond to attacks faster than traditional methods, significantly improving security posture. The increasing frequency and sophistication of cyber threats have prompted the need for advanced security solutions, with Artificial Intelligence (AI) emerging as a critical tool in the fight against cybercrime. AI, encompassing machine learning (ML), deep learning (DL), and natural language processing (NLP), enables cybersecurity systems to detect, prevent, and respond to threats more efficiently and proactively. This paper explores the applications of AI in cybersecurity, including threat detection, malware analysis, intrusion prevention, and incident response automation. It discusses how AI-driven systems improve real-time threat identification and reduce human error, enhancing the overall effectiveness of security measures. However, challenges such as data privacy concerns, adversarial attacks on AI models, and the shortage of skilled professionals must be addressed to maximize AI's potential in cybersecurity. The paper also highlights future directions, including AI's integration with Zero Trust Architecture, autonomous security systems, and the role of Explainable AI (XAI) for transparency. As AI technology evolves, its potential to reshape cybersecurity strategies and defend against increasingly complex threats continues to grow.*

**Keywords:** Artificial intelligence (AI), Cyber security, attacks


DOI: 10.48175/IJARSCT-24136