Volume 10, Issue 7, July – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul703

AI and Machine Learning in Cyber Security

Shaikh Mohammad Anas[1]; Kumbhoje M. R.[2]

[2]Assit Prof.

[1,2] Shri Shiv Chhatrapati College Junnar
Department of Commerce and Research Center
BBA & BBA(CA)

Publication Date: 2025/07/17

Abstract: Cybersecurity threats are evolving rapidly, requiring advanced and automated defense mechanisms. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for detecting, preventing, and mitigating cyber threats. This paper explores the role of AI and ML in cybersecurity, highlighting their applications in threat detection, anomaly identification, and predictive analytics. Additionally, the paper discusses the challenges and future directions of AI-driven cybersecurity solutions.

How to Cite: Shaikh Mohammad Anas; Kumbhoje M. R. (2025) AI and Machine Learning in Cyber Security. *International Journal of Innovative Science and Research Technology,* 10(7), 1010-1011.
https://doi.org/10.38124/ijisrt/25jul703

I. INTRODUCTION

The increasing reliance on digital infrastructure has led to a surge in cyber threats such as malware, phishing, ransomware, and data breaches. Traditional security measures are often insufficient in handling sophisticated attacks. AI and ML offer proactive solutions by enabling automated threat analysis and adaptive security mechanisms.

II. APPLICATIONS OF AI AND ML IN CYBERSECURITY

- *Threat Detection and Prevention*

AI-powered systems analyze vast amounts of data to identify patterns associated with cyber threats. ML algorithms detect anomalies that indicate potential security breaches. Techniques such as supervised and unsupervised learning help classify threats and predict malicious activities.

- *Phishing and Spam Detection*

Natural Language Processing (NLP) and ML algorithms are used to detect phishing emails and fraudulent websites by analyzing text patterns, domain authenticity, and user behavior.

- *Behavioral Analytics and Anomaly Detection*

AI monitors user behavior to detect deviations that could indicate an attack. For example, an unusual login attempt from a different location or device may trigger a security alert.

- *Malware Analysis and Threat Intelligence*

Deep learning models are trained to recognize malware signatures and predict new malware variants. AI enhances threat intelligence by analyzing global threat data and generating real-time security updates.

- *Automated Security Operations*

Security Information and Event Management (SIEM) systems use AI to automate incident response and reduce false positives, allowing security teams to focus on critical threats.

III. CHALLENGES IN AI-BASED CYBERSECURITY

- *Adversarial Attacks on AI Models*

Cybercriminals exploit vulnerabilities in AI models by manipulating input data, making threat detection systems less effective.

- *Data Privacy and Ethical Concerns*

The use of AI in cybersecurity requires large datasets, raising concerns about data privacy and compliance with regulations like GDPR.

- *False Positives and Model Bias*

AI models sometimes generate false positives or exhibit biases due to imbalanced training data, leading to inefficiencies in cybersecurity operations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul703

IV. FUTURE DIRECTIONS

Future research should focus on developing robust AI models resistant to adversarial attacks, enhancing interpretability in AI-driven security systems, and integrating AI with blockchain for secure authentication.

V. CONCLUSION

AI and ML have revolutionized cybersecurity by enabling intelligent threat detection and automated defense mechanisms. Despite challenges, continuous advancements in AI will play a crucial role in safeguarding digital systems from evolving cyber threats.

REFERENCES

[1]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305-316.
[2]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176.