Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

AI and Machine Learning in Security

Anjay Suryawanshi
Department of Computer Science
Dr. D. Y. Patil Arts, Commerce & Science College, Pimpri, Pune, Maharashtra, India

Shiva Arsul
Department of Computer Science
Dr. D. Y. Patil Arts, Commerce & Science College, Pimpri, Pune, Maharashtra, India

Abstract - The increasing dependence on digital systems and internet-based services has led to a rapid rise in cyber threats, posing serious challenges to information security. Conventional cybersecurity methods, which rely on predefined rules and signatures, are often ineffective against modern and evolving attacks such as malware, ransomware, phishing, and zero-day threats. To overcome these limitations, this paper examines the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing cybersecurity frameworks.

AI and ML techniques enable intelligent analysis of large volumes of security data to
detect anomalies, malicious patterns, and potential intrusions in real time. By learning from historical data and adapting to new attack behaviors, these systems improve threat detection accuracy and reduce false positives. detect anomalies, malicious patterns, and potential intrusions in real time. By learning from historical data and adapting to new attack behaviors, detect anomalies, malicious patterns, and potential intrusions in real time. By learning from historical data and adapting to new attack behaviors, these systems improve

threat detection accuracy and reduce false positives. The paper discusses the application of AI and ML in key cybersecurity areas, including network security, intrusion detection, endpoint

protection, and vulnerability management. It also highlights the integration of AI-driven security solutions with emerging technologies such as the Internet of Things (IoT), blockchain, and edge computing to strengthen cyber defense mechanisms.

The study concludes that AI- and ML-based approaches provide a proactive, adaptive, and effective solution for securing digital infrastructures against complex cyber threats.

Keywords-Artificial Intelligence, Machine Learning, Cybersecurity, Threat Detection, Intrusion Detection Systems, Malware Analysis, Network Security,
Anomaly Detection, Intelligent Security Systems, Cyber Threats

I. INTRODUCTION

The rapid growth of digital technologies, cloud computing, and internet-based services has led to a significant increase in cyber threats such as malware, ransomware, phishing, and data breaches. Traditional cybersecurity approaches, which rely heavily on rule-based and signature-based techniques, are increasingly ineffective against modern and evolving attacks.

Artificial Intelligence (AI) and Machine Learning (ML) offer intelligent and adaptive solutions by analyzing large volumes of security data, detecting anomalies, and identifying threats in real time. These technologies are widely applied in areas such as intrusion detection, malware analysis, network security, and endpoint protection. The integration of AI and ML strengthens cybersecurity frameworks by improving detection accuracy, response speed, and protection against emerging cyber threats.

II. LITERATURE REVIEW

Previous studies show that traditional cybersecurity methods are no longer effective against modern cyber attacks. Researchers have widely applied Artificial Intelligence (AI) and Machine Learning (ML) to improve threat detection by analyzing large volumes of security data and identifying abnormal behavior. Studies highlight the effectiveness of AI and ML in intrusion detection, malware detection, anomaly detection, and network security, with improved accuracy and reduced false positives. Research also shows that these techniques are useful in detecting zero-day attacks and insider threats. However, challenges such as adversarial attacks, data bias, and lack of transparency remain. Recent literature emphasizes the use of explainable AI and the integration of AI with technologies like IoT, blockchain, and cloud computing to enhance cybersecurity resilience. Overall, existing research supports AI- and ML-based solutions as essential for modern cybersecurity systems. However, most existing studies focus on specific security domains, highlighting the need for a comprehensive overview of AI and ML applications in cybersecurity, which this study aims to address.

III. RESEARCH METHODOLOGY

This study follows a descriptive and analytical research methodology to examine the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing cybersecurity systems. The research is conceptual and review-based, focusing on existing studies, security frameworks, and real-world applications rather than experimental implementation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

TABLE I
AI and Machine Learning Techniques Used in Cybersecurity

AI / ML Technique	Application Area
Supervised Learning	Malware Detection
Unsupervised Learning	Anomaly Detection
Deep Learning	Intrusion Detection Systems
Reinforcement Learning	Automated Incident Response

The first phase involves a comprehensive literature review of academic journals, conference papers, and industry reports to identify current trends, techniques, and challenges in AI-driven cybersecurity. In the second phase, key AI and ML techniques—such as supervised learning, unsupervised learning, deep learning, and reinforcement learning—are analyzed with respect to their applications in malware detection, anomaly detection, intrusion detection systems, endpoint security, and automated incident response, as summarized in **Table I**

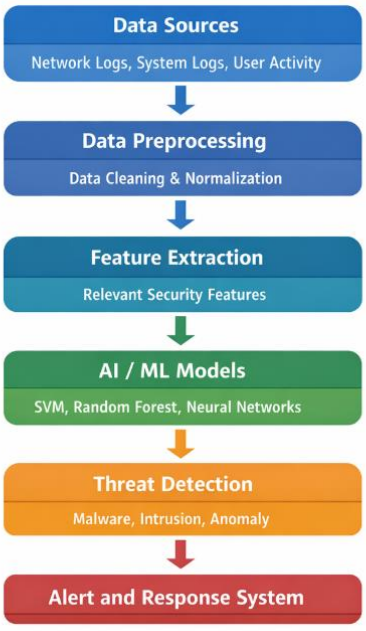

Fig. 1. Architecture of AI and Machine Learning Based Cybersecurity System

The third phase evaluates AI-based security frameworks and architectures, examining how data collection, preprocessing, model training, deployment, and real-time monitoring are integrated within intelligent security systems, as illustrated in **Fig. 1**. The final phase analyzes the advantages, challenges, and ethical issues associated with AI and ML in cybersecurity, including adversarial attacks, data bias, privacy concerns, scalability, and model interpretability. Overall, this methodology provides a structured understanding of the impact and future potential of AI- and ML-based cybersecurity solutions.

IV. RESULTS AND DISCUSSION

The findings demonstrate that Artificial Intelligence (AI) and Machine Learning (ML) significantly enhance cybersecurity performance compared to traditional rule-based systems. AI-driven security solutions improve threat detection accuracy, particularly for zero-day attacks, malware, and insider threats, while reducing false positives through intelligent behavior analysis. Automated monitoring and real-time response capabilities also reduce detection and response time, enabling faster incident mitigation.

TABLE II

Comparison between Traditional and AI-Based Cybersecurity Systems

Feature	Traditional Security Systems	AI & ML-Based Security Systems
Detection Approach	Rule and signature-based	Data-driven and learning-based
Zero-day Attack Detection	Low	High
False Positives	High	Reduced
Adaptability	Static	Dynamic and adaptive
Automation Level	Limited	High

As shown in **Table II**, AI- and ML-based systems offer greater adaptability, scalability, and automation than traditional security approaches. Despite these advantages, challenges such as adversarial attacks, data bias, explainability, and privacy concerns remain. Overall, the results confirm that AI and ML provide an effective and proactive approach to modern cybersecurity when combined with conventional security measures and human oversight. These findings align with recent studies that demonstrate the effectiveness of learning-based security models in real-world cyber defense scenarios.

V. CONCLUSION

This study concludes that Artificial Intelligence (AI) and Machine Learning (ML) play a vital role in strengthening modern cybersecurity systems. AI-driven security solutions improve threat detection accuracy, reduce response time, and enhance protection against evolving and unknown cyber threats. Although challenges such as adversarial attacks, data bias, and ethical concerns remain, responsible implementation of explainable AI and human oversight can address these issues. Overall, AI and ML represent essential and effective components of future cybersecurity strategies.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

VI. REFERENCES

[1] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[2] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[4] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proc. IEEE Symp. Security and Privacy*, 2017, pp. 39–57.

[5] A. Rajabi, S. M. Ghaffarian, and R. Jalili, "Malware detection using machine learning algorithms," *Computers & Security*, vol. 87, Article ID 101568, 2019.

[6] Y. Zhang, X. Wang, and X. Li, "Deep learning-based intrusion detection system for network security," *Future Generation Computer Systems*, vol. 117, pp. 45–56, 2021.