iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75092

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

A Comprehensive Review of Artificial Intelligence in Cybersecurity and Barriers to Its Adoption

Siddhesh Rajendra Salunkhe[1], Kevin Harry Agashe[2], Prof. Mukul Jagtap[3], Prof. Nagnath Dolare[4]
Department of Artificial Intelligence and Data Science, Keystone School of Engineering, Pune, Maharashtra, India

Abstract: ***Artificial Intelligence (AI) has emerged as a transformative force in modern cybersecurity, enhancing threat detection, predictive defense mechanisms, and adaptive response strategies. This review paper explores the integration of AI in cybersecurity systems, its key applications, and the barriers inhibiting large-scale adoption. By analyzing recent studies and industry practices, this work identifies both the technological potential and organizational challenges that influence AI-driven cybersecurity implementations. The paper concludes with recommendations for overcoming these barriers and future research directions to ensure secure and ethical AI deployment.***

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Threat Detection, AI Adoption, Barriers

I. INTRODUCTION

In recent years, Artificial Intelligence (AI) has revolutionized digital ecosystems by automating processes, enhancing data-driven decision-making, and improving threat management systems. Cybersecurity, a field focused on protecting systems and data from unauthorized access and attacks, has significantly benefited from AI innovations. AI models can detect anomalies, identify attack patterns, and respond to potential threats faster than traditional systems. However, despite these advancements, organizations often face difficulties adopting AI solutions due to cost, technical complexity, data privacy concerns, and lack of skilled professionals.

II. LITERATURE REVIEW

Numerous studies have investigated the growing role of AI in cybersecurity. Research by Singh et al. (2022) emphasizes how machine learning (ML) and deep learning (DL) models outperform traditional rule-based security systems. According to Kaur and Sharma (2023), AI enhances intrusion detection systems (IDS) by learning from network data and automatically recognizing malicious activities. However, Malik and Kumar (2024) noted that while AI-based defenses are effective, adversaries are now leveraging AI for offensive attacks, leading to the evolution of 'AI vs AI' warfare. This literature reveals both the promise and peril of AI integration within cybersecurity frameworks.

III. ROLE OF AI IN CYBERSECURITY

AI contributes to cybersecurity through automation, real-time monitoring, and intelligent analytics. Machine learning algorithms analyze vast datasets to identify anomalies that may indicate cyber threats. AI-powered tools like predictive analytics, behavior-based detection, and natural language processing (NLP) enhance capabilities in malware detection, phishing prevention, and vulnerability assessment.

Table 1: Applications of AI in Cybersecurity

AI Technique	Cybersecurity Application
Machine Learning	Intrusion detection, threat prediction
Deep Learning	Malware classification, phishing detection
Natural Language Processing	Spam and social engineering defense
Reinforcement Learning	Adaptive network defense and policy optimization

IV. INHIBITORS AND CHALLENGES IN AI ADOPTION

Despite the proven advantages of AI, several factors hinder its widespread adoption in cybersecurity. These include high implementation costs, lack of transparency in AI algorithms, data privacy concerns, shortage of skilled personnel, and fear of job displacement. Additionally, adversarial AI poses a serious threat, where attackers manipulate AI models to bypass detection. Ethical and legal challenges also persist, as organizations struggle to balance data usage and compliance regulations.

©IJRASET: All Rights are Reserved

Figure 1: Overview of AI Applications in Cybersecurity

This figure conceptually illustrates the integration of AI techniques such as machine learning and deep learning across various cybersecurity layers including endpoint protection, network defense, and user behavior analytics.

V. DISCUSSION AND ANALYSIS

AI's impact on cybersecurity is undeniably transformative, yet its adoption trajectory varies across industries. Organizations with advanced digital maturity adopt AI-based tools faster, while small enterprises remain cautious. The success of AI in cybersecurity depends not only on technological readiness but also on strategic alignment, ethical governance, and workforce competence.

VI. FUTURE SCOPE AND RECOMMENDATIONS

Future research should focus on explainable AI (XAI) models to improve transparency and trust in cybersecurity applications. Collaborative frameworks between academia, industry, and government agencies can foster secure AI innovations. Moreover, developing lightweight AI models suitable for real-time threat detection on edge devices could expand accessibility.

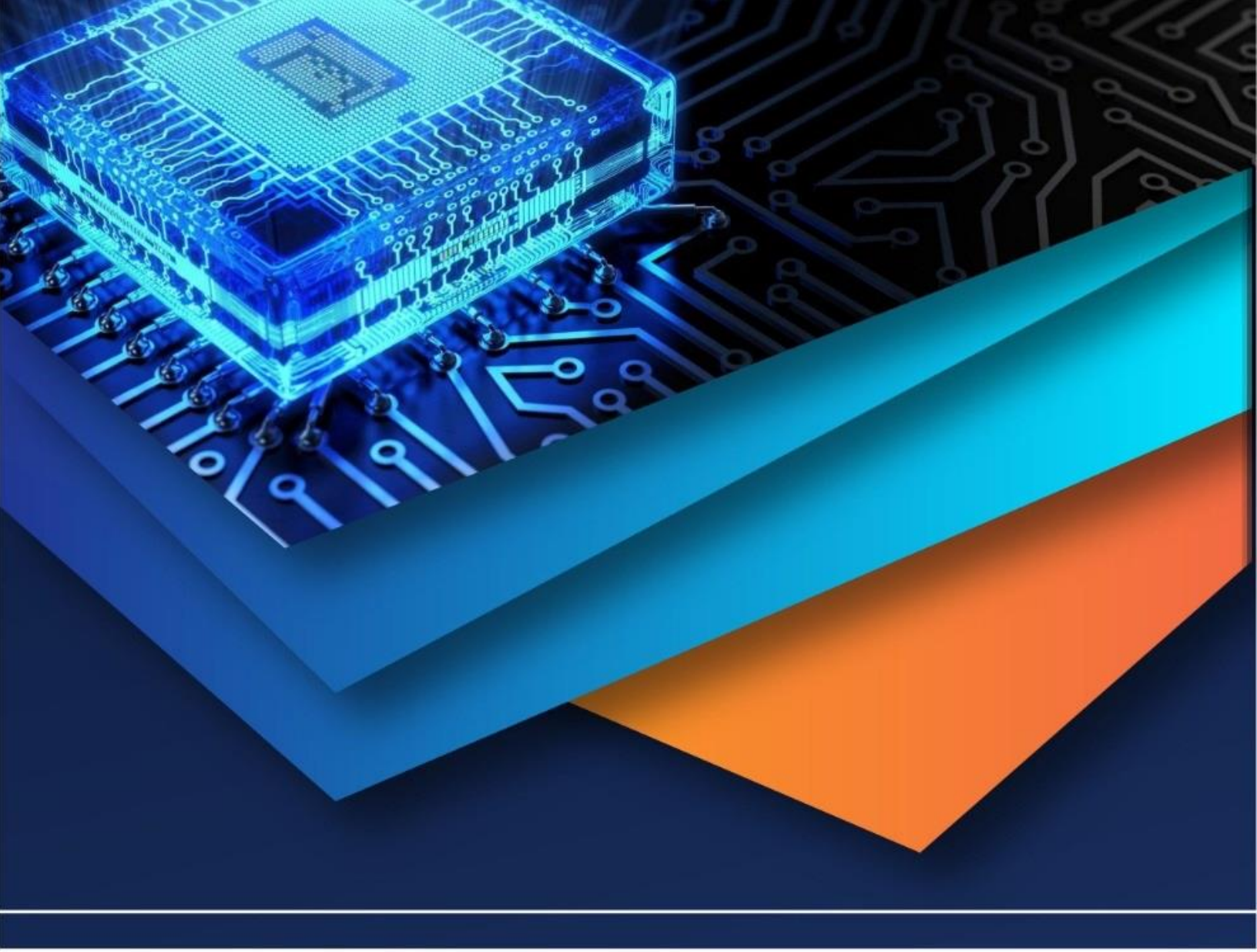
VII. CONCLUSION

This review highlights that AI offers immense potential to revolutionize cybersecurity through automation, prediction, and adaptive learning. However, barriers such as cost, expertise shortage, and ethical dilemmas must be addressed to realize its full potential. A balanced approach involving transparency, collaboration, and standardized policies will ensure the responsible adoption of AI-driven cybersecurity solutions.

REFERENCES

[1] Singh, R., et al., "AI-Powered Threat Detection Systems," IEEE Access, 2022.
[2] Kaur, P., and Sharma, N., "Machine Learning in Intrusion Detection Systems," IJCA, 2023.
[3] Malik, S., and Kumar, A., "Challenges of AI in Cyber Defense," IJCS, 2024.
[4] Das, R., "Barriers to AI Adoption in Security Systems," Journal of Information Security, 2023.
[5] Chen, L., "Explainable AI in Cybersecurity: A Review," Elsevier, 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)