IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, March 2026
Impact Factor: 8.2

AI-Driven Attack Detection System in Cyber Security

Ayesha Mehboob Fahim, Alviya Sajjad Fahim, Arfat Abrar Ulde
Department of Computer Science
Anjuman Islam Janjira degree college of Science, Murud Janjira MS India

Abstract: *The rapid growth of digital technologies and widespread internet usage has led to a significant rise in cyber-attacks, posing serious threats to modern digital systems and networks. Traditional attack detection mechanisms mainly depend on predefined rules and signature-based techniques, which limits their effectiveness against new, complex, and evolving cyber threats. To overcome these limitations, AI-driven attack detection systems have emerged as an advanced and intelligent solution in the field of cyber security. These systems use artificial intelligence and machine learning techniques to analyze network traffic, system logs, and user behavior in order to detect malicious activities in real time. By learning patterns from historical data, AI-based systems can accurately identify both known and unknown attacks while reducing false alarms. This paper explores the role of AI-driven attack detection systems, focusing on their working principles, advantages, and challenges. It also discusses how emerging AI technologies enhance threat detection, prediction, and automated response, making cyber defense systems more adaptive, efficient, and reliable in today's dynamic threat landscape.*

Keywords: Artificial Intelligence, Cyber Security, Attack Detection System, Machine Learning, Anomaly Detection, Network Security

I. INTRODUCTION

Cyber security has become a major concern due to the increasing dependence on digital technologies, cloud services, online transactions, and interconnected networks. Individuals, organizations, and governments are continuously exposed to cyber threats such as malware infections, phishing attacks, ransomware, denial-of-service attacks, and unauthorized system access. These attacks can lead to financial loss, data breaches, service disruption, and loss of trust.

Traditional attack detection systems are mostly rule-based or signature-based, meaning they rely on predefined patterns of known attacks. While these systems are effective against previously identified threats, they fail to detect new, unknown, or rapidly evolving attacks such as zero-day exploits and advanced persistent threats. This limitation makes traditional security approaches insufficient for modern cyber environments.

AI-driven attack detection systems provide a smarter and more adaptive approach to cyber security. By continuously learning from data and monitoring system behavior, AI-based solutions can detect abnormal patterns that indicate potential attacks. The integration of artificial intelligence into cyber security enables faster detection, improved accuracy, reduced false positives, and automated responses. This paper examines the challenges of cyber attack detection and highlights how AI strengthens modern cyber security systems

II. METHODOLOGY

This research focuses on analyzing AI-driven attack detection systems and their effectiveness in cyber security environments. A mixed research approach was used to evaluate existing techniques and practical implementations.

DOI: 10.48175/IJARSCT-35012

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, March 2026
Impact Factor: 8.2

III. DATA COLLECTION AND ANALYSIS

Data was collected from academic research papers, cybersecurity reports, and real-world attack datasets. The data includes information related to network traffic behavior, system activity logs, and known cyber attack patterns.

IV. SYSTEM EVALUATION

AI-based attack detection techniques such as machine learning classifiers, anomaly detection models, and behavioral analysis systems were studied. Key performance factors such as detection accuracy, false positive rate, response time, and adaptability to new threats were considered.

V. CASE ANALYSIS

Reported cyber attack incidents and AI-based detection implementations were reviewed to understand real-world challenges and mitigation strategies.

VI. CHALLENGESCONSIDERED

The study also considers issues such as data imbalance, computational cost, model training complexity, and the need for continuous learning in AI-driven systems.

VII. LITERATURE REVIEW

Several studies highlight the limitations of traditional attack detection systems in identifying modern cyber threats. Early research focused on signature-based detection, which was effective only against known attacks. However, researchers later emphasized the importance of anomaly-based and behavior-based detection methods.

Recent literature shows that machine learning algorithms such as decision trees, support vector machines, and neural networks significantly improve attack detection accuracy. Studies also indicate that deep learning models can detect advanced persistent threats and zero-day attacks more effectively. AI-driven systems reduce false alarms and provide scalable solutions for large networks. Existing research strongly supports the integration of artificial intelligence in cyber security for proactive and adaptive attack detection.

VIII. RESULTS AND DISCUSSION

Results

The analysis shows that AI-driven attack detection systems outperform traditional security mechanisms in several areas:

- Improved Detection Accuracy: AI systems accurately identify both known and unknown attacks.
- Reduced False Positives: Machine learning models minimize unnecessary alerts.
- Real-Time Monitoring: AI enables continuous and automated threat detection.
- Adaptive Learning: Systems improve over time by learning from new data.
- Faster Response: Automated alerts allow quicker mitigation of attacks.

Discussion

The results indicate that traditional security tools alone are insufficient for modern cyber defense. AI-driven systems provide intelligent detection and adaptability, which are essential for handling evolving cyber threats. However, challenges such as data quality, model complexity, and resource requirements must be addressed. Combining AI tools with human expertise and layered security strategies offers the most effective protection.

DOI: 10.48175/IJARSCT-35012

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, March 2026
Impact Factor: 8.2

IX. CONCLUSION

This research concludes that AI-driven attack detection systems are essential for modern cyber security environments. Traditional security approaches are no longer sufficient to handle the growing complexity and volume of cyber attacks. Artificial intelligence enables intelligent, adaptive, and real-time detection of both known and unknown threats.

The integration of machine learning, anomaly detection, and behavioral analysis significantly improves detection accuracy while reducing false positives. Although challenges such as data dependency, computational cost, and model interpretability exist, the benefits of AI-driven systems outweigh these limitations. Future advancements in explainable AI and secure AI model development will further strengthen cyber defense mechanisms. AI-driven attack detection systems are therefore a critical component in building resilient, future-ready cyber security infrastructures.

ACKNOWLEDGEMENT

I sincerely express my gratitude to my respected faculty members for their valuable guidance, encouragement, and academic support throughout this research work. I am thankful to cyber security researchers and professionals whose published studies and reports provided essential knowledge and direction for this paper. I also extend my appreciation to my classmates for their discussions and feedback, and to my family and friends for their constant motivation and support during the completion of this research

REFERENCES

1. Mitchell, T. M., Machine Learning, McGraw-Hill.
2. Goodfellow, I., Bengio, Y., Courville, A., Deep Learning, MIT Press.
3. Buczak, A. L., Guven, E., “A Survey of Data Mining and Machine Learning Methods for Cyber Security,” IEEE Communications Surveys.
4. ISACA, AI-Driven Cybersecurity and Threat Intelligence.
5. SpringerLink, Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation.