IJARASEM

ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 2, March- April 2025

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.028

AI and Machine Learning for Advanced Threat Detection

Mr.N.Karthick, M.Muthuselvam, S.Deepakraj

Assistant Professor, Department of Computer Applications, Sri Krishna College of Arts and Science, Coimbatore, India

Computer Science and Application Student, Department of Computer Application, Sri Krishna College of Arts and Science, Coimbatore, India

Computer Science and Application Student, Department of Computer Application, Sri Krishna College of Arts and Science, Coimbatore, India

ABSTRACT: The increasing complexity and volume of cyber threats demand advanced detection mechanisms beyond traditional security measures. AI and machine learning (ML) offer intelligent, adaptive, and proactive threat detection solutions. Traditional threat detection methods rely on signature-based techniques that struggle to identify new, evolving, or zero-day threats, making networks and systems vulnerable to sophisticated cyberattacks. AI-powered threat detection systems enhance security by identifying anomalies, predicting potential attacks, and automating responses in real time, thereby reducing security risks and improving incident response efficiency. Machine learning models, such as supervised and unsupervised learning algorithms, neural networks, and deep learning techniques, analyze vast datasets to detect and prevent security threats before they cause harm.

I. INTRODUCTION

Cybersecurity threats have evolved rapidly, with attackers leveraging advanced tactics such as polymorphic malware, phishing, and insider threats. Traditional security approaches, such as rule-based intrusion detection systems, often fail against new attack vectors. AI and ML have emerged as powerful tools in cybersecurity, enabling systems to learn from vast amounts of data, recognize patterns, and detect anomalies. This paper explores how AI-driven threat detection improves security by providing real-time responses, reducing false positives, and adapting to new threats.

II. LITERATURE REVIEW

Several studies have explored AI and ML applications in cybersecurity:

- **Intrusion Detection Systems (IDS):** Research by Buczak and Guven (2016) highlights ML-based IDS techniques for real-time threat identification.
- **Anomaly Detection Models:** Studies such as Chandola et al. (2009) demonstrate the effectiveness of AI in identifying malicious activities based on deviations from normal behavior.
- **Deep Learning for Threat Analysis:** Works by Kim et al. (2020) discuss how neural networks improve malware classification and phishing detection.
- **AI-driven SIEM Systems:** Recent advancements integrate AI into Security Information and Event Management (SIEM) systems to enhance threat intelligence.

III. PROBLEM STATEMENT

Traditional security methods rely on predefined rules and signatures, which are ineffective against evolving threats. Cybercriminals exploit zero-day vulnerabilities, evade signature-based defenses, and use AI to bypass security measures. The challenge lies in developing adaptive, scalable, and intelligent threat detection mechanisms that can identify and mitigate advanced cyber threats in real time.

IV. METHOD TO SOLVE

To address these challenges, AI-based threat detection methods include:

1. **Supervised Learning Models:** Training ML algorithms on labeled datasets to classify normal vs. malicious activities.

2. **Unsupervised Learning for Anomaly Detection:** Identifying suspicious activities based on deviations from expected behavior.
3. **Deep Learning for Pattern Recognition:** Using neural networks to detect sophisticated threats, such as polymorphic malware.
4. **Natural Language Processing (NLP):** Detecting phishing emails and social engineering attacks through text analysis.
5. **Automated Threat Response Systems:** Integrating AI-driven Security Orchestration, Automation, and Response (SOAR) platforms.

V. RESULT (ANALYSIS)

AI-powered cybersecurity systems have demonstrated significant improvements in detecting and mitigating threats. Studies show:

- **Reduced False Positives:** AI models improve accuracy by minimizing false alarms compared to traditional rule-based systems.
- **Faster Detection and Response:** Machine learning algorithms analyze vast datasets in real time, significantly reducing incident response time.
- **Improved Threat Intelligence:** AI-driven SIEM solutions enhance predictive analytics, allowing organizations to anticipate and prevent attacks.
- **Enhanced Malware Detection:** Deep learning models outperform conventional antivirus systems in identifying previously unknown malware.

VI. CONCLUSION

AI and ML play a transformative role in advanced threat detection, offering real-time, intelligent, and scalable security solutions. By leveraging AI-driven anomaly detection, automated response mechanisms, and predictive analytics, cybersecurity systems can proactively combat sophisticated cyber threats. Future research should focus on improving AI transparency, adversarial attack resilience, and the integration of AI into global cybersecurity frameworks.

REFERENCES

1. Buczak, A. L., & Guven, E. (2016). "A survey of data mining and machine learning methods for cyber security intrusion detection."
2. Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly detection: A survey."
3. Kim, T., Kang, B., Rho, S., & Kim, H. (2020). "A deep learning approach for detecting malicious web traffic."
4. Sommer, R., & Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection."
5. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). "Cyber threat detection using artificial intelligence."
6. Vinayakumar, R.,Soman, K. P. , & Poornachandran, P. (2019). "Applying convolutional neural networks for network intrusion detection.

IJARASEM

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com