Artificial Intelligence in Cyber Threat Detection

J. Devi Prasath & B. Mani Shankar
Department of Data Science
Sri krishna Adithya College of Arts and Science

Dr. S. Thilagavathi
HOD, Department of Data Science
Sri krishna Adithya College of Arts and Science

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
J, Devi Prasath, et al. "Artificial Intelligence in Cyber Threat Detection." *Shanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 3, 2026, pp. 135–38.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i1-Feb.10272

Abstract

The rapid expansion of the digital infrastructure has drastically increased the vulnerabilities of an organization to different cyber threats. In modern digital times, all sensitive information about financial data, healthcare records, business strategies, and personal information is stored and transmitted online. Due to this very reason, cyber attackers keep finding new ways to hack a system by exploring different kinds of vulnerabilities. Traditional cybersecurity systems rely heavily on predefined rules and signature-based detection mechanisms, which are often inefficient against newly emerging or unknown threats. Fortunately, this is where Artificial Intelligence comes into play. For detecting such large-scale datasets for unusual patterns or the detection of suspicious activities, AI can do these tasks much faster and more accurately. By employing ML and DL, AI can learn from some historical attack data continuously for better performance. Artificial Intelligence-driven solutions are proactive protection by detecting threats before they cause serious damage. This paper discusses the role of AI in cyber threat detection, different AI techniques applied in cybersecurity, real-world applications, benefits, challenges, and future development. This study focuses on how AI has changed the game in cybersecurity from a reactive approach to an intelligent and predictive defense system.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Intrusion Detection, Malware Analysis, Network Security

Introduction

The cybersecurity issue has reached the acme in today's digitized world. Digital data volume has increased since organizations have started adopting cloud computing, online banking, e-commerce, and remote working systems. Simultaneously, this growth has brought expansion in the attack surface for cybercriminals. Sophisticated tools are utilized by hackers to steal data, disrupt services, and demand ransom payments. Traditional security systems were designed to detect known threats by using signature-based methods. These systems compare incoming files or network traffic against a database of known malicious signatures. While efficient in previously identified threats, these systems fail at detecting zero-day attacks and APTs. Artificial Intelligence offers a new approach to cybersecurity.

Instead of relying on just predefined rules, AI systems base themselves on the analysis of behavior and patterns of anomalies. In an intelligent way, AI will be able to identify suspicious activities if an attack is new because it learned from past data. Such an intelligent detection mechanism makes AI a powerful tool in modern cybersecurity strategies.

Evolution of Cyber Threats

Over the last decades, cyber threats have gradually developed. Initially, cyber-attacks were simple and mostly targeted individual computers. Most of the early viruses were designed either out of curiosity or for minor mischief. As soon as internet connectivity spread, cyber-attacks started to be achieved in a more organized way and with financial reasons.

Today, cybercriminals operate as highly organized groups. They conduct ransomware campaigns, phishing kits, botnets, and exploit kits for a well-structured assault. In cases of ransomware attacks, critical data is encrypted and can only be decrypted upon receipt of payment in cryptocurrency. Phishing attacks dupe users into revealing sensitive information like passwords and bank details.

Advanced Persistent Threats mean complex targeted attacks on organizations, especially government institutions and enterprises. It is hard to detect these kinds of threats because one attacker remains hidden in the systems for years.

With the ever-increasing sophistication of cyber-attacks, no less than intelligent detection systems able to adapt to new attack strategies will do the trick. It is in this direction that Artificial Intelligence plays its part.

Role of Artificial Intelligence in Cybersecurity

Artificial Intelligence helps in improving cybersecurity through the addition of automation, flexibility, and predictive analysis. AI systems can deal with the huge volume of data being generated by networks, servers, and devices. It is almost impossible to monitor the data manually.

AI-based cybersecurity systems have several functions:

- Continuous Monitoring of Network Traffic
- Identification of abnormal user behavior
- Detection of malware patterns
- Automated threat response
- Risk Assessment and Vulnerability Prediction

Contrary to previous systems, AI systems are capable of identifying unfamiliar and familiar threats through the detection of unusual deviations from normal behaviors. For instance, if a person tries to log into a system from a strange location or at a strange time, the AI system recognizes the behavior.

Machine Learning Techniques in Threat Detection

Machine Learning is a field in AI that allows systems to be trained to learn from the data they receive without being programmed to perform. ML algorithms are applied in the detection of cyber attacks due to their accuracy.

Supervised Learning

In the case where the model is required to learn, the learning process is referred to as supervised learning. In this case, malware detection is done with regard to the labels provided, e.g., malicious or non-malicious files. Here, models like Decision Tree, Random Forest, and Support Vector Machine are used.

Unsupervised Learning

Unsupervised learning does not require labels on the data. Instead, it looks for hidden patterns or anomalies. The use of this method is seen in identifying unknown dangers or abnormal behavior in the network. The clustering method, like K-Means, helps in clustering similar data points.

Reinforcement Learning

Reinforcement learning involves training models through rewards and penalties. In cybersecurity, this technique can help systems learn optimal defense strategies through continuous interaction with network environments.

Deep Learning in Cybersecurity

Deep Learning is a sophisticated form of Machine Learning that makes use of multi-layer neural networks. It is best utilized for analyzing large and complex data sets.

Convolutional Neural Networks (CNN) are also capable of detecting malware effectively by analyzing file structures in the form of images. Recurrent Neural Networks (RNN) find application in analyzing network traffic logs.

The Deep Learning approaches are capable of detecting complex threats. However, this needs large datasets as well as computational power.

Applications of AI in Cyber Threat Detection

Malware Detection

AI-based systems analyze file behavior rather than relying only on signatures. They monitor how a file interacts with the system, such as modifying registry entries or accessing sensitive files. Suspicious behavior triggers alerts.

Phishing Detection

AI examines email content, sender information, embedded links, and writing style. It can identify subtle indicators of phishing that human users may overlook.

Intrusion Detection Systems (IDS)

AI enhances IDS by continuously monitoring network traffic. It detects unusual spikes in traffic, unauthorized access attempts, and abnormal data transfers.

Fraud Detection in Banking

Financial institutions use AI to analyze transaction patterns. If a transaction deviates from a customer's usual behavior, the system may temporarily block it for verification.

Benefits of AI in Cybersecurity

AI has a substantial impact on the performance of cybersecurity. This is because AI detects attacks and threats much faster, and its accuracy is also higher. In addition, AI helps reduce human workload, and its response to attacks also prevents the

AI may also aid in predictive data analysis by discovering weaknesses before they are exploited by hackers, thereby enhancing the security posture..

Challenges and Limitations

Though there are many benefits in using AI, there are also certain challenges involved. To start with, building an AI model demands high quantities of data. If the quality is bad, then wrong predictions will result.

False positives are still a problem, and if false alerts are too frequent, users might lose trust in the model. Finally, there is always a possibility of attacks using adversarial methods.

Cost to implement AI-based security solutions is high, especially for small organizations. Updating these solutions and hiring professionals is also very costly.

Future Trends

The integration of AI with other emerging technologies such as IoT, cloud computing, and 5G networks has a positive impact on cybersecurity. AI-powered SOC will provide automation for detecting and responding to security incidents.

Explainable AI (XAI) would enhance transparency levels as the security analysts will be in a position to understand the decision-making process of the AI systems. This would enhance trust in AI-based cybersecurity systems.

Conclusion

In conclusion, the advent of advanced digital technologies has raised the stakes in terms of cyber attacks and their complexity. The existing traditional security measures, which base their responses on set guidelines and characteristics, are no longer effective in the detection of unknown cyber attacks. Artificial Intelligence is an advanced and intelligent approach in the management of cybersecurity, where large amounts of data are analyzed in line with identifying unusual patterns.

AI-based security systems employ Machine Learning or Deep Learning techniques for improved detection accuracy and response time. AI has the capability of learning from past threats and adapting to new ones, thus making it more efficient compared to traditional security solutions. AI systems are also seen to have improved response time since they automate the detection of new threats.

Despite the challenges like the expense, data requirements, and false messages, AI plays a vital role in cyber defense. Artificial Intelligence is expected to improve further with a more effective implementation in the future and help strengthen security systems.

Reference

1. 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.
2. 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.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
4. Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Computer Science, 2(3), 160.
5. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), 1–58.
6. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Applying Deep Learning Approaches for Network Traffic Prediction. Journal of Network and Computer Applications, 86, 1–17.
7. Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2011). Zero-day Malware Detection Based on Supervised Learning Algorithms. International Conference on Industrial Electronics and Applications, 1–6.
8. Patcha, A., & Park, J. M. (2007). An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. Computer Networks, 51(12), 3448–3470.
9. Shaukat, K., et al. (2020). A Survey on Machine Learning Techniques for Cyber Security in Big Data. IEEE Access, 8, 119134–119162.
10. IBM Security. (2023). Cost of a Data Breach Report. IBM Corporation.