CompSci Journal
Double Blind Peer Reviewed, Open Access International Research Journal.
ISSN: 3067-3089 | *Website: https://csjour.com | Volume-2, Issue-2 | April - 2026*

Original Article

Role of Artificial Intelligence in Cyber security

Vrunda Sanjay Sable
Lecturer, Hirwal education trust's collage of scince (computer science and information technology), Mahad, raigad

Manuscript ID:
CSJ-2026-020236

Volume 2

Issue 2

Pp.187-190

April 2026

ISSN: 3067-3089

Submitted: 12 Mar. 2026

Revised: 25 Mar. 2026

Accepted: 15Apr. 2026

Published: 30 Apr. 2026

Correspondence Address:
vrunda sanjay sable
Lecturer, Hirwal education trust's collage of scince (computer science and information technology), Mahad, raigad
Email: sablevrunda@gmail.com

Quick Response Code:

Web. https://csjour.com/

DOI: 10.5281/zenodo.21155534

DOI Link:
https://doi.org/10.5281/zenodo.21155534

Abstract

Due to the accelerated advancement of digital technology, it is no surprise to find that cyber-crimes have become more sophisticated than ever and are being carried out at an unprecedented rate. Traditional security models and current anti-virus software are unable to keep pace with the number of attacks on organizations, due to all of the data generated and the extremely large amounts of information that must be processed. As such, new technologies have emerged to improve the detection of and response to both existing attacks and future threats, including Artificial Intelligence (AI). In this paper, we will look at the uses of AI in cyber protection, along with advantages and disadvantages, as well as possible future developments. More specifically, AI-based technologies like machine learning (ML) and natural language processing (NLP) in the field of Computer Science have provided enhanced capabilities to improve the protection of cyber systems and increase the overall effectiveness of threat detection and management activities.

Keywords: *Artificial Intelligence (AI), Cybersecurity, Machine Learning, Deep Learning, Threat Detection, Network Security, Malware Detection, Phishing Detection, Behavioral Analytics, Natural Language Processing (NLP), Automated Threat Response, Fraud Detection.*

Introduction

Organizations are becoming more and more reliant on cloud-based systems and interconnected ones, making Cybersecurity an ever-increasing area of concern. Cyber threats like malware, phishing, ransomware and data breaches are on the rise and growing increasingly sophisticated. Traditional security tools typically utilize pre-defined rules or signatures to detect and respond to threats. Unfortunately these tools are becoming less and less effective at detecting new or unknown types of cyber threats. Artificial Intelligence can help to provide an intelligent way to secure a network through dynamic security mechanisms that learn from data patterns to detect threats in real time. New AI-based cybersecurity systems can monitor network traffic, recognize abnormal behavior, and respond to cyber threats faster than ever before. With the rise of technology in current society today, we have all become very dependent on the use of computer systems, networks, and online services to store/process very large amounts of sensitive information/data. As our technology evolves, however, so do the methods that criminals use to steal information such as hacking, malware, phishing, and data breaches. Traditional methods of cyber security have had difficulty keeping up with this rapidly changing landscape of cyber-attacks. As a direct result of these challenges, there has been an increasing amount of interest in using artificial intelligence (AI) in the field of cybersecurity. AI has the ability to perform functions that would normally require human-like level intelligence (i.e., learn, recognize patterns, make decisions, solve problems, etc.) And because of this, allowing security systems to effectively and quickly monitor for unusual activity, detect potential sources of the threat and respond to the cyber-attack in real-time. Machine learning, deep learning, and behavioral analytics, are being used to analyze large amounts of data in order to identify suspicious behavior indicative of an imminent cyber-attack by utilizing machine learning enabled Cyber Security Tools. Traditional Cyber Security Tools typically rely on pre-configured rules, whereas AI systems continue to evolve through their experience of newly acquired data sets, resulting in a much higher level of accuracy when it comes to identifying and addressing new or emerging threats. When an organization implements systems that employ AI methodologies, it will provide greater accuracy.

How to cite this article:
Sable, V. S. (2026). Role of Artificial Intelligence in Cyber security. CompSci Journal, 2(2), 187–190. https://doi.org/10.5281/zenodo.21155534

Artificial Intelligence in Cybersecurity

Artificial Intelligence enables computer systems to execute tasks which normally require human intelligence abilities. AI technologies in cybersecurity provide protection through their ability to detect threats and predict attacks and execute security tasks automatically. Cybersecurity employs the following primary AI technologies:

- Machine Learning (ML) enables systems to learn from historical data which leads to the identification of cyber threats.
- Deep Learning uses neural networks to identify complicated attack patterns which require deep analysis.
- Natural Language Processing (NLP) enables users to evaluate threat intelligence reports while it also helps them identify phishing email messages.
- Behavioral Analytics uses user behavior monitoring to identify instances of insider threats.

Applications of AI in Cybersecurity

Threat Detection

The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The system has been developed to examine data until October 2023. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The system has been developed to examine data until October 2023. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. The system has been developed to examine data until October 2023. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. The system has been developed to examine data until October 2023. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities. The system has been developed to examine data until October 2023. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. The AI system monitors network traffic to identify cybersecurity threats through its detection of unusual network behavior. Machine learning algorithms can identify malware, suspicious login attempts, and abnormal system activities.

Benefits of AI in Cybersecurity

1. AI detects cyber threats through its real-time capabilities.
2. AI technology enables fast security data analysis of extensive data sets.
3. Automation technology decreases human errors which occur during manual analysis work.
4. AI systems have the ability to discover patterns which human observers will not identify.
5. AI technology enables security teams to anticipate future cyber threats through its

Quick Threat Detection

Networks and users are able to track their behavior through artificial intelligence (AI) systems, ensuring that anything out of the ordinary is detected. Through learning the usual behaviour of networks and users, AI systems can identify an unusual activity very quickly, including malware, phishing attacks and unauthorised user access.

Predicting Future Cyber-attacks

By analysing the most common behaviours in a data set of previous cyber-attacks through machine learning allows for the ability to create patterns to help predict and prevent future attacks before they take place.

Automated Threat Response

When a cyber-threat occurs with a fast enough response time, such as the deletion of a virus on a computer and even to block an IP address will all occur within this timeframe without any human intervention required.

Improved Fraud Detection

Banks and online services use AI algorithms to detect fraud before it happens by analysing user behaviours of their customers to flag any unusual behaviours such as logging in from an unrecognised location, suddenly changing their spending behaviour etc.

Reduced Workload for Humans in Cyber Security

Every day cyber security teams receive thousands of alerts of potential cyber threats. AI can assist cyber security teams filter out most of these false alarms and question real alerts, improving an organisation's ability respond to a real threat and allowing experts to focus on the most urgent matters.

Constant Monitoring (Year-a-Round Protection)

Artificial Intelligence (AI) can monitor a network with no breaks for rest or fatigue. As a result, it will provide continuous protection for a business against cyber threats.

Improved Malicious Software Detection

Malware protection is a primary focus of protecting an organisation from cyber threats. Traditional malware detection programs operate off of known malware definitions and AI has the ability to identify new malware by establishing the behaviours of the example (new or previously unknown) malware.

12 Enhanced Phishing Detection

Email phishing scams can often go unnoticed until it is too late. AI-powered email filtering systems can reduce this threat by filtering out suspected phishing attempts through analyzing an email's language patterns, links that may raise suspicions and sender behaviours. Predictive capabilities.5. Challenges of AI in Cybersecurity

Gh analyzing an email's language patterns, links that may raise suspicions and sender behaviours.

Conclusion

The cyber security field depends on artificial intelligence which provides essential methods for threat detection and enables organizations to handle security breaches more efficiently while its predictive capabilities protect systems against imminent security threats. Ongoing development work is necessary to combine AI technologies with current cybersecurity systems, which will improve defense capabilities against contemporary cyber threats. AI technology will become an essential component for digital infrastructure protection and sensitive information security throughout all future technology developments. AI (Artificial Intelligence) is reshaping how we protect our networks through the inclusion of machine learning, behavioral analysis, and anomaly detection. Cyber security companies are using AI to help detect cyber threats faster and more accurately and allow for more efficient response and tracking of cyber-attacks with real-time alerts. With the advancement of technology, cyber criminals are enhancing their techniques; therefore, AI has become a necessary element for defending against cyber criminal activities. By using AI techniques, Cyber Security professionals can identify suspicious behavior on networks prior to causing significant harm and help formulate proactive countermeasures with the goal of minimizing the risk of damage to critical assets and data (i.e., sensitive data and IT infrastructure). AI provides supplemental assistance to Cyber Security personnel by analyzing massive volumes of data that can be analyzed to identify priority(s) (i.e., perpetrator detecting). Furthermore, AI also assists Cyber Security teams with terrorism mitigation by assisting with fraud detection, detecting and preventing digital malware, detecting and preventing phishing attacks, and as an integral part of an enterprise-wide Intrusion Detection System. The on-going proliferation of cyber-crime will continue to challenge all organizations that use technology and should therefore incorporate AI into cyber security solutions to ensure appropriate protection against emerging threats. Beyond the challenges posed by the use of AI in Cyber Security, it should be noted that cyber-criminals are able to utilize AI to develop more sophisticated attacks; therefore, organizations must continually update and improve their AI-generated cyber security defence. In addition, corporate America must manage the ongoing concerns regarding privacy, ethical, and potential skills shortages as they relate to AI applications within Cyber Security. Although AI continues to evolve; it is not a total replacement for human expertise; rather, AI serves as a complementary means of enhancing the overall effectiveness and efficiency of cyber security solutions to protect, preserve, and promote secure digital environments.

Acknowledgement

I would like to express my sincere gratitude to all those who contributed directly and indirectly to the completion of this research paper entitled "Role of Artificial Intelligence in Cybersecurity." I am especially thankful to the management, Principal, and faculty members of Hirwal Education Trust's College of Science (Computer Science and Information Technology), Mahad, Raigad, for providing valuable guidance, encouragement, and academic support throughout the study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Achine Learning and Security – by Clarence Chio and David Freeman, O'Reilly Media, 2018.
2. Artificial Intelligence for Cybersecurity – Edited by Sanjay Misra, Robertas Damaševičius, and Rytis Maskeliūnas, Springer, 2020.
3. Artificial Intelligence and Machine Learning for Cybersecurity – by Sushil Jajodia, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang, CRC Press, 2021.
4. Asaf Shabtai, Lior Rokach, & Yuval Elovici (2015). "A Survey of Data Mining Techniques for Cyber Security." Published in Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery.
5. Igor Kotenko & Evgeny Doynikova (2016). "Machine Learning for Network Security." Published in Computer Networks.
6. N. Moustafa & Jill Slay (2015). "UNSW-NB15 Dataset for Network Intrusion Detection Systems." Published in IEEE conference proceedings.
7. Ian Goodfellow, Jonathon Shlens, & Christian Szegedy (2015) "Explaining and Harnessing Adversarial Examples." Presented at International Conference on Learning Representations.
8. Nicolas Papernot, Patrick mcdaniel, Arunesh Sinha, & Michael Wellman (2016). "sok: Security and Privacy in Machine Learning." Presented at IEEE European Symposium on Security and Privacy.
9. National Institute of Standards and Technology (NIST). "Artificial Intelligence and Cybersecurity Framework."

10. European Union Agency for Cybersecurity (ENISA). "Artificial Intelligence and Cybersecurity: Threats and Opportunities."
11. IBM (2023). "AI in Cybersecurity Report."
12. Cisco (2023). "AI-Driven Security Report."
13. Mcafee (2022). "Artificial Intelligence in Cybersecurity."
14. Palo Alto Networks (2023). "AI and Machine Learning in Threat Detection."
15. Kaspersky (2022). "Machine Learning Methods for Cybersecurity."
16. Microsoft (2023) "AI for Cyber Defense."
17. Google (2024). "Artificial Intelligence and Cybersecurity Applications."
18. MIT Technology Review (2022). "AI in Cybersecurity: Opportunities and Challenges."
19. World Economic Forum (2023) "Global Cybersecurity Outlook."
20. Gartner (2023). "Artificial Intelligence in Security Operations."
21. International Data Corporation (IDC). "AI-Based Cybersecurity Market Report."
22. Symantec (2021). "Artificial Intelligence in Threat Detection."
23. Crowdstrike (2023). "AI-Powered Threat Intelligence."
24. Check Point Software Technologies (2022). "AI in Network Security."
25. "Role of Artificial Intelligence in Cybersecurity." Published in International Journal of Computer Applications, 2021.
26. "Artificial Intelligence for Intrusion Detection Systems." Published in International Journal of Advanced Computer Science and Applications, 2020.
27. "Deep Learning Applications in Cybersecurity." Published in Journal of Information Security, 2019.
28. "AI-Based Malware Detection Techniques." Published in IEEE Access, 2021.
29. "Cybersecurity Threat Detection Using Machine Learning." Published in Future Generation Computer Systems, 2020.
30. "AI-Driven Cybersecurity Threats and Defensive Strategies." Published on arxiv, 2024.
31. "Explainable Artificial Intelligence for Cybersecurity." Published on arxiv, 2022.