ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: AN OVERVIEW

Vijay Raut
Research Scholar, Dr. D Y Patil School of Management Research Centre, Pune

Dr. E B Khedkar
Director and Research Center Head, Dr. D Y Patil School of Management Research Centre, Pune

Abstract
AI reduces manual work and speeds up data security. Teams use AI to find and label sensitive data across the environment. This works on local infrastructure or in cloud apps. AI also detects attempts to move data outside the company. It can block the action or alert the security team. Extended detection and response (XDR) and security information and event management (SIEM) tools help teams find cyberthreats across the business. Both systems rely on AI. XDR tools use AI to watch endpoints, emails, identities, and cloud apps for strange behavior. They connect incidents and show them to the team. XDR systems also use advanced models to stop attacks like ransomware. They offer tips to improve security coverage. SIEM systems use AI to collect signals from across the company. This gives teams a clear view of events. Teams use AI to get useful details from threat intelligence. This helps them handle cyber risks early. This paper reviews the role of AI in cyber security.
***Keywords**: Artificial Intelligence, Cyber threat, Cyber Security, AI tools*

1. Introduction

AI reduces manual work and speeds up data security. Teams use AI to find and label sensitive data across their systems. This works on local hardware or in cloud apps. AI also spots attempts to move data outside the company. It blocks the action or alerts the security team. Extended detection and response (XDR) and security information and event management (SIEM) tools help teams find cyberthreats across the business. Both systems rely on AI. XDR tools use AI to watch endpoints, emails, identities, and cloud apps for odd activity. They connect incidents and show them to the team. XDR systems also use advanced models to stop attacks like ransomware. They offer tips to improve security coverage. SIEM systems use AI to collect signals from across the company. This gives teams a clear view of events. Teams use AI to get useful details from threat intelligence. This helps them handle cyber risks early. This paper reviews the role of AI in cyber security (Byrnes & Spear, 2023).

We must distinguish between two related concepts. These are AI for cybersecurity and security for AI. AI for cybersecurity uses tools to better detect, respond to, and reduce threats. It covers an organization's full environment. These tools analyze and connect events from multiple sources. This process helps teams identify patterns that show a potential threat. AI security focuses on protecting the AI systems themselves. (Liang et al., 2023) It includes strategies, tools, and practices to guard models, data, and algorithms. You need systems to work as intended. Attackers must not use flaws to change outputs or steal private information. AI for cybersecurity uses systems to strengthen an organization's total defense. AI security protects the systems (Hua et al., 2024).

2. Benefits of AI for cybersecurity

Artificial intelligence changes how we handle cybersecurity. It helps security professionals respond to more threats. They handle more data and a wider attack surface. Here are ways AI helps teams work better (Cabanac, 2024):

Faster threat detection

Security solutions like SIEM or XDR log thousands of events. These suggest strange behavior. Most events are harmless. Some are not. The risk of missing a threat is high. AI identifies incidents that matter. It connects separate activities to show real dangers.

Simplified reporting

Tools with generative AI combine information from many sources. They create clear reports. Security professionals share these quickly with others in the organization.

Vulnerability identification

AI detects weaknesses in the system. These include unknown devices, cloud apps, or old operating systems. It also finds unprotected sensitive data.

Skills enhancement

Generative AI translates threat data into natural language. Analysts do not need to write code queries to work well. Junior analysts can handle harder tasks. The technology also provides repair steps and advice. New team members learn quickly how to stop attacks.

Actionable insights

AI collects and studies data from sources like security logs, network traffic, and threat feeds. It

gives a full picture of security status. It reveals hidden attack patterns.

Reduction of false positives and false negatives
AI reduces false positives and false negatives. It uses techniques like pattern recognition, anomaly detection, and context. The systems learn continuously. They make precise decisions. This stops useless alerts from overwhelming security teams.

Scalability
AI improves scalability in cybersecurity. It automates tasks and processes large data sets in real time. It learns without stopping. Threat volume and complexity are growing. AI scales and adapts to meet these changes. This keeps security systems strong and fast. They can handle the demands of modern IT networks.
Artificial intelligence is part of many cybersecurity tools and makes them work better. Here are a few examples:

3. AI-powered cybersecurity tools

Next-generation firewalls and AI
Old firewalls use administrator rules to allow or block traffic. Next-generation firewalls do more. They use AI and access threat intelligence data. This helps them find new cyber threats (Clarivate, 2024).

AI-enhanced endpoint security solutions
These tools use AI to find endpoint weaknesses like old operating systems. AI also checks if malware is on a device. It sees if strange amounts of data leave or enter an endpoint. AI automatically separates the endpoint from the rest of the network during an attack.

AI-driven network intrusion detection and prevention systems
These tools watch network traffic. They find unauthorized users trying to break into the organization. The systems use AI to process huge amounts of data fast. They identify and block attackers before damage occurs.

AI and cloud security solutions
Many organizations use multiple clouds for infrastructure and apps. It is hard to track threats moving between these different places. AI aids cloud security. It analyzes data from all sources to spot weaknesses and possible attacks (Elsevier, 2024).

Internet of Things (IoT) security
Organizations often have many IoT devices. These are possible entry points for attacks. AI detects threats against single devices. It also finds suspicious patterns across many devices.

XDR and SIEM
These solutions take information from many security products, log files, and outside sources. They help analysts understand events in their environment. AI combines this data into clear findings.

4. Best practices for using AI in cybersecurity

Using AI in security operations needs careful planning. The right plan helps you add tools that improve results. This boosts operational success and helps your team feel better.

Develop a strategy
Many AI products exist for security, but not all fit your organization. Your AI tools must work well together and fit your security setup. Otherwise, they create more work for your team. Look at your biggest security problems first. Find AI tools that fix those specific issues. Make a plan to add AI to your current systems and workflows (Gao et al., 2024; Gunkel, 2025).

Integrate your security tools
Cybersecurity AI works best when it analyzes data from the whole organization. Siloed tools make this hard. Buy tools that work together and fit your network. XDR and SIEM tools are good examples. You can also give your team time and money to connect these tools. This gives you full visibility of your digital assets (Goyal et al., 2025).

Manage data privacy and quality
AI systems use training data to make choices. Bad or corrupted data leads to bad results. The AI will make wrong decisions. You must set up processes during the planning phase. These processes should clean the data and protect privacy.

Use AI ethically
Years of collected data often contain errors, bias, or old information. AI logic is not always clear. You might not know how the system reaches a conclusion. Do not let AI make the final call if fairness is at risk. Biased data can lead to unfair treatment of people. Read more about responsible AI.

Continuously test your AI systems
Test your systems often after you launch them. New data comes in constantly. You must catch bias or quality problems early.

Define policies for using generative AI
Verify that staff and partners know your rules for generative AI. They must not paste private or sensitive data into prompts. That data could become public (Knox & Knox, 2024).

5. New trends in AI for cybersecurity

AI is part of cybersecurity now. It changes how teams find and stop threats. It also reshapes the workforce. Several patterns appear as AI grows common in the industry:

Security experts will spend more time on major decisions and hard problems. AI will handle the daily work.

Employers will need people for hybrid roles. These jobs mix cybersecurity knowledge with AI skills. Examples include AI cybersecurity analysts or data scientists who focus on security.

Security centers will move toward active threat hunting. Teams will use AI to help with deep searches. They will look for hidden threats that standard tools might miss.

Security centers will change into spaces run by AI. Humans will look at the results and make decisions. They will not have to manage too much data.

Vendors will sell better AI security products. These include video analysis tools. They also include drones and robots for physical safety.

Deception tech will build smart traps. These traps look like real assets. Criminals will struggle to tell the real targets from the fake ones.

Fraud detection systems will use machine learning to stop fraud early. They predict cheating before it happens. This reduces false alarms and makes detection more accurate.

AI agents can handle heavy tasks on their own. They manage duties like sorting alerts. This gives people time to work on other needs.

6. Conclusion

AI is used by teams to locate and mark sensitive data within their systems. This functions in cloud apps or on local hardware. Attempts to transfer data outside the organization are also detected by AI. It either notifies the security personnel or stops the action. Teams can identify cyberthreats throughout the company with the use of security information and event management (SIEM) and extended detection and response (XDR) solutions. AI powers both of these systems. AI is used by XDR tools to monitor identities, emails, endpoints, and cloud apps for unusual activity. They link incidences together and provide them to the team. Advanced models are also used by XDR systems to prevent ransomware assaults. They provide advice on how to increase security coverage. AI is used by SIEM systems to gather information from all areas of the business. This provides teams with a clear picture of the security position.

References

1. Byrnes, J., & Spear, A. (2023). Algorithmic Epistemic Injustice.
2. Cabanac, G. (2024). The tortured phrases of scientific publishing. Retraction Watch.
3. Clarivate. (2024). Pulse of the Library 2024: Assessing the pulse of the library. Clarivate Analytics.
4. Elsevier. (2024). Insights 2024: Attitudes toward AI. Elsevier.
5. Gao, Z., Brantley, K., & Joachims, T. (2024). Reviewer2: Optimizing Review Generation Through Prompt Generation. arXiv.
6. Goyal, A., Tariq, M. D., Ahsan, A., Khan, M. H., Zaheer, A., Jain, H., Maheshwari, S., & Brateanu, A. (2025). Accuracy of artificial intelligence in meta-analysis: A comparative study of ChatGPT 4.0 and traditional methods in data synthesis. World Journal of Methodology, 15(4), 102290. https://doi.org/10.5662/wjm.v15.i4.102290
7. Gunkel, D. J. (2025). AI Signals The Death Of The Author. Noema Magazine.
8. Hua, Y., Liu, F., Yang, K., Li, Z., Na, H., Sheu, Y.,... & Beam, A. (2024). Large Language Models in Mental Health Care: a Scoping Review. arXiv.
9. Knox, M. P., & Knox, A. W. (2024). Artificial Intelligence in Higher Education: Ethical Challenges, Governance Frameworks, and Student-Centered Pathways. ResearchGate.
10. Liang, W., Zhang, Y., Cao, H., Wang, B., Ding, D., Yang, X.,... & Zou, J. (2023). Can large language models provide useful feedback on research papers? A large-scale empirical analysis. arXiv preprint arXiv:2310.01783.