ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Siasha Arora

Semester III, Student of Computer Science, Manipal University, Jaipur

ABSTRACT

Artificial Intelligence (AI) refers to the application of intelligent algorithms and machine learning techniques to enhance the detection, prevention, and response to cyber threats. AI empowers cybersecurity systems to analyze vast amounts of data, identify patterns, and make informed decisions, at speeds and scales beyond human capabilities.

The role of AI in bolstering security measures is multifaceted. It can automate routine tasks such as log analysis and vulnerability scanning, freeing up human analysts to focus on more complex and strategic activities. AI in cybersecurity plays a crucial role in threat detection. AI-powered systems can detect threats in real-time, enabling rapid response and mitigation. Moreover, AI can adapt and evolve, continuously learning from new data and improving its ability to identify and counter emerging threats.

AI in cybersecurity revolutionizes threat detection, automates responses, and strengthens vulnerability management. As threats grow more sophisticated, adopting stronger cyber security preparedness ensures organizations can respond faster and minimize potential impact. By analyzing behaviors, detecting phishing, and adapting to new threats, AI enhances cybersecurity strategies, enabling proactive defense and safeguarding sensitive data.
KEYWORDS-AI, cybersecurity, revolution, data, threats, mitigation

INTRODUCTION

AI in cybersecurity reinforces cyber threat intelligence, enabling security professionals to detect and mitigate threats arising from AI and cybercrime trends by:

Search for characteristics of cyberattacks: AI analyzes massive volumes of data to identify patterns and indicators of compromise. Understanding how neural networks work also strengthens this analysis by helping AI models detect subtle anomalies that may signal early stages of an attack. This approach helps security teams identify suspicious network behavior, unusual login attempts, and abnormal traffic from IoT devices or endpoints in real-time.
Strengthen defenses: AI can help security teams isolate compromised devices, block malicious traffic, and stop malware by continuously monitoring systems. Besides, it predicts high-risk areas where breaches are most likely, allowing organizations to proactively address vulnerabilities before they raise serious concerns.[1,2,3]
Analyze data to authenticate users: AI tools can help security teams analyze user authentication data, such as fingerprints, typing styles, and voice patterns. Besides, they can monitor user behavior during sessions, detecting anomalies and triggering additional verification when needed.
Attribute attacks to specific threat actors: AI can analyze tools used, IP addresses, and behavioral patterns and link incidents to known threat actors. This makes it easy for security teams to understand and identify specific threat groups.

Enhance phishing and spam detection: AI helps scan email links, attachments, and messages, blocking phishing and spam attempts before they escalate.
Support collaborative threat intelligence sharing: AI enables organizations to contribute to and benefit from shared knowledge within security communities, improving collective resilience against evolving AI-driven threats. This intelligence-led approach is especially critical for the AI data center, where attack surfaces expand with scale and automation.
Strengthening cybersecurity currently requires human intervention. However, tasks such as system monitoring can be automated through AI. Automating the process will increase organizations' threat intelligence capabilities and save them time discovering new threats. This is vital as cyberattacks increase in sophistication.

Cybersecurity automation using AI is safe because it is built on existing use cases in various business environments. For example, human resources (HR) and information technology (IT) teams use AI to onboard new employees and provide them with the resources and appropriate level of access to do their job effectively. [4,5,6]

Automation is particularly important in cybersecurity given the ongoing shortage of expert security staff. This allows organizations to enhance their security investments and improve operations without having to worry about finding additional skilled personnel.

The benefits of automating AI in cybersecurity include:

Cost-efficiency: Pairing cybersecurity with AI results in faster data collection. This makes incident management response more dynamic and efficient. It also removes the need for security professionals to carry out manual, time-consuming tasks so they can focus on more strategic activities that add value to the business.
Removing human error: A common weakness of traditional security defenses is the need for human intervention, which can lead to costly human error. Artificial intelligence in cybersecurity removes the human element from most security processes. This is a more efficient approach because human resources can be reallocated to where they are most required.
Better decision-making: Automating cybersecurity helps organizations identify and correct potential deficiencies in their security strategy. In this way, they are able to implement formalized procedures that can result in more secure IT environments.
However, organizations also need to be aware that cyber criminals adjust their methods to resist new AI cybersecurity tools. Hackers also use AI to create advanced attacks and deploy new and updated forms of malware to target both traditional and AI-enhanced systems.

DISCUSSION

Key applications of AI in cybersecurity
1. Password protection and authentication
With AI in cybersecurity, organizations can better protect passwords and secure user accounts through authentication. Most websites include features that allow users to log in to purchase products or contact forms for people to input sensitive data. Extra security layers are necessary to keep their information secure and prevent it from getting into the hands of malicious actors.

AI tools, such as CAPTCHA, facial recognition, and fingerprint scanners enable organizations to automatically detect whether an attempt to log in to a service is genuine. These solutions help

prevent cybercrime tactics like brute-force attacks and credential stuffing, which could put an organization's entire network at risk.

2. Phishing detection and prevention control
Phishing remains one of the biggest cybersecurity threats facing businesses across all industries. AI within email security solutions enables companies to discover anomalies and indicators of malicious messages. It can analyze the content and context of emails to quickly find whether they are spam messages, part of phishing campaigns, or legitimate. For example, AI can quickly and easily identify signs of phishing, such as email spoofing, forged senders, and misspelled domain names. [7,8,9]

ML algorithm techniques allow AI to learn from data to make analysis more accurate and evolve to address new threats. It also helps AI better understand how users communicate, their typical behavior, and textual patterns. This is crucial to preventing more advanced threats like spear phishing, which involves attackers attempting to impersonate high-profile individuals like company CEOs. AI can intercept suspicious activity to prevent a spear-phishing attack before it causes damage to corporate networks and systems.

3. Vulnerability management
As cyber criminals deploy more sophisticated methods and techniques, thousands of new vulnerabilities are discovered and reported every year. As a result, businesses struggle to manage the vast volume of new vulnerabilities they encounter every day, and their traditional systems cannot prevent these high-risk threats in real time.

AI-powered security solutions such as user and entity behavior analytics (UEBA) enable businesses to analyze the activity of devices, servers, and users, helping them identify anomalous or unusual behavior that could indicate a zero-day attack. AI in cybersecurity can protect businesses against vulnerabilities they are unaware of before they are officially reported and patched.

4. Network security
Network security involves the time-intensive processes of creating policies and understanding the network's topography. When policies are in place, organizations can enact processes for identifying legitimate connections versus those that may require inspection for potentially malicious behavior. These policies can also help organizations implement and enforce a zero-trust approach to security. [10,11,12]

However, creating and maintaining policies across multiple networks requires a significant amount of time and manual effort. Organizations often do not deploy the correct naming conventions for their applications and workloads. This means security teams may have to spend more time determining which workloads belong to specific applications. AI learns organizations' network traffic patterns over time, allowing it to recommend the right policies and workloads.

5. Behavioral analytics
With behavioral analytics, organizations can identify evolving threats and known vulnerabilities. Traditional security defenses rely on attack signatures and indicators of compromise (IOCs) to

discover threats. However, with the thousands of new attacks that cyber criminals launch every year, this approach is not practical.

Organizations can implement behavioral analytics to enhance their threat-hunting processes. It uses AI models to develop profiles of the applications deployed on their networks and process vast volumes of device and user data. Incoming data can then be analyzed against those profiles through AI-based anomaly detection to prevent potentially malicious activity.

Top AI-powered cybersecurity tools
Modern enterprise security demands tools that can operate at machine speed, process high volumes of threat data, and deliver actionable intelligence without overburdening security teams. AI-powered cybersecurity solutions meet this requirement by enhancing threat detection accuracy, automating incident response workflows, reducing false positive rates, and systematically strengthening an organization's overall security posture across every layer of the environment.

1. AI-powered endpoint security solutions
These solutions protect endpoints like laptops, desktops, and mobile devices from malware and ransomware. AI analyzes device behavior in real time and uses deep learning to catch zero-day threats before they execute.[13,14,15]

2. AI-based NGFW
AI-powered Next-Generation Firewalls (NGFWs) offer advanced threat protection, intrusion prevention, and application control. They perform deep-packet inspection and block both known and unknown threats before they reach critical systems.

3. Security information and event management (SIEM)
AI-powered SIEM solutions collect and analyze security data across the environment. They automate alert triage, cut through false positives, and help SOC teams respond to real threats faster.

4. AI-driven cloud security solutions
These solutions monitor cloud environments for misconfigurations, unauthorized app usage, and suspicious data flows. They provide consistent protection and compliance enforcement across multi-cloud deployments.

5. AI-powered NDR solutions for cyber threat detection
Network Detection and Response (NDR) solutions use AI to monitor network traffic and detect threats that bypass traditional tools. They identify lateral movement and suspicious activity, triggering automated responses before damage occurs.

How AI optimizes security operations in real time?

Winning the Mean-Time-to-Respond (MTTR) race

The Critical Benchmark: According to the FortiGuard Labs 2025 Cyberthreat Predictions report, newly discovered vulnerabilities are now being exploited at a record average of just 4.76 days—a 43% increase in speed compared to previous periods.

AI transforms security operations by automating threat detection, accelerating incident response, and reducing analyst workload. It continuously monitors network traffic, correlates events, and prioritizes alerts based on risk severity. AI-powered red teaming simulates real-world attacks to expose vulnerabilities before threat actors exploit them. Purple teaming builds on this by combining offensive insights with defensive systems, refining detection logic and response playbooks for a stronger, more proactive security posture.[16,17,18]

How can generative AI be used in cybersecurity?
Generative AI, known for its ability to create new data that resembles existing data, is a powerful tool for enhancing cybersecurity strategies and defenses.

Realistic simulations: Generative AI can create highly realistic simulations of cyberattacks, allowing security teams to test their defenses and incident response plans against a wide range of potential threats. This proactive approach helps identify vulnerabilities and improve preparedness before a real attack occurs.

Predicting attack scenarios: By analyzing vast datasets of past attacks and security incidents, generative AI can identify patterns and trends, enabling it to predict potential future attack scenarios. This predictive capability allows organizations to stay one step ahead of cybercriminals and proactively implement countermeasures.

Enhancing threat detection: Generative AI can augment threat detection & response systems by generating synthetic data that mimics real-world attack patterns. This expands the training data available for machine learning models, improving their ability to identify and flag even subtle or novel threats.

Generative AI acts as a powerful ally in the ongoing battle against cyber threats. By creating realistic simulations, predicting attack scenarios, and enhancing threat detection, it empowers cybersecurity professionals to proactively defend their organizations and stay ahead of the ever-evolving threats. Learn how generative AI security addresses emerging risks such as data leakage, prompt injection, and AI-powered attacks.

Benefits of artificial intelligence (AI) in managing cyber risks
Implementing AI in cybersecurity offers a wide range of benefits for organizations looking to manage their risk. Typical benefits are:

Ongoing learning: AI’s capabilities constantly improve as it learns from new data. Techniques like deep learning and ML enable AI to recognize patterns, establish a baseline of regular activity, and discover any unusual or suspicious activity that deviates from it. AI’s ability to learn on an ongoing basis makes it more difficult for hackers to circumvent an organization’s defenses.

Discovering unknown threats: As cyber criminals devise more sophisticated attack vectors, organizations are left vulnerable to unknown threats that could cause massive damage to networks. AI provides a solution for mapping and preventing unknown threats, including vulnerabilities that have yet to be identified or patched by software providers.
Vast data volumes: AI systems can handle and understand vast amounts of data that security professionals cannot. In this way, organizations can automatically discover new threats among vast amounts of data and network traffic that might go undetected by traditional systems.
Improved vulnerability management: In addition to discovering new threats, AI enables organizations to manage vulnerabilities better. It helps them assess their systems more effectively, improve problem-solving, and make better decisions. It can also identify weak points in networks and systems so that organizations are constantly focused on the most critical security tasks.
Enhanced overall security posture: Manually managing the risk of a range of threats, from denial-of-service (DoS) and phishing attacks to ransomware, can be difficult and time-consuming. But with AI, organizations are able to detect various types of attacks in real time and efficiently prioritize and prevent risks.
Better detection and response: Threat detection is a necessary element of data and network protection. AI-enabled cybersecurity can result in rapid detection of untrusted data and more systematic and immediate response to new threats.

RESULTS

5 key challenges and risks of AI in cybersecurity
Adversarial AI: Cybercriminals use AI to craft sophisticated attacks that evade detection. These adversarial techniques actively target and manipulate AI-powered security systems.
Data poisoning: Attackers can corrupt the data AI models train on. This compromises the model's ability to detect threats accurately over time.
Model bias: AI models trained on limited or skewed data can produce inaccurate results. This leads to missed threats or excessive false positives that burden security teams.
Over-reliance on automation: Automating too much without human oversight can be dangerous. AI can miss context that experienced analysts would catch, leaving critical gaps in defense.
Evolving AI-driven threats: Threat actors continuously adapt their methods to bypass AI defenses. Security models must be regularly updated to keep pace with these rapidly changing attack techniques. Learn how agentic AI security helps reduce risks tied to autonomous actions, prompt injection, and tool misuse. Explore how prompt injection attacks are emerging as a key AI security threat and the strategies to defend against them.[18,19,20]
7 best practices for implementing AI in cybersecurity
Use high-quality training data: AI is only as good as the data it learns from. Ensure training data is accurate, diverse, and regularly updated. Poor or biased data leads to missed threats and inaccurate detections that can put the entire security infrastructure at risk.
Maintain human oversight: AI should assist analysts, not replace them. Human review of AI-driven decisions ensures critical context is never missed. Experienced analysts bring judgment and intuition that automated systems cannot fully replicate.
Regularly update AI models: Cyber threats evolve constantly. AI models must be retrained and updated frequently to stay effective. Outdated models become easy targets for adversaries who understand how to exploit their limitations.

Ensure transparency and explainability: Security teams should understand how AI reaches its conclusions. Explainable AI builds analyst trust and makes it easier to validate, audit, and improve automated decisions over time.
Test AI systems continuously: Regular red teaming and adversarial testing identifies weaknesses in AI defenses before attackers can exploit them. Continuous testing ensures AI systems remain reliable as the threat landscape shifts.
Integrate AI across the security stack: AI delivers the most value when connected across endpoints, network, cloud, and security operations. Siloed deployments limit visibility and reduce the effectiveness of automated threat detection and response.
Establish clear governance policies: Define how AI is used, monitored, and audited within the organization. Clear governance ensures responsible adoption, maintains accountability, and helps organizations meet regulatory and compliance requirements. Learn how AI agent security helps address the new security considerations introduced as AI takes on more autonomous roles.
AI-driven defense for the future cybersecurity landscape
Cyber threats are constantly evolving, making strong security measures more critical than ever. AI-powered tools help security teams identify threats early, prevent breaches in real time, and protect organizations from financial and reputational damage.[19,20]

AI learns continuously from new data, making it essential for identifying the latest attack vectors and closing vulnerabilities faster than traditional methods. Enterprises must develop a clear AI adoption strategy to ensure effective integration into existing security operations. As organizations scale AI adoption, security frameworks must evolve alongside emerging threats while addressing governance challenges such as ethical oversight and regulatory compliance.

The key to leveraging the most of the technology is using the right AI-powered tools. That's where state-of-the-art cyber security tools like Fortinet's FortiAI stand out.

Fortinet's AI-driven solution, FortiAI, is designed to help security teams detect and respond to threats with precision and speed. This virtual security analyst utilizes machine learning to identify and classify threats in real-time, reducing the burden on security teams and enabling faster incident response.

Evolving, AI-driven threats demand intelligent defense - adopt AI-powered cybersecurity to stay ahead of breaches and risk. Transform cyber defense with Fortinet Generative AI security

CONCLUSIONS

In 2026, cyber threats have grown more relentless, more automated, and harder to outpace than ever before. AI in cybersecurity has moved from an experimental advantage to an operational necessity, forming the backbone of how organizations detect attacks, predict threats, and respond before damage spreads.

In the United States alone, cyberattacks target critical infrastructure, hospitals, financial institutions, and federal agencies daily. The organizations holding their ground share a common thread: they have integrated AI into the heart of their security operations.

At the same time, cybercriminals have not ignored AI. The same technology powering your defenses is being weaponized to craft more convincing phishing emails, build malware that

evades detection, and automate attacks at machine speed. This dual nature of AI, its capacity to both protect and threaten, defines the cybersecurity landscape of 2026.[20]

REFERENCES

1. Brynjolfsson, Erik; Mitchell, Tom (22 December 2017). "What can machine learning do? Workforce implications". Science. 358 (6370): 1530–1534. Bibcode:2017Sci...358.1530B. doi:10.1126/science.aap8062. PMID 29269459.
2. Shin, Minkyu; Kim, Jin; van Opheusden, Bas; Griffiths, Thomas L. (2023). "Superhuman artificial intelligence can improve human decision-making by increasing novelty". Proceedings of the National Academy of Sciences. 120 (12) e2214840120. arXiv:2303.07462. Bibcode:2023PNAS..12014840S. doi:10.1073/pnas.2214840120. PMC 10041097. PMID 36913582.
3. Chen, Yiting; Liu, Tracy Xiao; Shan, You; Zhong, Songfa (2023). "The emergence of economic rationality of GPT". Proceedings of the National Academy of Sciences. 120 (51) e2316205120. arXiv:2305.12763. Bibcode:2023PNAS..12016205C. doi:10.1073/pnas.2316205120. PMC 10740389. PMID 38085780.
4. "What is Generative AI? | IBM". www.ibm.com. 2024-03-22. Retrieved 2025-07-22.
5. Wilkinson, Lindsey (2023-11-22). "The rise of generative AI: A timeline of triumphs, hiccups and hype". www.ciodive.com. Retrieved 2026-07-14.
6. Robinson, Kristin (2026-03-17). "A Short History of AI-Generated Music: From 'Fake Drake' to Blockbuster Legal Settlements". Billboard. Retrieved 2026-07-14.
7. Gambhire, Akshaya; Shaikh Mohammad, Bilal N. (8 April 2020). Use of Artificial Intelligence in Agriculture. Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST) 2020. SSRN 3571733.
8. Jump up to: Briefer, Elodie F.; Sypherd, Ciara C.-R.; Linhart, Pavel; Leliveld, Lisette M. C.; Padilla de la Torre, Monica; Read, Eva R.; Guérin, Carole; Deiss, Véronique; Monestier, Chloé; Rasmussen, Jeppe H.; Špinka, Marek; Düpjan, Sandra; Boissy, Alain; Janczak, Andrew M.; Hillmann, Edna; Tallet, Céline (7 March 2022). "Classification of pig calls produced from birth to slaughter according to their emotional valence and context of production". Scientific Reports. 12 (1): 3409. Bibcode:2022NatSR..12.3409B. doi:10.1038/s41598-022-07174-8. PMC 8901661. PMID 35256620.
9. Moreno Millán, M; Sevilla Guzmán, E; Demyda, S E (2011). "Population, Poverty, Production, Food Security, Food Sovereignty, Biotechnology and Sustainable Development: Challenges for the XXI Century". Bulletin of University of Agricultural Sciences and Veterinary Medicine Cluj-Napoca. Veterinary Medicine. 1 (68).
10. Liundi, Nicholas; Darma, Aditya Wirya; Gunarso, Rivaldi; Warnars, Harco Leslie Hendric Spits (2019). "Improving Rice Productivity in Indonesia with Artificial Intelligence". 2019 7th International Conference on Cyber and IT Service Management (CITSM). pp. 1–5. doi:10.1109/CITSM47753.2019.8965385. ISBN 978-1-7281-2909-9.
11. Talaviya, Tanha; Shah, Dhara; Patel, Nivedita; Yagnik, Hiteshri; Shah, Manan (2020). "Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides". Artificial Intelligence in Agriculture. 4: 58–73. doi:10.1016/j.aiia.2020.04.002.
12. Bernstein, Phillip (2022). Machine Learning: Architecture in the Age of Artificial Intelligence. London: RIBA Publishing. ISBN 978-1-914124-01-3.
13. Heathcote, Edwin (2024-01-20). "AI is coming for architecture". Financial Times. Archived from the original on 2026-03-10. Retrieved 2026-07-27.

14. Matoso, Marília (2023-10-18). "Will Artificial Intelligence Replace Architects?". ArchDaily. Retrieved 2026-07-27.
15. Brynjolfsson, Erik; Li, Danielle; Raymond, Lindsey (2025-02-04). "Generative AI at Work". The Quarterly Journal of Economics. 140 (2): 889–942. doi:10.1093/qje/qjae044. ISSN 0033-5533. Archived from the original on 2025-06-05.
16. Noy, Shakked; Zhang, Whitney (2023-07-14). "Experimental evidence on the productivity effects of generative artificial intelligence". Science. 381 (6654): 187–192. Bibcode:2023Sci...381..187N. doi:10.1126/science.adh2586. PMID 37440646.
17. Estrada, Sheryl (18 August 2025). "MIT report: 95% of generative AI pilots at companies are failing". Fortune. Retrieved 15 October 2025.
18. Niederhoffer, Kate; Kellerman, Gabriella Rosen; Lee, Angela; Liebscher, Alex; Rapuano, Kristina; Hancock, Jeffrey T. (22 September 2025). "AI-Generated "Workslop" Is Destroying Productivity". Harvard Business Review. Retrieved 15 October 2025.
19. Griffith, Erin (2 April 2026). "How A.I. Helped One Man (and His Brother) Build a $1.8 Billion Company". The New York Times. Retrieved 6 April 2026.
20. Frąckowiak-Szymański, Przemysław (26 June 2025). "The Pros and Cons of Vibe Coding". Software Mind. Retrieved 7 November 2025.