Global Trends in Science and Technology

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

Artificial Intelligence in Cybersecurity: From Threat Detection to Autonomous Defense

Fnu Mohsin[1*]

[1]Washington University of science and technology

[1]mohsinashiq447@gmail.com

open access

Corresponding Author
Fnu Mohsin
mohsinashiq447@gmail.com

Article History:
Submitted: 01-10-2026
Accepted: 18-11-2026
Published: 22-11-2026

Key words

Artificial Intelligence, cybersecurity, machine learning, threat detection, malware detection, phishing detection.

Global Trends in Science and Technology is licensed under a Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

Cybersecurity is being revolutionized by Artificial Intelligence (AI), which provides the tools necessary for intelligent, adaptive, and automated solutions to detecting and responding to cyber threats. This review explores the use of AI in cybersecurity, covering the role and techniques of machine learning, detection of malware and phishing attacks, intrusion detection, intelligent security monitoring, anomaly detection, and automated incident response. Key challenges such as data quality, adversarial attack, false positive, privacy, ethics, and lack of model explain ability are also discussed. In addition, future directions towards autonomous and adaptive cyber defense are examined. AI has the power to enhance cybersecurity, but it must be used responsibly, monitored by humans, and continually improved.

INTRODUCTION

Digital technologies, cloud computing, Internet of Things (IoT) devices, mobile applications and interconnected networks have changed the world of today's society in many ways. But the growing reliance on digital infrastructure has also brought new opportunities for criminals [1]. Healthcare, financial, educational, government, manufacturing and other organizations are increasingly targeted by malware, ransom ware, phishing, denial-of-service, data breaches, insider threats, and advanced persistent threats. The traditional cybersecurity models that are primarily based on rules, signatures and manually configured security controls are often ineffective against emerging and new attacks that are fast evolving [2]. As a result, there is an increased demand for intelligent, adaptive, and automated cybersecurity solutions.

Artificial Intelligence (AI) is a promising technology that has the potential to address these challenges

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

by allowing computer systems to process vast amounts of security-related information, identify intricate patterns, and facilitate automated decision-making. There are multiple techniques involved in AI, such as machine learning, deep learning, natural language processing, and intelligent automation [3]. These methods can be used in cybersecurity for network traffic analysis, malware classification, intrusion detection, vulnerability assessment, user behavior analysis, fraud detection, and security incident response. The advantages of AI-based systems lie in their ability to learn from the past and current data, which can help them detect unusual activities that could signal malicious actions and even uncover potential threats that traditional security methods might miss [4].

A primary benefit of AI in cybersecurity is that it can handle vast amounts of constantly updated data at lightning speed. Security events, such as logs, network packets, authentication information, endpoint information, and more are created in huge volumes in modern organizations. This type of information is hard to come by manually, can be time consuming, and may lead to slow threat detection [5]. AI can help security teams to automatically sift through all these data sources, flagging suspicious events and ensuring quicker responses based on insights. AI-based systems can play a role in an autonomous defense by autonomously identifying threats and automatically triggering preconfigured responses, isolating affected systems and adapting to new attack patterns [6].

While the possibilities are great, the assimilation of AI into cybersecurity also poses considerable problems. Adversarial attacks, poisoned training data, model evasion techniques, and more are ways in which cyber attackers can manipulate AI systems. Adopting AI-powered security solutions is further complicated by concerns about data privacy, model transparency, false positives, computational needs, and ethical decision-making [7]. Additionally, attackers can leverage AI to automate and intensify attacks, establishing a technological arms race between defenders and attackers.

When exploring the role of AI in cyber security, you need to take into account what it can do—and can't do as well. This review highlights the evolution of AI-powered cybersecurity solutions from threat detection to automated and autonomous cyber defense. It also explores significant applications, challenges, ethical considerations, and new research avenues, offering a broad overview of the potential impact of AI on the future of cybersecurity.

AI AND MACHINE LEARNING TECHNIQUES FOR CYBER THREAT DETECTION

Cyber-attacks are becoming more complex and more numerous; thus, there is a great need for intelligent techniques that are able to identify cyber-attacks fast and accurately. Artificial Intelligence (AI) is now playing a significant role in the field of cyber threat detection, with Machine Learning (ML) being a key technology [8]. Machine learning approaches can learn patterns from historical data

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

and real-time data, whereas conventional security mechanisms are mainly rule-based and on the basis of known patterns of attacks. This functionality can be used to detect unusual behavior, and even to recognize new or emerging threats that haven't been previously encountered by AI systems [9].

In Cybersecurity, machine learning techniques can be broadly classified into three categories: Supervised Learning, Unsupervised Learning, and Reinforcement Learning. In supervised learning algorithms, training examples are provided that consist of examples of legitimate and malicious activity [10]. Popular methods used are decision trees, random forest, support vector machines, logistic regression, and artificial neural networks. These models can be used for network traffic classification, malicious file detection, phishing detection, and the identification of normal activities from known attack patterns [11]. However, they are highly dependent on the quality, diversity and representativeness of the training data.

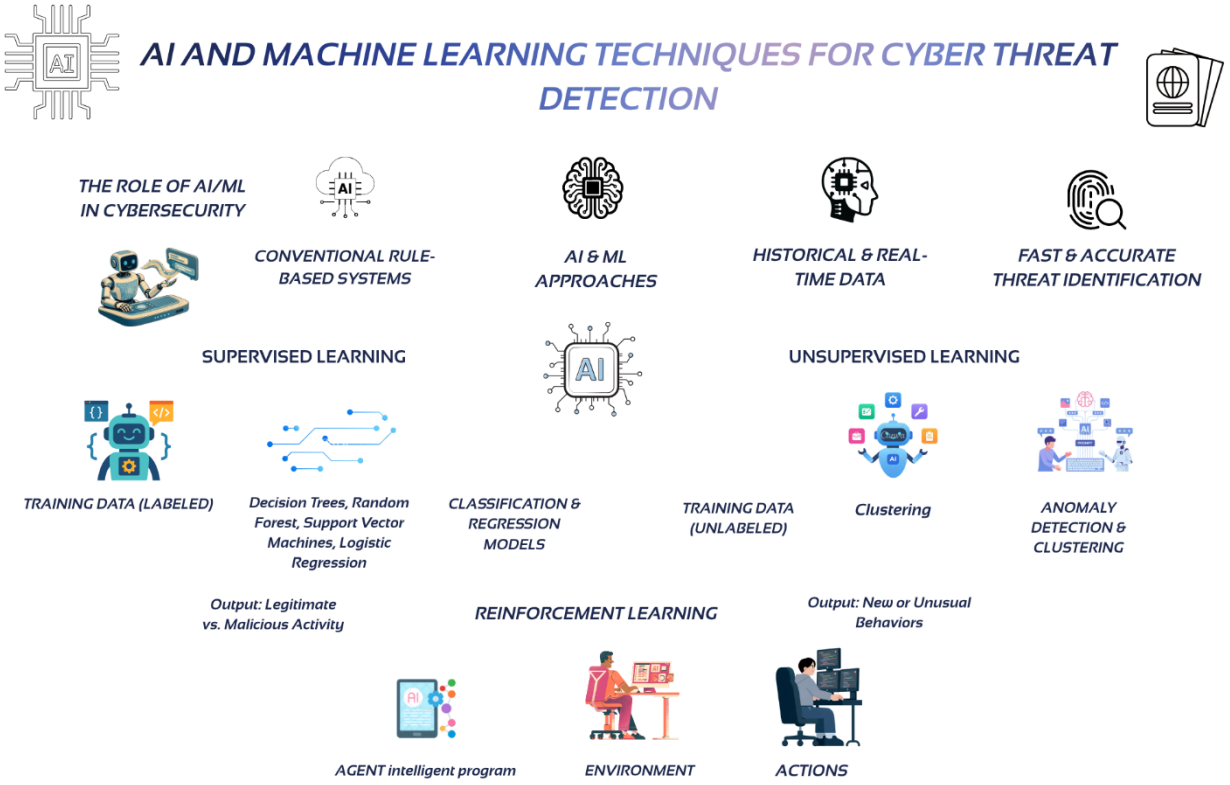


Figure 1. AI and Machine Learning Techniques for Cyber Threat Detection

Unsupervised learning is a type of learning that doesn't need any labels and it is very helpful in discovering new or unusual behaviors. Algorithms such as clustering, dimensionality reduction, and anomaly detection can be used to analyze large datasets and identify any patterns or anomalies that may indicate some form of abnormal activity [12]. An unsupervised system, for instance, can recognize odd network connections, unexpected logins, or irregular data exchanges that might signify that a cyber-attack is currently happening. This is especially useful in cases where new threats arise

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

more rapidly than the signatures security teams can write for them, making unsupervised learning valuable [13].

AI for threat detection has also been enhanced by a specialized subset of machine learning known as Deep Learning (DL). The neural networks, convolutional neural networks, recurrent neural networks, and transformer-based architectures can handle intricate cybersecurity data, such as network traffic, system logs, executable files, and textual information [14]. These models can automatically learn high-level representations from large sets of data, without requiring much manual feature engineering.

INTRUSION DETECTION AND PHISHING DETECTION

Cybercrime has grown at a tremendous pace and malware, phishing attacks and network attacks are being developed on a regular basis. Standard cybersecurity solutions rely mainly on patterns and rules to pinpoint malicious activity. These techniques are still very effective at identifying known threats, but may not be as effective at detecting new, more modified or more sophisticated attacks [15]. Alternative approaches involve the use of Artificial Intelligence (AI) and Machine Learning (ML), which enable security systems to effectively process vast amounts of data, recognize complex patterns, and recognize suspicious activities with adaptability [16]. The use of artificial intelligence (AI) for malware detection, identification of phishing attacks, and intrusion detection is growing and growing.

AI in cybersecurity has numerous use cases, with one prominent application being the detection of malware. Malware: These are viruses, worms, trojans, spyware, ransom ware and other malicious programs that can be used to gain control of a computer network or to steal information. Traditional signature based anti-virus solutions typically scan files for signatures that have been defined in the past [17]. These systems can be complemented with AI-powered techniques that can classify attributes and actions of suspicious or unwanted programs. Machine learning models can be trained to detect if a software application is malicious or not by analyzing their executable files, system calls, API interactions, memory behaviors, and network communication [18]. With deep learning, more intricate relationships within large datasets can be discerned, and previously unknown variants of malware can be detected.

AI can also play a crucial role in phishing detection. Phishing attacks try to trick users into disclosing personal information such as a password, financial data, or authentication credentials, via fake email, web sites, messages, or social engineering. AI systems can detect suspicious emails based on the content of the emails, URLs, characteristics of the domain, structure of the website, information about the sender and linguistic patterns [19]. Natural Language Processing (NLP) can be especially effective

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

in analyzing the linguistic features of phishing emails and identifying whether they are a phishing attack or not. Machine learning algorithms are also able to identify suspicious domain names, dubious links and other signs of malicious sites [20].

Another significant use of AI-powered cybersecurity is the intrusion detection system (IDS). IDS solutions watch network traffic, devices, and system activities for any unauthorized access or potentially harmful activities. Anomaly detection is one of the capabilities that AI-powered IDS can use to create a "normal" profile of network activity and flag any large deviations from it [21]. Supervised learning can be used to recognize known attack types and unsupervised learning can be used to detect previously unseen attacks. The Deep learning models can handle high dimensional network data and identify complex attack patterns that may be challenging to identify using traditional rule-based methods [22].

While these benefits exist, there are limitations in AI-based malware, phishing, and intrusion detection systems like false positives, dataset imbalance, limited training data, adversarial attacks, and constantly evolving threat patterns. Malicious attackers can specifically change the attack patterns or malicious code to outsmart AI models [23]. Thus, a continuous training of the model, high-quality datasets, explainable AI and human supervision are crucial to maintaining reliable detection. In summary, AI offers a robust base to enhance cybersecurity capabilities, making these tools faster, more scalable and more adaptable when it comes to detecting malware, phishing and intrusion attempts [24].

DATA ANALYSIS, REPORTING AND SEARCHING FOR INSIDER THREAT

As digital systems, cloud services, connected devices, and computer networks become more integral to organizations, ongoing security monitoring has become a critical business need. Today, there are many modern information systems creating voluminous data such as network traffic, authentication logs, system logs, application events, and user activity. It is hard, time-consuming and easily prone to human error to analyze this information manually [25]. Traditional security monitoring methods are rule or signature based and can work well when there are known threats, but might not be effective in detecting new or more advanced attacks. AI and ML provide intelligent solutions by automatically analyzing a large volume of information and detecting unusual patterns that can signify potential cybersecurity threats [26].

Anomaly detection is a crucial aspect of AI's role in cybersecurity. It is a process of noticing activities that deviate from normal or expected activities. An unusual login from an unfamiliar location, an unexpected surge in network traffic, accessing sensitive files or data without proper authorization, or unusual data transmission, for instance, may be signs of potential malicious activity [27]. AI-based

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

systems can create a baseline of normal behavior, and continually compare new activities to this baseline. If there are major deviations, alerts can be sent to security analysts. This ability is crucial when it comes to detecting new or changing attacks [28].

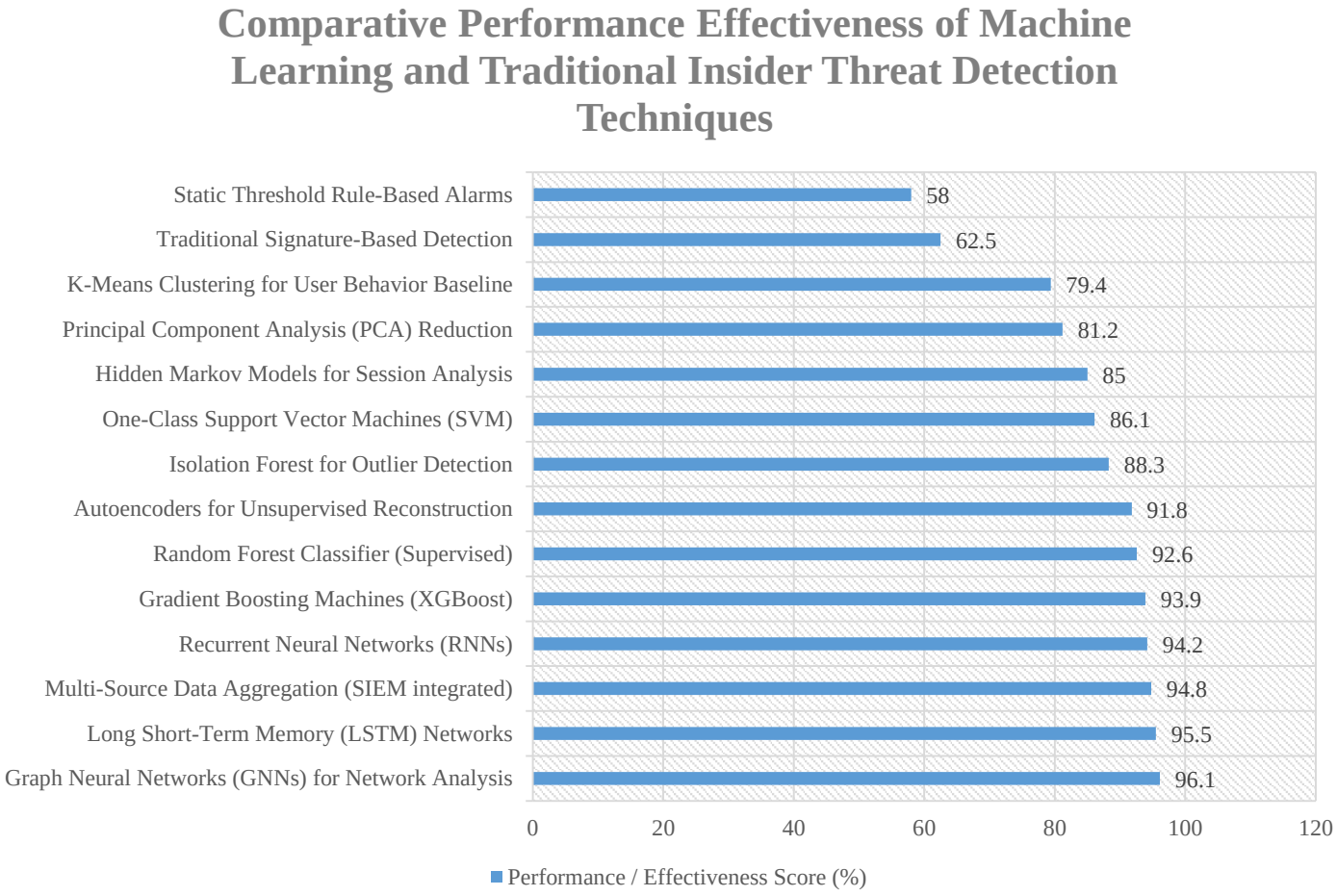


Figure 2. Comparative Performance Effectiveness of Machine Learning and Traditional Insider Threat Detection Techniques

There are various types of machine learning algorithms that can be used in intelligent anomaly detection. Unsupervised learning techniques are capable of identifying concealed patterns in the data sets without the need for a large amount of labeled attack data. Similarities in activities can be captured through clustering techniques and observations far from the normal pattern can be found using outlier detection techniques [29]. More complex cybersecurity data, such as a system's normal behaviors, can be captured by deep learning models like autoencoders or recurrent neural networks and then learned in detail. These can enhance the capability of security systems to detect subtle changes that traditional rule-based systems might not detect [30].

In addition, AI can enhance security monitoring by aggregating data from various security sources. Firewalls, intrusion detection systems, endpoint devices, servers, cloud platforms and security

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

information and event management systems can all combine their data for analysis. This enables AI systems to uncover connections between unrelated occurrences [31]. For example, multiple failed login attempts followed by data access patterns that involve accessing files in unusual ways and transferring large amounts of data could be a coordinated security incident and not a series of unrelated activities [32].

AUTOMATED INCIDENT RESPONSE AND CYBER DEFENSE WITH AI

Rapid incident response is a key element of modern-day cybersecurity as attacks are becoming more sophisticated, frequent and fast. Human security analysts, who manually review alerts, must determine where an attack is coming from, its level of severity, and take the necessary defense actions, are a significant part of the traditional incident response process [33]. While manual response is still necessary, the sheer volume of alerts in modern digital environments can render it cumbersome and time-consuming, especially when dealing with its complexity. While human expertise is essential, digital environments generate so many security alerts that manually responding to them can be time-consuming and inefficient, particularly when dealing with the complexity of the digital environment [34]. With the help of Artificial Intelligence (AI), one can automate some aspects of incident response and build quicker, smarter, and more adaptive cyber defense.

AI Incident Response is the use of machine learning, deep learning, natural language processing (NLP), and automated decision-making to identify, analyze, prioritize, and respond to cybersecurity incidents. Once the potential threat has been identified, AI systems can analyze the logs, network traffic, user activity, and endpoint activity to decide if the event is a real security incident [35]. AI can analyze data from various sources, identify patterns, and provide a clearer understanding of the extent and severity of an attack, aiding security teams in their response [36]. This can shorten investigative time and give investigators time to concentrate on high-risk incidents.

Automated cyber defense augments those capabilities, enabling security systems to take a preprogrammed or intelligent response with little or no human involvement. For instance, an AI-based system can automatically isolate a compromised endpoint, block an insecure network connection, disable a compromised account, or deny access to malicious files [37]. These can minimize the time between threat detection and containment, especially in fast evolving attacks. For organizations dealing with a large-scale incident, automation can assist with responding to the situation before security staff gets in touch [38].

AI can also benefit Security Orchestration, Automation and Response (SOAR) environments by orchestrating security tools and automating repetitive tasks. AI can prioritize alerts based on their risk while automatically triggering response actions, rather than analysts having to manually review each

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

alert. Natural Language Processing can also help in the analysis of threat intelligence reports, security notifications and incident descriptions to enable organizations to extract relevant information more efficiently [39]. Even with its benefits, autonomous cyber defense is not without its challenges. Badly made automated decisions can interfere with legitimate users or systems, as well as false positives and inaccurate models can miss complex attacks. Adversarial attacks or disguising input into AI systems could also be used to attack AI [40]. Thus, the role of human oversight, explainable AI, well-defined response policies, and on-going system assessment are still relevant.

AI-powered incident response and automated cyber defense are significant steps away from traditional reactive cybersecurity and are moving toward proactive and more autonomous defense strategies. AI can enhance the effectiveness and speed of the modern cybersecurity workflow by making swift decisions, instantly analyzing threats, and reacting to security events coordinately [41].

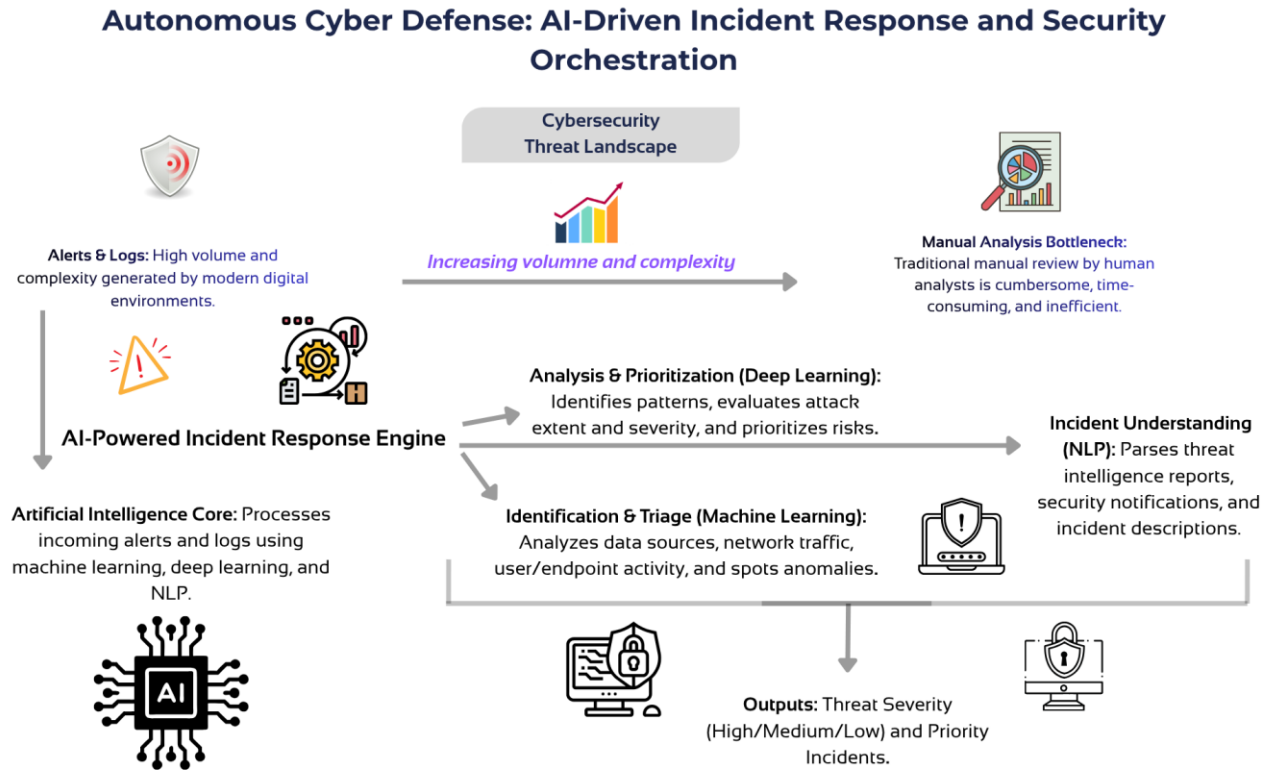


Figure 3. Autonomous Cyber Defense: AI-Driven Incident Response and Security Orchestration

ISSUES, LIMITATIONS AND ETHICAL CONCERNS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

While Artificial Intelligence (AI) has shown great promise in enhancing cybersecurity, there are also challenges technical, operational, and ethical to overcome. Large volumes of quality data are essential for training and decision-making in AI-driven cybersecurity solutions. Some cybersecurity datasets, however, are incomplete, imbalanced, outdated, or inaccessible; that is, organizations may not want

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

to share their sensitive security information [42]. Sub-par training data can lead to lower model accuracy and more false positives and false negatives. As a result, AI tools for cybersecurity are highly dependent on the quality and variety of the data that powers them [43].

One of the other drawbacks is the susceptibility of AI models to adversarial attacks. The adversary can knowingly alter the input to the machine learning system, or cause it to misclassify the malicious behavior as legitimate. Adversarial techniques can include slight changes in network traffic, malware traits, or other security-related information. The other issue of concern is data poisoning, where an attacker tries to manipulate the training set with inaccurate or dubious data [44]. These risks are clear indicators that AI systems can be targets in the cybersecurity landscape.

Lack of transparency and explain ability is also a big issue. There are also some advanced AI models, such as deep learning, which are essentially "black boxes" (or "black art") and difficult to understand how a specific AI decision was made. In critical situations, where accountability and trust in decision making is important, unaccounted actions can lead to issues [45]. Security analysts should know what to do before potentially disruptive actions, as well as why the AI system has believed an activity is malicious. Explainable Artificial Intelligence (XAI) can thus be of significant value to improve transparency and aid human decision-making [46].

Ethics and privacy issues need to be taken into account as well. Cybersecurity systems that rely on artificial intelligence can be used to manage sensitive data, such as user behavior, interactions, login information, and network activity. Too much, or inappropriate, monitoring or use of this information can pose a privacy threat. Organizations need to create proper data protection policies, and ensure that the implementation of AI systems is carried out responsibly in compliance with regulations and ethics [47].

Moreover, AI can be also applied in a malicious way, such as in automated phishing attacks, social engineering, creating malware, discovering vulnerabilities, and bypassing security measures. This results in an everlasting technological rivalry between security and attack. Other challenges include the high implementation costs, lack of skilled professionals, computational needs, model bias, and the challenge of maintaining AI systems as threats continuously change [48]. These challenges call for a combination of AI powers and human expertise, data governance, frequent model testing, techniques that are explainable, privacy protection, and effective security measures, all in a balanced manner. AI should thus be considered a useful tool rather than a full replacement for cybersecurity experts, and help them better meet the growing challenges of new threats [49].

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Trends in Science and Technology
ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

FUTURE DIRECTIONS: TOWARDS AUTONOMOUS AND ADAPTIVE CYBERSECURITY

Artificial Intelligence (AI) is likely to play an even greater role in the future of cybersecurity, with the creation of autonomous and adaptive defenses. Traditional security methods might not be as effective against a threat which constantly adapts its tactics and methods. Looking forward, AI-powered cybersecurity solutions should not just detect threats, but continuously adapt, make decisions, and proactively respond [50].

An upcoming field is the progress of independent cybersecurity frameworks that can recognize, assess and respond to dangers with minimum human engagement. These systems could be monitoring networks at all times, alerting to suspicious behavior, determining potential threats and automatically take defensive measures [51]. This can substantially shorten response times and improve managing of the massive amount of security incidents. But the human element will still be needed, especially in making decisions with high risk that can have an impact on critical systems or sensitive information [52].

Another promising course is adaptive AI. Future models for cybersecurity could be constantly learning from new patterns in attacks, as well as continuously evolving network conditions, without the use of static training sets. A reinforcement learning and other continual-learning techniques might allow security systems to learn from past experience to enhance their defensive strategy [53]. This flexibility could be very useful in identifying zero-day attacks or new forms of attack not seen before.

CONCLUSION

Artificial Intelligence (AI) is a technology that has revolutionized the cybersecurity landscape and has opened up new possibilities for detecting, analyzing, and responding to the growing complexity of cyber threats. The proliferation of digital infrastructure, networked systems, cloud computing, and IoT devices has added more and more security events that companies are struggling to manage. In such a setting, traditional cyber-security tools, which are mainly rule/signature based, may lack the ability to detect unknown and evolving attacks. More adaptive solutions are provided by AI and Machine Learning (ML): AI systems can learn from data to improve their security functions, detect complex patterns, and assist in quicker security decision-making.

This review has shed light on the critical use of AI in several pivotal domains of cybersecurity. An AI threat detection system can be used to analyze a large amount of network and system data and detect suspicious activity and potential attacks. Patterns and behaviors can also be identified using machine learning and deep learning methods, aiding in the identification of malware, phishing attempts, and network intrusions. These methods can be valuable in detecting emerging and unknown threats, with

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

the aid of intelligent security monitoring and anomaly detection. Moreover, AI-powered incident response can automate repetitive security tasks, prioritize alerts, and facilitate the quick containment of cyber incidents. These capabilities highlight AI's potential to enhance the speed, scale and efficiency of cyber security operations.

While these advantages are there, there are significant challenges to adopting AI in cybersecurity. Accurate, diverse, and representative datasets are critical for the effectiveness of AI models. AI systems can be unreliable due to false positive, false negative errors as well as changing attack patterns, computation requirements, and lack of model interpretability. In addition, cyber attackers can take advantage of vulnerabilities in AI with adversarial attacks, data poisoning, and other forms of manipulation. Additionally, privacy and ethical considerations must be taken into account, as AI-driven security systems can handle sensitive data related to users, devices, and organizational operations. These challenges serve as a reminder that AI is not foolproof, and that there should be appropriate safeguards in place.

The integration of AI-driven automation and human intelligence is expected to result in more adaptive and intelligent cybersecurity systems in the future. In the future, autonomous systems could be able to monitor environments all the time, detect threats and take action to defend in real time. But human supervision, explainable AI, robust data governance, ongoing model monitoring and responsible security measures will continue to be crucial. Research should therefore aim at creating strong and transparent AI technologies with privacy protection and adversarial resistance.

AI has the potential to significantly reshape cybersecurity by moving defense strategies from reactive protection toward proactive, adaptive, and increasingly autonomous defense. The successful deployment of this will require not only technological advances, but a responsible approach, as well as human-AI collaboration and ongoing research. As AI evolves and overcomes these current challenges and ethical issues, it holds the promise of being a valuable part of future cybersecurity strategies and enhancing security against the constantly changing nature of cyber threats.

REFERENCES

[1]. Ozkan-Okay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, Beloev I. A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access. 2024 Jan 18; 12:12229-56.

[2]. Manoharan A, Sarker M. Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: https://www. doi. org/10.56726/IRJMETS32644. 2023; 1.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

[3]. Mohammed A. Artificial Intelligence-Driven Cybersecurity Crimes: Emerging Threats, AI Bots, and Advanced Defense Strategies. Euro Vantage journals of Artificial intelligence (EVJAI). 2026 Mar 13; 3(1):46-65.

[4]. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems. 2025 Aug; 67(8):6969-7055.

[5]. Oloyede J. Leveraging artificial intelligence for advanced cybersecurity threat detection and prevention. Available at SSRN 4976072. 2024 Oct 3.

[6]. Basu A. The impact of artificial intelligence on cybersecurity. InAbu Dhabi International Petroleum Exhibition and Conference 2024 Nov 4 (p. D021S077R001). SPE.

[7]. Khan F. Advances in Artificial Intelligence for Electrical Systems: Machine Learning Methods, Applications, and Emerging Challenges. American Journal of Artificial Intelligence and Computing. 2026 Aug 12;2(2):1-9.

[8]. Hernández-Rivas A, Morales-Rocha V, Sánchez-Solís JP. Towards autonomous cybersecurity: A comparative analysis of agnostic and hybrid AI approaches for advanced persistent threat detection. InInnovative applications of artificial neural networks to data analytics and signal processing 2024 Dec 3 (pp. 181-219). Cham: Springer Nature Switzerland.

[9]. Onur F, Gönen S, Barışkan MA, Kubat C, Tunay M, Yılmaz EN. Machine learning-based identification of cybersecurity threats affecting autonomous vehicle systems. Computers & Industrial Engineering. 2024 Apr 1; 190:110088.

[10]. Sewak M, Sahay SK, Rathore H. Deep reinforcement learning in the advanced cybersecurity threat detection and protection. Information Systems Frontiers. 2023 Apr; 25(2):589-611.

[11]. Khan F. Deep Learning Applications in Power Systems: A Review Study. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[12]. Malik A, Arshid K, Noonari N, Munir R. Artificial intelligence-driven cybersecurity framework using machine learning for advanced threat detection and prevention. Scholars Journal of Engineering and Technology. 2025; 13(06):401-23.

[13]. Kaneti VR, Jayasutha D, Yamini B, Dinesh MG, Gracious LA, Girija P. Leveraging Artificial Intelligence for Advanced Threat Detection and Autonomous Response in Cybersecurity. InImplementing Enterprise Cybersecurity with AI 2026 (pp. 135-160). IGI Global Scientific Publishing.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

[14]. Dalal A. Cybersecurity and artificial intelligence: How ai is being used in cybersecurity to improve detection and response to cyber threats. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2018 Nov 20; 9(3):10-61841.

[15]. Khan F. Artificial Intelligence in Electrical Power Systems: A Comprehensive Review of Machine Learning Techniques and Applications. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[16]. Raji A, Olawore A, Mustapha A, Joseph J. Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. World Journal of Advanced Research and Reviews. 2023 Dec; 20(3):2005-24.

[17]. Al-Rubaye RH, Türkben AK. Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks. Babylonian Journal of Networking. 2024 Apr 30; 2024:45-56.

[18]. Banik S, Dandyala SS. The role of artificial intelligence in cybersecurity opportunities and threats. International Journal of Advanced Engineering Technologies and Innovations. 2023; 1(04):420-40.

[19]. Djenna A, Bouridane A, Rubab S, Marou IM. Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry. 2023 Mar 8; 15(3):677.

[20]. Dhanushkodi K, Thejas S. Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE access. 2024 Nov 8; 12:173127-36.

[21]. Truong TC, Zelinka I, Plucar J, Čandík M, Šulc V. Artificial intelligence and cybersecurity: Past, presence, and future. InArtificial intelligence and evolutionary computations in engineering systems 2020 Feb 9 (pp. 351-363). Singapore: Springer Singapore.

[22]. Akpabio E, Narad S. Artificial intelligence and cybersecurity: challenges, opportunities, and defensive. ICT Systems and Sustainability: Proceedings of ICT4SD 2024, Volume 6. 2025 Mar 26; 6:291.

[23]. Shukla PK, Raghuvanshi CS, Sharan HO. AI-Enhanced Cybersecurity: Leveraging Artificial Intelligence for Threat Detection and Mitigation. Journal of Computational Analysis & Applications. 2024 Dec 15; 33(8).

[24]. Abbasi N, Nizamullah FN, Zeb S, Fahad M, Qayyum MU. Machine learning models for predicting susceptibility to infectious diseases based on microbiome profiles. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Aug 25;3(4):35-47.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

[25]. Chirra BR. Revolutionizing Cybersecurity: The Role of AI in Advanced Threat Detection Systems. International Journal of Advanced Engineering Technologies and Innovations. 2024; 4(1):480-504.

[26]. Muheidat F, Mallouh MA, Al-Saleh O, Al-Khasawneh O, Tawalbeh LA. Applying AI and machine learning to enhance automated cybersecurity and network threat identification. Procedia Computer Science. 2024 Jan 1; 251:287-94.

[27]. Malhotra L, Bhushan B, Singh RV. Artificial intelligence and deep learning-based solutions to enhance cyber security. InProceedings of the international conference on innovative computing & communication (ICICC) 2021 Apr 24.

[28]. Dalal A. Leveraging artificial intelligence to improve cybersecurity defences against sophisticated cyber threats. Available at SSRN 5422354. 2020 Feb 16.

[29]. Oad SK. Artificial Intelligence in Data Science: A Comprehensive Review. American Journal of Artificial Intelligence and Computing. 2026 Mar 17;2(1):1-25.

[30]. Baltabek A, Pogorelov V, Razaque A, Kalpeyeva Z. Artificial Intelligence for Cybersecurity: Enhancing Threat Detection and Response. Computing & Engineering. 2024 Dec 31; 2(4):14-21.

[31]. Akpabio E, Narad S. Artificial Intelligence and Cybersecurity: Challenges, Opportunities, and Defensive Techniques. InInternational Conference on ICT for Sustainable Development 2024 Aug 8 (pp. 291-302). Singapore: Springer Nature Singapore.

[32]. Aslam MS, Jamal M. Machine Learning in Healthcare: Revolutionizing Clinical Decision-Making with Data Analytics. Global Trends in Science and Technology. 2026 Mar 18;2(2):23-42.

[33]. Khan OU, Abdullah SM, Olajide AO, Sani AI, Faisal SM, Ogunola AA, Lee MD. The Future of Cybersecurity: Leveraging Artificial Intelligence to Combat Evolving Threats and Enhance Digital Defense Strategies. Journal of Computational Analysis & Applications. 2024 Dec 15; 33(8).

[34]. Santoso F, Finn A. An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. IEEE Transactions on Services Computing. 2023 Nov 8; 17(3):1293-310.

[35]. Timothy MJ, Rajasekharam B, Ampolu KV, Mogili U. Threat detection using AI in cybersecurity systems. Int. J. Inf. Secur.(IJIS). 2023; 7(1):1-7.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

[36]. Mughaid A, AlZu'bi S, Hnaif A, Taamneh S, Alnajjar A, Elsoud EA. An intelligent cyber security phishing detection system using deep learning techniques. Cluster Computing. 2022 Dec; 25(6):3819-28.

[37]. Sinha AR, Singla K, Victor TM, Kumar R, Pattnaik PK. Artificial intelligence and machine learning for cybersecurity applications and challenges. Risk detection and cyber security for the success of contemporary computing. 2023 Nov 9:109-46.

[38]. Adeyemi DS. Autonomous response systems in cybersecurity: A systematic review of AI-driven automation tools. Communication in Physical Sciences. 2023 Sep 19; 9(4):878-98.

[39]. Arora A. Transforming cybersecurity threat detection and prevention systems using artificial intelligence. Available at SSRN 5268166. 2025 May 23.

[40]. Czaja P, Gdowski B, Niemiec M, Mees W, Stoianov N, Votis K, Kharchenko V, Katos V, Merialdo M. Cybersecurity challenges and opportunities of machine learning-based artificial intelligence. Neural Computing and Applications. 2025 Nov; 37(33):27931-56.

[41]. Kabeer MM. Utilizing Machine Learning for Continuous Process Improvement in Lean Six Sigma. Global Trends in Science and Technology. 2025 May 7;1(2):49-63.

[42]. Katnapally N, Murthy L, Sakuru M. Automating cyber threat response using agentic AI and reinforcement learning techniques. J. Electrical Systems. 2021 Jan; 17(4):138-48.

[43]. Naqvi SG, Sheraz S, Mehmood I, Yasin M. Cyber-physical systems and artificial intelligence: the role of cyber security, machine learning, threats and benefits to modern economies and industries. Pakistan Journal of Humanities and Social Sciences. 2023 Jun 19; 11(2):1475-84.

[44]. Erdenetsogt T, Jamal M. Machine Learning for Big Data Analytics: A Comprehensive Review. Global Trends in Science and Technology. 2026 Apr 25;2(2):199-218.

[45]. Dehghantanha A, Yazdinejad A, Parizi RM. Autonomous cybersecurity: Evolving challenges, emerging opportunities, and future research trajectories. InProceedings of the workshop on autonomous cybersecurity 2023 Nov 6 (pp. 1-10).

[46]. Moamin, S.A., Abdulhameed, M.K., Al-Amri, R.M., Radhi, A.D., Naser, R.K. and Pheng, L.G., 2025. Artificial intelligence in malware and network intrusion detection: a comprehensive survey of techniques, datasets, challenges, and future directions. *Babylonian Journal of Artificial Intelligence*, *2025*, pp.77-98.

[47]. Edmund E, Enemosah A. AI and machine learning in cybersecurity: Leveraging AI to predict, detect, and respond to threats more efficiently. International Journal of Science and Research Archive. 2024; 11(01):2625-45.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.92-107

[48]. Ali R, Ali A, Iqbal F, Khattak AM, Aleem S. A systematic review of artificial intelligence and machine learning techniques for cyber security. InInternational Conference on Big Data and Security 2019 Dec 20 (pp. 584-593). Singapore: Springer Singapore.

[49]. Raza H, Singh A, Erdenetsogt T, Kabeer MM, Aslam MS, Farooq M. Machine Learning Driven Decision Making in the Modern Data Era. PERFECT: Journal of Smart Algorithms. 2026 Jan 6;3(1):11-22.

[50]. Bali P. Artificial intelligence: A boon or threat for cyberspace security. International Journal of Engineering, Science and Mathematics. 2018 Apr; 7(4):549-60.

[51]. Riza AZ, Jennsen L, Anggani P, Rafeen AI, Ruth PN, Sookun D, Sookun V, Yusri NA, Sern LJ, Luximon L, Omer ML. Leveraging Machine Learning and AI to Combat Modern Cyber Threats.

[52]. Mohammed A. AI and Machine Learning in Cybersecurity: Strategies, Threats, and Exploits. Innovative Computer Science Journal. 2023 Mar 16.

[53]. Merlano C. Enhancing cyber security through artificial intelligence and machine learning: A literature review. Journal of Cybersecurity. 2024; 6:89.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.