IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131263

AI-Generated Cyber Threats the Rise of Autonomous Hacking Systems

Jayasudha Yedalla

Colorado Technical University, Colorado, USA

Abstract: In today's technological landscape, artificial intelligence (AI) has become prominent in various fields, including cyber security. While AI has strengthened security measures and protected networks, hackers increasingly target AI-generated cyber threats and autonomous hacking systems. This shift has made it more challenging for traditional defences to remain effective, as attackers utilize AI to launch and execute cyber-attacks and identify vulnerabilities to exploit. This work aims to describe how AI has evolved in the context of cyber threats and what types of hacking an AI system can perform autonomously while exploring the potential of AI in cyber security. Additionally, it analyses the ethical dimensions surrounding AI as a double-edged tool and examines some defence strategies that can be implemented against AI-driven attacks. Cyber security professionals are better positioned to develop systems to combat autonomous hacking by understanding the current risks and potential mitigation measures.

INTRODUCTION

Artificial intelligence in cyber security has been a double-edged sword, improving security while posing a threat to the entire system. Cognitive cyber threats represent a significant advancement over routine and iterative threats. They employ artificial intelligence, automation, deep learning, and natural language processing to carry out attacks almost independently. These systems perform reconnaissance and vulnerability assessments, develop malware, and select attack techniques autonomously and automatically.

Initially, the threats were exclusively computer concerns, meaning that the attacks on the systems, vulnerabilities needed someone to type them manually. Nevertheless, new tools have emerged through Artificial Intelligence making hacking easy, faster and even smarter thereby increasing the daily threats in the cyber world. AI is used in cyber warfare in various ways, such as in deep fake technology, AI-generated phishing campaigns, and botnets for exploiting the discovered vulnerability. The usage of the generative AI models fuels this trend even more as hackers are now capable of developing invisible viruses and modulating virtual spaces.

This paper examines the future of AI-created threats. It highlights the general concept of autonomous hacking systems, their functioning, their impact on cyber security, and the difficulties of protecting against such threats. It also discusses current and emerging countermeasures that may contain AI attacks, such as AI-secured cyber security, ethical standards for managing AI, and legislation proposed for AI cyber threats. Understanding the changing AI threats scenario is essential in designing a security strategy and protecting future attacks on digital structures.

AI's contribution to Cyber security: Enriching guards against Attacks Rather than introducing more dangers

Machine learning in cyber security has broadened its capabilities with the internet and networking systems to help in automation, analysis, and decision making. AI powers security defences by identifying anomalies and threats in real time and reacting autonomously (Sarker, 2024, p.S3). However, these same advancements have also introduced AI or generative AI cyber threats in which the attackers use machine learning AI to advance the hacking techniques (Usman et al., 2024)[2]. As has been mentioned, autonomous hacking systems are effective in evading conventional security solutions in addition to being able to act more flexibly and be capable of carrying out a massive attack with little to no interference from a human being (Kaloudi & Li, 2020)[3]. Despite this, several AI-based cyber security solutions have been developed to mitigate these threats. At the same time, the fact that artificial intelligence has both military and civilian applications is part of the problem. These threats require constant research and development regarding offense and defense (Heckel & Weller, 2024)[4].

2. THE SHIFT FROM HUMAN-DRIVEN CYBER-ATTACKS TO AI-POWERED AUTOMATION

What was once done manually, reconnaissance, exploitation, and attack launching, were skills and knowledge that would be provided solely by a human expert. Nevertheless, with the emergence of new waves in Artificial Intelligence (AI), it is now possible for hackers to set up the bot and allow it to launch the attack with little human intervention (Valencia,

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024
DOI: 10.17148/IJARCCE.2024.131263

2024)[5]. AI-based cyber threats are based on deep learning methods and determine the systems' weaknesses that must be attacked in search of the most effective and fastest way to intrude (Andreoni et al., 2024)[6].
Other forms of AI have also enhanced innovative ways of producing phishing content, synthetic user account creation, and deep fake cyber deception that requires little human input (George, 2024)[7]. Consequently, the threats about automation means that current countermeasures cannot be effective against future corporate risks as AI advances (Jimmy, 2021).

3. EVOLUTION OF AI IN CYBER THREATS

Cyber threats have evolved with the help of AI allowing the attackers to become more proficient at their work. One of them, adversarial machine learning, enables them to control and penetrate AI models without being detected. Artificial intelligence has enhanced ordinary phishing and social engineering schemes by adding more authenticity to the scams. First, there is the kind of malware that can change its behaviour in real time in order to avoid easy identification, thus making it even more dangerous.

To reduce such risks, organisations must implement future security measures such as ZTA and AI security to prevent new threats.

3.1 Historical Development of Cyber Threats and Hacking Techniques

Cyber threats have risen significantly in recent decades, from viruses and worms to complex malware, ransomware, and cyber-attacks by nation-states (Alam & Rafiq, 2022)[9]. However, it is essential to understand that initial cyber-attacks were more human-cantered and involved simple hacking and script-based relaying (McCall, 2024)[10]. Modern hackers also use AI to speed up attacks, such as machine learning for credential stealing, reconnaissance, and bot-generating exploits (Kozí, 2023).

3.2 Introduction of AI in Cyber security (Both Offensive and Defensive Applications)

In recent years, AI has become an essential concept in cyber security. It has improved the ability of a defence system comprising intrusion detection, behavioural analytics, and threat mitigation (Jabbarova, 2023)[12]. Yet cybercriminals are using AI similarly to create self-evolving malware, automate social engineering attacks, and augment the concept of deception in cyberspace (Singh et al., 2024). This has led to a remarkable ability to find fresh approaches to hacking because an AI system has more time and data to analyse than the human mind (Kilovaty, 2025)[14]. For example, generative AI can develop polymorphic malware that transforms, bypasses, and passes antivirus software (Ratnawita, 2025). It can also replicate interactions with a high level of accuracy, making it difficult to identify, 2025).

3.3 The Transition from Rule-Based Automation to AI-Driven Autonomous Attacks

First, threat detection was based solely on the rules and automations written in advance and possessed such features as signatures and heuristics (Faber, 2019)[17]. Although they had some protection against such attacks, these traditional systems were ineffective in addressing emerging threats. With the help of machine learning and deep learning, it is possible to implement artificial intelligence assisted attacks that are capable of learning from attacks previously used, create probable new variants, and react to actual countermeasures (Humphreys et al., 2024). AI-based cyber threats are not just a static threat after its creation. Moreover, in adversarial AI, attack approaches can change, conceal themselves and use undiscovered vulnerabilities to launch attacks before the steering committee can intervene (Vardhan et al., 2025)[19]. This shift signifies a rotational change in the cyber security policies with the need to counter rising threats from AI-enabled attackers using AI.

Section	Description
AI-Enhanced Cyber Threats	Attackers use AI to improve proficiency, including adversarial machine learning to penetrate AI models and advanced phishing schemes. AI-driven malware can alter behaviour in real-time to evade detection.
Countermeasures Suggested	Adoption of Zero Trust Architecture (ZTA) and AI-based security to combat evolving threats.
Historical Development of Cyber Threats	Cyber threats evolved from simple viruses and worms to advanced malware and state-sponsored attacks. AI is now used for credential theft, reconnaissance, and automating exploits.
AI in Cybersecurity (Offensive and Defensive)	AI enhances defence with intrusion detection, threat mitigation, and behavioural analytics. Offensively, AI is used for self-evolving malware, automated social engineering, and bypassing security systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131263

Shift to AI-Driven Autonomous Attacks	Transition from rule-based automation to AI-enabled attacks that adapt and learn from previous threats, exploiting unknown vulnerabilities.
Key Challenge	AI's dual-use nature in both offensive and defensive strategies complicates cyber security efforts.
Recommendations	Continuous monitoring, advanced AI security measures, and proactive threat intelligence are essential to counter AI-enhanced threats.

4. CAPABILITIES OF AUTONOMOUS HACKING SYSTEMS

Introducing AI in cyber threats has created self-suspending hacking systems capable of conducting cyber-attacks independently. These systems employ ML, DL, and AL to perform reconnaissance, identify available vulnerabilities, dynamically generate malware, perform complex and compelling social engineering, and more (Kaloudi & Li, 2020). AI operations in hacking execute hack operations and make them more effective, especially when it comes to evading security measures, by learning from their past failures (Andreoni et al., 2024).

This is because conventional reconnaissance assists these systems in analyzing networks and identifying vulnerabilities in real time. Machine learning algorithms process public data, such as metadata, software versions, and configurations, to foresee vulnerabilities (Usman et al., 2024). Similarly, the NLP approach helps AI find a leaked database of sensitive data, social engineering, and various public repositories with detailed attack intelligence (Heckel & Weller, 2024).

AI in malware generation has led to the development of malicious software that can bend the rules to fool the detector system. Polymorphism, metamorphism, and adversarial machine learning are some of the features that AI uses to alter its code for the emission of new threats, hence cannot be easily detected (George, 2024). The latest generation of malware is also capable of self-replication, self-sensing, and self-adaptation about the targeted defence structures (Sarker, 2024). Cognitive ransomware attacks have gone a notch higher in determining the strategic targets to hit using financial details and system sensitivity (Vardhan et al., 2025).

Deep fake technologies have become a standard weapon in the cybercriminal's arsenal, creating realistic imitation voices, images, and videos used in the impersonations. Phishing that utilizes artificial intelligence to send emails, instant messages, and phone calls that look real and feel natural (McCall, 2024). These are advanced phishing campaigns since they can change in response to the target's actions and the posts enacted within the targeted social media account (Jabbarova, 2023).

Whereas previously social engineering has been practiced by hackers solely on people, now it utilizes automation and AI. AI personas are persistent and converse with targets beyond requests for information but create a rapport, then ask higher risk questions (Ratnawita, 2025). Reinforcement learning makes it possible for the AI systems to study previous scams and improve the steps used in the following scams, which makes social engineering even more efficient (Asia & Brouwer, 2025). Also, bystander impersonation attacks, which involve formulating attacks in the targeted victim's exact messaging, writing or talking style, have become a threat to cyber security workers (Kilovaty, 2025).

Some cases demonstrate the effectiveness of AI-based cyber threats, as seen in real-world scenarios. Deep fakes have also been used to simulate and impersonate business professionals in unlawful transactions (Singh et al., 2024). Although typically executed by humans, phishing has evolved with an AI system that can infiltrate numerous email systems and filters, leaving many organizations' data at risk (Akhtar & Rawol, 2024). Furthermore, it is essential to recognize that machine learning and artificial intelligence concepts have been integrated into malware, allowing these programs to learn and evolve in their operations (Valencia, 2024). These examples underscore the need to enhance security against the growing threat of self-learning malicious programs.

5. IMPACT OF AI-GENERATED CYBER THREATS ON THE CYBER SECURITY LANDSCAPE

Artificial Intelligence in the recent past has become a prominent cause of cyber threats, and it eradicates some hurdles while creating new ones. The use of automation in hacked systems today, with artificial intelligence, makes it even harder to combat since it's more advanced than traditional hacking. The use of AI for security purposes has developed an uptick in escalating computer-based attacks as cybercriminals take advantage of artificial intelligence systems. Artificial Intelligence now performs cyber-attacks at a speed beyond traditional defences, therefore security tactics need immediate changes (Kaloudi & Li, 2020).

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024
DOI: 10.17148/IJARCCE.2024.131263

5.1 Increased Speed and Efficiency of Cyber attacks

A hacking technique that has proven much more advanced than traditional human hacking involves using AI technology. Traditional cyber-attacks require detailed reconnaissance work alongside manual scripting and testing to complete their execution. AI-powered hacking systems execute an entire attack automatically through automated vulnerability scanning until they launch custom-made exploits in less than two seconds. Machine learning algorithms work in real time on billions of data units and analyse security systems' vulnerabilities with little or no interference from human beings (Usman et al., 2024).

It integrates a paradigm that can improve the efficiency from the errors gathered in previous attempts and adjust the strategies on the fly. For example, deceptive attack strategies, such as AI-driven brute force, can crack passwords through prioritizing likely combinations learnt from the user's behaviour. Malware using AI technology can self-evolve through adaptations that make it overcome standard antivirus programs by altering its signature. The new technological developments shorten the implementation period of cyber-attacks while simultaneously boosting their performance (Heckel & Weller, 2024).

5.2 Challenges for Traditional Cyber security Defences

The enhanced development of artificial intelligence in cyber threats is an emerging factor that is difficult to counter with conventional cyber security measures. Legacy security solutions, such as firewalls and virus scanning that rely on existing patterns, are ineffective against new attacks, which can transform into different forms in minutes, if not seconds. Most cyber security measures still utilize a fixed set of threat signatures, which AI-generated malware can easily bypass as it can alter its form to avoid detection by existing systems (Andreoni et al., 2024).

Also, AI overwhelms security monitoring systems with data so that analysts cannot distinguish actual threats from noises. This depletes traditional security operations centres (SOCs), resulting in slow responses and making it easier for systems to be penetrated. With more advanced AI attacks emerging dynamically in contemporary society, organizations have to move from a defensive approach, where they wait to be attacked and then deal with it, to an offensive approach, using artificial intelligence-aided tools to counter the attacks.

5.3 AI's Ability to Bypass Conventional Security Measures.

Among AI's most severe cyber threats, it does not impede exceeding traditional security tools and measures. Some of the presented hacking tools use deep learning and reinforcement learning for better penetration testing of systems. These systems can independently identify approaches to exploiting holes in the system before the patches are released into the market, thus giving cyber criminals a vantage point (Sarker, 2024).

It is also being increasingly applied to further social engineering techniques. Deep fake involves making fake realistic videos based on one's desire, and its use is a tool employed by attackers to trick targets into releasing vital information or processing counterfeit transactions. AI-driven phishing attacks can process large amounts of data to write more complex and credible messages to the recipients, enhancing the chances of making them fall for the phishing attempt (Ratnawita, 2025).

AI also manipulates cyber security tools. In recent years, the bad guys have not remained idle and are devising ways to penetrate AI-driven security systems using a tactic known as adversarial machine learning. Criminals feed AI with wrong data, which makes the AI categorize otherwise malicious activities as safe, thus avoiding being blocked by AI technologies (Asia & Brouwer, 2025).

5.5 There are several questions to raise on ethical issues of AI based on its dual-use nature:

The applicability of AI as both a tool for enhancing the defensive line and a weapon of attack raises significant ethical issues. AI enables governments, corporations, and ethical hackers to create practical security tools for improved cyber defence; however, cybercriminals may exploit these developments maliciously (Jabbarova, 2023).

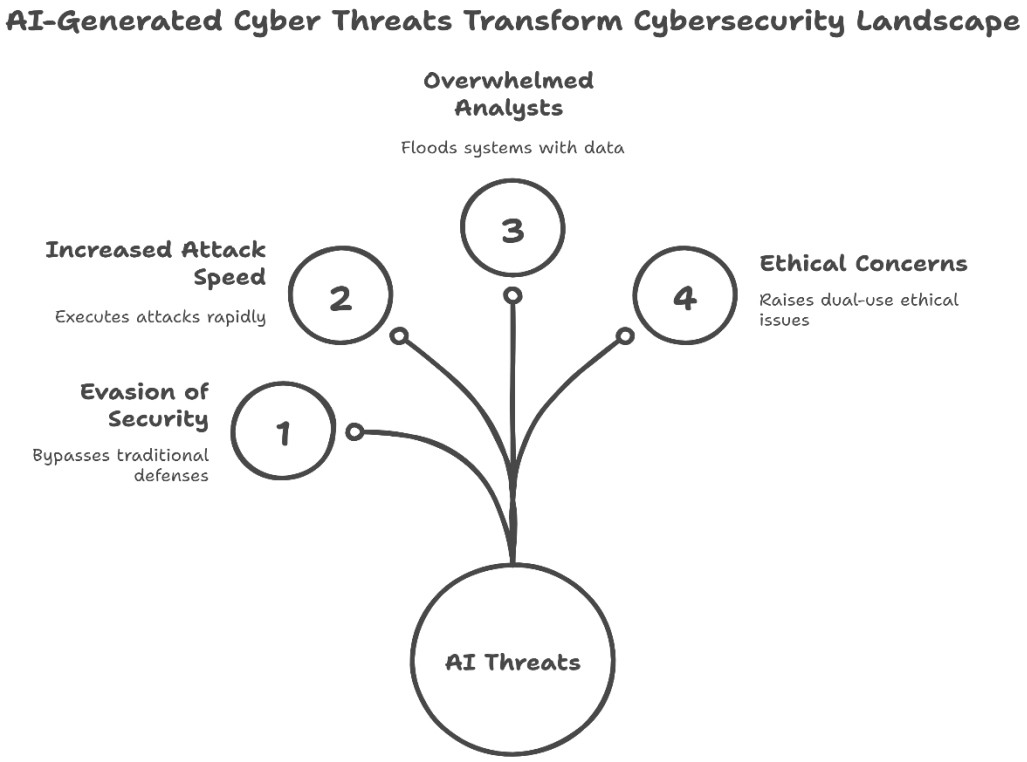
This is also an ethical concern, especially when addressing issues such as the spread of fake news by AI or even cyber warfare. Deep fake technology, botnets powered by artificial intelligence, and the currently observed automated fake news campaigns pose significant risks to democratic processes, national security, and individual privacy. Availability is another important implication related to the use of AI for hacking; due to current technological advancements, a typical computer hacker can obtain a copy of an already trained AI model to enhance their hacking skills (Singh et al., 2024).
To mitigate these challenges, policymakers and cyber security professionals need to set up strict codes of prohibition and virtues regarding the use of AI. Barring the acquisition and use of AI for creating cyber weapons and to sustain AI as an instrument of security instead of destruction, international cooperation is crucial (Humphreys et al., 2024).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131263



6. DEFENCE STRATEGIES AGAINST AI-GENERATED CYBER THREATS

The rise of AI-generated cyber threats necessitates robust defence strategies that leverage AI-driven security solutions, ethical AI frameworks, regulatory measures, and skilled cyber security professionals. Small and large organisations should incorporate methods of Artificial Intelligence into threat detection, anomaly recognition and automatic reactive processes to manage advanced threats. Data mining and analysis are other ways that are used when it comes to detecting threats because machine learning is capable of identifying patterns of malicious behaviour in real-time to prevent any future threats. Automated security systems can take actions by themselves, it can shut down affected systems, block traffic to and from the malicious sources, and even counterattack all by themselves even before severe damage occurs. AI in cyber security can help improve the organization's capabilities of both threat forecasting and mitigation in addition to its preparedness for such cyber threats (Sarker, 2024).

The roles of ethical first principles in AI are essential for controlling the adverse effects of creating autonomous hacking systems. Applicants should ensure that the use of AI in security technologies is appropriately addressed by observing the culture of openness, and adherence to the correct standards of conduct and fairness. Specific codes of ethics should be laid in place to avoid the misuse of artificial intelligence. It should be subjected to constant research and scrutiny to eliminate the mishaps of the same. Security can be improved by adopting explainable AI since it will enhance the understanding and validation of the decision-making process initiated by the AI. The presence of a set of rules that are appropriate for AI development, deployment, and regulation will allow avoiding cases when AI technologies will be used for harming individuals or other entities (Grant, 2022).

To this effect, the paper argues that regulatory and policy mechanisms are critical in reducing the threats arising from AI accommodation of cyber threats. Due to the increasing use of artificial intelligence in cyber security, governments and international organizations must encourage the development of legal requirements that regulate the use of artificial intelligence. Some of the policies have to do with the creation and distribution of hacking tools through AI technology, which makes such tools available to the wrongdoers. They should also dictate cyber security in organizations to ensure that organizations adopt AI protection against emerging threats. Departments of information technology in different countries should therefore collaborate to combat the risks of AI-generated cyber threats and avoid the development of AI cyber weapons across the world. There is an urgent need to regulate the use of AI for cyberspace security while at the same time encouraging policymakers to develop AI technologies (Andreoni et al., 2024).

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024
DOI: 10.17148/IJARCCE.2024.131263

Cyber security specialists actively participate in containing cyber threats of AI origins by constantly changing strategies. Given the increasing advanced and complex AI facilitated attacks, security professionals must promote their knowledge on AI-enabled threat intelligence, adversarial machine learning, and automated defence. Continuous learning in the field and continuing education is critical for preventing and eradicating all new and developing threats originating or enhanced by artificial intelligence in front-line cyber security teams. Combining artificial intelligence and human input is feasible in any security framework and enhances the protection by not automating it but extending its usage. A proactive model is to integrate cutting-edge cyber security applications with human experts by ensuring adequate protection against the threat of AI-facilitated cyber-attacks (Asia & Brouwer, 2025).

DISCUSSION

AI and ML are being integrated into cyber security quickly, increasing the system's threat detection and prevention. However, cybercriminals also utilize these technologies to stage even more complicated stunts, particularly on multi-cloud platforms. The use of AI and ML is a risky factor that has developed because attackers also use these technologies to breach traditional security measures. The first threat described is adversarial machine learning, to which the attackers modify the AI models by inputting poisoned data or changing the input type. One potential risk of using this type of attack is in the environments that link multiple clouds since security measures, especially those working in layers, may differ from cloud to cloud. Such threats are significantly increased with the essence of multi-cloud environments, including the scalability and interconnectivity issues; therefore, it becomes imperative to use adversarial training and rigorous validation methods.

Deep fake phishing also poses a significant threat because artificial intelligence makes the fake content appear convincingly real. This technique is a threat at the core of traditional verification methods and hinders threat identification because it works seamlessly, unlike deep fakes of videos, voices, and text. In a multi-cloud environment with multiple communication points of engagement, the deep fake attack can be so sophisticated that it needs artificial intelligence-enabled modes of analysis and verification.

Also, it reveals the weaknesses of the multi-cloud system that AI-enabled attackers can attack and exploit. Lack of coherent security measures, different levels of encryption, and the problem of ID & Access in a multiplatform environment benefit the attackers. In particular, the given weak points can be detected by an AI, attacks can be launched using an AI, and the attacker can emulate normal users.

CONCLUSION

Incorporating AI and ML in cyber security has undeniably boosted overall security improvements significantly. On the other hand, hackers and cybercriminals have incorrectly exploited the same technologies to conduct more complex and covert attacks, particularly in the Ascend multi-cloud setup. It is imperative to state that the use of AI and ML is dual, hence lengthening the security role that organizations should embrace innovative and responsive security measures.

Some of these are presented by adversarial machine learning, deep fake phishing, and AI malware that have exposed downfalls to current multi-cloud security models. The vulnerability of these weaknesses is enough for the attackers to strike, outdo, or operate through the current traditional approaches of security, which is known as the Perimeter Defence Model, to the new advanced model called the Zero Trust Architecture (ZTA). Continuous verification, using least privilege access, and functioning with AI-based threat intelligence forms what ZTA offers as a satisfactory solution to these emerging threats.

In other words, cyber security in multiple clouds will require AI for defence and detection in the future. Organizations must form robust, growth-static architectures to counter AI-enabled threats in real time. As AI technologies develop daily, the concepts and measures that must be applied to prevent cyber threats to digital resources will also change accordingly.

REFERENCES

[1]. Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. International Journal of Multidisciplinary.
[2]. Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR). https://doi.org/10.1145/3391195

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131263

[3]. Usman, Y., Upadhyay, A., Gyawali, P., et al. (2024). Is generative AI the next tactical cyber weapon for threat actors? Unforeseen implications of AI-generated cyber attacks. arXiv preprint. https://arxiv.org/abs/2401.18312

[4]. Heckel, K. M., & Weller, A. (2024). Countering autonomous cyber threats. arXiv preprint. https://arxiv.org/abs/2410.18312

[5]. George, A. S. (2024). Riding the AI waves: An analysis of artificial intelligence's evolving role in combating cyber threats. Partners Universal International Innovation Journal.

[6]. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cyber security defences. Valley International Journal Digital Library.

[7]. Sarker, I. H. (2024). AI-driven cyber security and threat intelligence: Cyber automation, intelligent decision-making, and explainability. Google Books.

[8]. Andreoni, M., Lunardi, W. T., Lawton, G., & Thakkar, S. (2024). Enhancing autonomous system security and resilience with generative AI: A comprehensive survey. IEEE Access. https://doi.org/10.1109/ACCESS.2024.0123456

[9]. Valencia, L. J. (2024). Artificial intelligence as the new hacker: Developing agents for offensive security. arXiv preprint. https://arxiv.org/abs/2406.07561

[10]. Vardhan, H., AN, K. S., & Sangers, B. (2025). Future trends and trials in cybersecurity and generative AI. In CyberSecurity With Generative AI (pp. TBD). IGI Global.

[11]. Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. IT Journal Research and Development.

[12]. Kilovaty, I. (2025). Hacking generative AI. Loyola of Los Angeles Law Review. Retrieved

[13]. McCall, A. (2024). Cybersecurity in the age of AI and IoT: Emerging threats and defense strategies.

[14]. Kovací, P. D. (2023). Threat actors seeking to exploit AI capabilities: Types and their goals. Strategic Impact.

[15]. Jabbarova, K. (2023). AI and cybersecurity: New threats and opportunities. Journal of Research Administration.

[16]. Singh, K., Saxena, R., & Kumar, B. (2024). AI security: Cyber threats and threat-informed defense. 8th Cyber Security in Computing Conference. Retrieved from

[17]. Faber, I. J. (2019). Cyber risk management: AI-generated warnings of threats. ProQuest.

[18]. Ratnawita, R. (2025). Cybersecurity in the AI era: Measures against deepfake threats and artificial intelligence-based attacks. Journal of the American Institute.

[19]. Asia, S., & Brouwer, R. (2025). AI-enhanced ethical hacking: Redefining cyber security testing and analysis.

[20]. Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024).AI hype as a cybersecurity risk: The moral responsibility of implementing generative AI in business. AI and Ethics.https://doi.org/10.1007/s43681-024-00255-1