THE ASIAN BULLETIN OF GREEN MANAGEMENT AND CIRCULAR ECONOMY
Vol 5, Issue 1(2025)
THE ASIAN BULLETIN OF GREEN MANAGEMENT AND CIRCULAR ECONOMY
ISSN (online): 2959-0035
http://abgmce.com/10.62019/abgmce. v5i1.125
ISSN (Print): 2959-0027

Ethical Hacking in the AI Era: Enhancing Cybersecurity for Sustainable Digital Transformation

Bismah Hassan*, Khalid Bin Muhammad, Khaliq Ahmed

Chronicle

Article history

Received: Jan 3, 2025
Received in the revised format: Feb 2, 2025
Accepted: Feb 28, 2025
Available online: March 11, 2025

Bismah Hassan and Khaliq Ahmed are currently affiliated with Department of Computer Science, Iqra University, Karachi, Pakistan.
Email: bismah@iqra.edu.pk
Email: khaliq@iqra.edu.pk

Khalid Bin Muhammad is currently affiliated with the Department of Computer Science, Ziauddin University, Karachi, Pakistan.
Email: khalid.muhammad@zu.edu.pk

***Corresponding Author:**

Abstract

This research article explores the intersection of ethical hacking and artificial intelligence (AI), highlighting the evolving landscape of cybersecurity in the context of AI advancements. As AI technologies become increasingly integrated into various sectors, ethical hacking emerges as a critical practice to identify vulnerabilities and mitigate risks associated with AI systems. This study examines the ethical implications of AI in hacking practices, the role of ethical hackers in safeguarding AI applications, and the potential for AI to enhance ethical hacking methodologies. Through a comprehensive literature review and case studies, the findings reveal the dual nature of AI as both a tool for ethical hacking and a potential source of new vulnerabilities. The article concludes with recommendations for integrating ethical considerations into AI development and ethical hacking practices.

Keywords: AI, implications, hacking, cybersecurity, risks.

INTRODUCTION

Knowledge In today's hyperconnected world, cybersecurity has evolved from a niche technical concern to a basic necessity for businesses, governments, and individuals. The fast expansion of digital transformation has induced an overwhelming dependence of organizations and individuals on complex technological infrastructure, characterizing the way they store and manage massive volumes of sensitive data. Such a digital dependency allowed new avenues for facets of efficiency and innovation to thrive, although it stood open for attacks from an increasing frequency of cyber threats-multiplied in complexity and intensity [1]. Cybercriminals, usually armed with evolving tools and threats, are ever on the lookout to exploit every weakness and vulnerability in the security system, making every day the blah diary days inept at solving the weaknesses within themselves.

The Rising Threat Landscape

As per the Cybersecurity Ventures 2023 Cybersecurity Report, cybercrime will cost the global economy $10.5 trillion annually by 2025, up from $3 trillion in 2015 [2]. This explosive growth of cyber threats means businesses can no longer rely solely on conventional cybersecurity protocols: firewalls, antivirus programs, and signature-based intrusion detection systems, which typically respond only after an attack has occurred. As a result, proactive security needs to be taken up to prevent cybercriminals from penetrating

critical infrastructures. Cyberattacks can be divided into a number of forms, such as phishing scams, ransomware, zero-day exploits, and attacks on systems' availability like DDoS attacks. These threats manifest very serious risks to national security, economic stability, intellectual property, and personal privacy. These attacks attacking multinational firms, governmental organizations, and health institutions demonstrate a greater necessity for advanced defenses. To counter these challenges, cybersecurity experts are taking a proactive approach called Ethical Hacking. While the gist of malicious hacking is attacking systems for financial reward or some kind of disruption, ethical hacking (also known as white-hat hacking) involves professionals who are legally and systematically concerned with testing the security infrastructure of systems, thereby finding possible security loopholes before an actual attacker has a chance to exploit them.

The Role of Ethical Hacking in Cybersecurity

Ethical hacking is very important in every modern cybersecurity strategy. By providing real-world representation of attacks, ethical hacking assists organizations to identify and fix vulnerabilities before hackers exploit them [3]. These exploits form the basis of penetration testing, a controlled and systematic way of assessing an organization's defenses by attempting to breach systems like real attackers would. The central purpose of ethical hacking is to bolster cybersecurity resilience by uncovering flaws in the systems, mending misconfigurations, and giving attention to weak access controls. By carrying out rigorous tests and risk assessments, ethical hackers help firms bolster their security posture and proactively avert costly breaches, as shown in Figure 1 as contributions of ethical hacking.

Key Contributions of Ethical Hacking

- Proactive Security Approach - Ethical hackers enable organizations to assess and remove threats before they mature into a full-blown attack.
- Regulatory Compliance - In many industries like healthcare, finance, and government, penetration testing and security audits are mandated to comply with legal regulations. Ethical hacking checks for such compliance standards as GDPR, HIPAA, and PCI-DSS.
- Incident Response Readiness - Ethical hackers help organizations develop better incident response plans to contain losses in case of cyberattack.
- Enhanced Security Awareness - Ethical hacking creates awareness among staff and IT teams about potential threats to company information security, reducing the chance for human error to become the weakest link in a company's cybersecurity strategy.

Artificial Intelligence: Changing Game of Ethical Hacking

The advent of AI tech was revolutionary in ethical hacking, enabling faster, better, and more-efficient identification and mitigation of possible cyber threats. AI-powered systems automate the security process with far less scope for error while speeding processes rapidly so that threat detection is more effective than traditional manual penetration testing [4]. Real-time analysis of huge datasets, identification of patterns, and detection of anomalies lend a boost to ethical hackers in keeping a leg up on cybercriminals. As depicted in Figure 2, AI-enabled solutions are capable of continuously monitoring

networks by keeping an eye on suspicious activities and should be able to accurately predict possible cyber threats beyond human capacity.

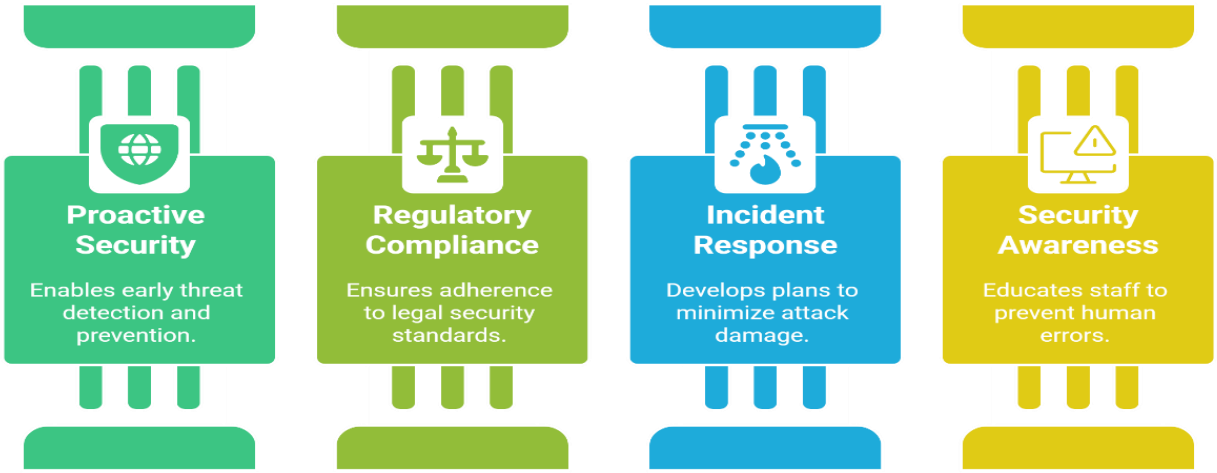

Figure 1.
Strengthening Cybersecurity through Ethical Hacking Practices.

But now, with growing sophistication, the cyber threats don't bind themselves to methodologies of ethical hacking; they have invented tools and strategies really advanced to overcome the hurdles of penetration. Here comes the effective use of Artificial Intelligence.

Figure. 2.
AI-Enhanced Cybersecurity Process

KEY CONTRIBUTIONS OF AI TO ETHICAL HACKING

Automated Threat Detection: AI-powered tools can scour entire networks in seconds, spotting weak points and flagging vulnerabilities that require immediate attention. How does an intelligent online work? In other words, what other technology is used? Real-Time Anomaly Detection: Machine learning algorithms can detect unusual patterns in

behavior such as attempts at unauthorized entry or data exfiltration and notify security teams instantaneously. Predictive analytics: AI can predict any kind of cyberattack based on previous attack data, whereby companies would take proactive measures to try and stop the attack.

Advanced Malware Detection: AI-driven cybersecurity solutions are capable of specifically detecting zero-day exploits and polymorphic malware that tend to evade typical security software.

Adaptive Security Protocols: AI is a dynamic security protocol adjustment and access control in direct response to the threats it faces, allowing for a much more resilient defense mechanism.

The Growing Role of AI in Cybersecurity Operations

Capgemini found that 69% of organizations believe that AI technology will be pivotal in discovering and fighting cyber threats [5]. Unabated, high demand prevails among modern enterprises to invest heavily in machine learning-based security solutions to automate vulnerability assessments and improve cyber defense. AI-powered systems are now deployed worldwide with many tools such as IBM Watson for Cyber Security, Darktrace, and Deep Instinct to analyze security logs, detect suspicious activities, and even predict attack vectors even before they materialize. These smart systems are combating the reduction of response times by preventing cyberattacks before they can do serious damage. While AI boosts the capabilities of ethical hackers, it incorporates new problems and raises many questions. Cybercriminals are deploying AI attacks, infecting computers with adaptive malware, scamming victims from deepfake phishing, and deploying automated password breakers that can sidestep classical security [6]. This presents a hallmark of the double-edged sword of AI in the field, whose virtue lies in its ability to bolster defensive mechanisms but also in its ability to arm cyber adversaries.

This paper examines the transformational impact of AI in ethical hacking, the benefits, challenges, and prospects. The main focus areas are:

- An introduction to how AI enhances ethical hacking through improved efficiencies, automation, and threat detection capabilities.
- The challenges of AI ethical hacking, for example, ethical challenges, adversarial attacks, and workforce skill gaps.
- Opportunities for AI in ethical hacking, with a focus on national security, predictive analysis, and automated security frameworks.
- Opportunities in AI-ethical hacking towards the future, including systems for developing ethical AI frameworks and increasing automation.

With the evolution of cyber threats, organizations must proactively adopt advanced tools powered by AI to counter evolving attackers. For sure, the union of AI and ethical hacking has the potential to rewrite the future of cybersecurity, bringing about a much more secure, resilient, and harder-to-breach digital ecosystem.

The Role of AI in Ethical Hacking

In the rapidly changing world of cybersecurity, the use of artificial intelligence in ethical hacking has transformed the way security personnel approach threat detection, vulnerability management, and risk mitigation. Ethical hacking, which was once mainly dependent on manual penetration tests and rule-based security measures, benefits from

AI's real-time analytical, predictive modeling, and advanced anomaly detection capabilities. Such leaps in technology have made cybersecurity more efficient, proactive, and responsive, thereby allowing organizations to ward off increasingly sophisticated cyber threats.

AI: The Game-Changer of Ethical Hacking

Traditional ethical hacking techniques include manual code reviews, penetration testing, and security audits, which take a lengthy time and a lot of expertise. Yet, with increasingly advanced and automated attacks, it becomes a challenge for human analysts to catch up. AI powers these stealthy ethical hacking solutions by speeding up tedious security processes with a high level of automation, coming in hot to cut down on time taken for the speedy identification and effective remediation of threats [7]. Artificial intelligence assists ethical hackers in finding vulnerabilities in large and complex networks that might not be conceived otherwise. The machine-learning algorithms can analyze security logs, identify the patterns of deviations, and predict possible threats even before they materialize into a full-fledged cyberattack. With cybercriminals using AI for automating attacks like deepfake-based phishing, AI-generated malware, and adaptive ransomware, the ethical hacking community needs to leverage AI-powered tools to suppress the active cyber threats, as illustrated in Figure 3 on the role of AI in hacking.

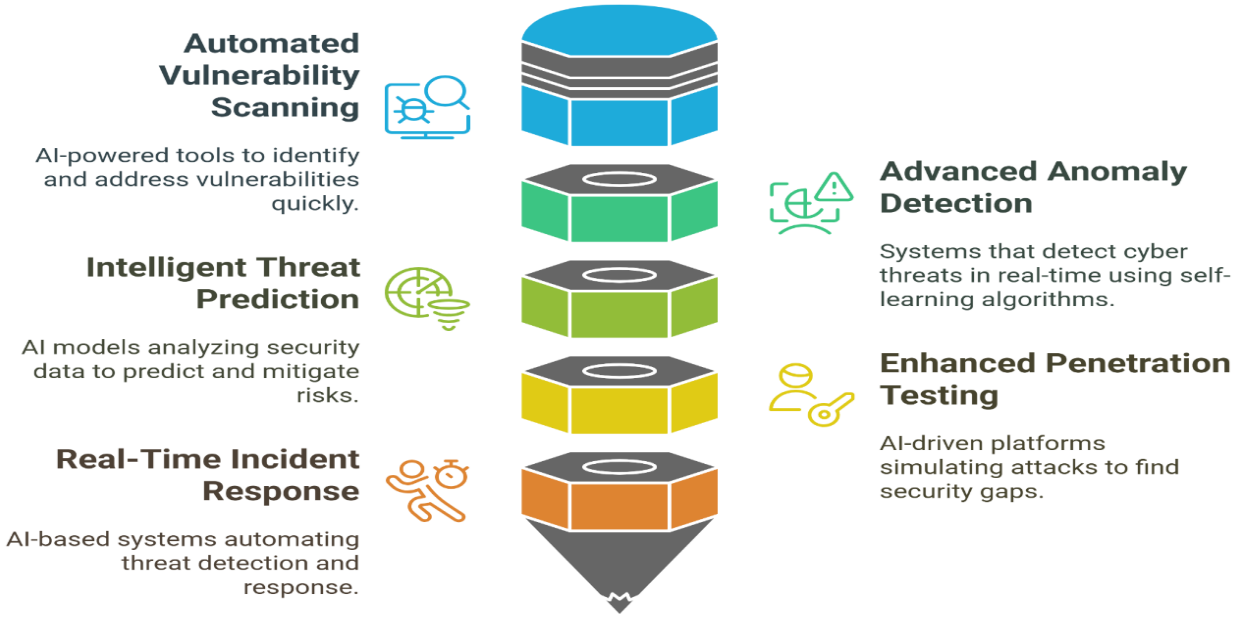

Figure 3.
AI's Role in Enhancing Cybersecurity

How AI is Revolutionizing the World of Ethical Hacking: An AI-based ethical hacking tool would equate with a multi-faceted approach to cybersecurity, automating detection, improving predictive abilities, and making a lot more effective the real-time response. Here's how AI essentially is changing the ethical hacking scenario:

Automated Vulnerability Scanning

The most remarkable gift of AI to ethical hacking is in automated vulnerability assessment. AI security tools proactively scan, survey, and assess the digital infrastructures for security holes that human analysts may not notice.

How it Works:

- AI Baseline vulnerability scanners utilize machine learning models to compare current systems and applications configurations with known vulnerability databases.
- AI VAPT tools look out for misconfigurations, weak protocols, and outdated software versions while doing deep packet inspection.
- AI becomes good in detecting even the zero-day vulnerabilities by identifying behavioral patterns that go against the normal operation of the system.

Example from the Real World: Over 22,000 new vulnerabilities get reported every year by the NVD. AI-based scanners such as Tenable.io, Qualys, and Nessus, allow companies to keep up with the speedy advancements in the field which will allow them to apply security patches before attackers exploit them.

Advanced Anomaly Detection

AI enhances ethical hacking by identifying anomalous behavior in real time for organizations to detect unusual patterns that could suggest a likely cyberattack.

How It Works:

- AI models are trained on normal behavioral network characteristics to create the 'normal' model.
- AI detects anomalies, which include unauthorized login attempts, rare file accesses, and possible data exfiltration.
- Unlike rule-based security systems that rely mainly on manual identification, AI does continually learn and change to adapt to evolving modes of attacks.

Example: Darktrace uses self-learning algorithms to detect real-time cyber threats. The system keeps an eye out for subtle deviations from the 'normal' that could suggest an ongoing insider threat, infiltration with malware, or a data breach, effectively without the necessity of pre-programmed attack rules.

Intelligent Threat Prediction

One of AI's revolutionary skills is predicting cyber-attacks based on historical attack data, threat intelligence feeds, and system log analysis. This capacity affords AI-executed analytics the elegance of permitting an organization to shore up its defenses before the attacks are perpetrated.

- AI analysis of historical cyber occurrences to single out attack potentials.
- Machine learning algorithms use pattern recognition to predict how cybercriminals are likely to exploit existing vulnerabilities.
- Provides actionable advice to organizations so security measures can be strengthened ahead of time before the attack happens.

An Example in the World: IBM Watson for Cyber Security uses cognitive AI models to analyze billions of security documents, identifying attack vectors before they emerge; the system therefore enables cybersecurity teams to proactively address risks, reducing the likelihood of successful cyber intrusions [8,9].

Enhanced Penetration Testing

AI-enabled penetration testing is the new kid on the block when it comes to becoming faster and more efficient with an ethical hacking assessment. Conventional penetration

testing involves human testers simulated cyberattack which may take as long as weeks or even months. Artificial Intelligence enhances this process by automating reconnaissance, scanning, and testing security defenses.

How It Works:

- AI systems conduct reconnaissance by collecting information about target systems, such as open ports, firewall configuration, and system vulnerabilities.
- AI penetration testing tools simulate cyberattacks as stress tests for an organization's various defense mechanisms on attack scenarios.
- AI acts a support to human ethical hackers by providing a detailed risk assessment and prioritizing the vulnerabilities based on exploitability potential and damage it might cause.

Real-World Example: Platforms like Metasploit AI and Core Impact build in penetration testing with artificial intelligence, enabling security teams to simulate attack scenarios and uncover exploitable security gaps more quickly than traditional manual methods.

Real-Time Incident Response

Automated AI-driven incident response systems provide immediate response to security breaches, ensuring that counter-cyberattack operations will prevent additional damages [10].

How It Works:

- AI performs continuous monitoring on the networks for suspicious activity.
- When an ongoing cyber attack is detected, AI security solutions automatically block the malicious activity, contain the affected systems, and notify the security team.
- AI security tools automatically adjust firewall rules, revoke access rights, and quarantine threats from spreading.

A Real-world Example: Systems like Splunk, QRadar, and Azure Sentinel perform real-time analysis of security data, allowing cyber threats to be detected and remediated through AI-driven security information and event management.

AI as an Indispensable Tool for Ethics-Certified Hackers: AI, possessing enormous processing and analytical data capabilities throughout a large information system, is an indispensable tool for ethical hackers. AI sentimental hacking solutions allow an organization to:

- Detect and counter cyber threats faster than human analysts.
- Automate tedious security tasks, thereby enhancing efficiency.
- Forecasting future attack patterns and preventive security measures.
- Provide instantaneous feedback, allowing for reduced effects and damages from subsequent actions of security breaches.

The Cybersecurity Forecast by Gartner will have 60% of the enterprise operations led by regular operational cybersecurity AI operations by 2025, thus suggesting a heavy dependency on AI solutions [11]. Even as cyber threats keep evolving, ethical hackers will have to adopt AI powers to nap a jet course to stay above cyber adversaries, thus ensuring code-laden digital assets are more or less kept out of the cyber-attack showcase

Figure 4.
AI's Role in Enhancing Ethical Hacking

Challenges in AI-Driven Ethical Hacking

Benefits of AI in Ethical Hacking

- **Increased Efficiency and Automation:** AI removes repetitive and laborious tasks and thus gives ethical hackers time to think about complex security strategies. Automated, AI-driven tools can scan thousands of systems within minutes, a job that would otherwise have taken a human hacker days to weeks to complete.
- **Advanced Threat Discovery:** Cybersecurity experts often react to cybersecurity incidents on discovery, but AI comes in to employ the proactive approach by detecting weaknesses before they are exploited. A machine-learning model can recognize attack patterns and alert the security teams about potential breaches before they happen.
- **Data-Driven Fees:** AI powers the cybersecurity decision-making processes by helping identify security trends in vast datasets that get unnoticed in seconds. AI-based analytics provide deeper insights that allow easy sorting and prioritization of ethical hacks according to high-risk vulnerabilities.
- **Detection of Phishing Emails:** AI-enabled email security tools can prevent phishing attempts using lanquage patterns and automatic link checking to scan incoming messages, intervening much faster before malicious emails reach employees. This has greatly reduced the success rate of phishing attacks.
- Government Statistics, as seen in figure 4, show the effects of AI:
- **Speed of Analysis:** AI will analyze and process security data up to 100 times faster than human analysts can, hence reducing the time for threat detection.
- **Cost Savings:** Cost savings of up to 30% could be achieved using AI-backed automation in cybersecurity operations.
- **Accuracy Rate:** The AI-based systems themselves reach an accuracy rate of up to 95% in threat detection, far outstripping traditional manual methods.

Beyond numerous advantages, ethical hacking aided by AI poses various challenges which require a resolved focus to exploit the potentials manifold.

- **Ethical Concerns and Biases in AI Systems:** As AI systems are trained from the already biased data, they may even continue the bias inadvertently. If biased datasets are chosen to train an AI model, it would lead to false positives or negatives and may miss an important vulnerability. They can also turn privacy violations when the AI-driven

security tools incidentally go on to analyze personal or sensitive data without proper regulations [12].

- **Adversarial Attacks on AI Models:** At the same time AI can become a target for such attacks. Hackers can manipulate AI models through feeding misleading data to induce false classifications of an AI threat detected or by ignoring such a real vulnerability. Security of AI models against instances of such adversarial attacks indeed poses a daunting challenge.
- **Skills Gaps in the Workforce:** AI cybersecurity needs a high skill set such that people performing other responsibilities in AI and ethical hacking. There simply aren't enough of these specialists to make AI work the way it needs to in the realm of ethical hacking.
- **Regulatory and Legal Issues:** AI-driven ethical hacking continues to operate in a gray area while legislation and guidelines are still forthcoming from regulators and the government to ensure that such AI-driven security practices remain ethical and lawful.

Addressing Ethical Challenges

In dealing with such challenges, organizations need to institute:

- Fairness and Accountability: AI systems must be transparent, auditable, and regularly reviewed to reduce biases and ensure ethical/enforceable decision-making.
- Workforce Development: Investments in AI and cybersecurity training programs would help bridge the skills gap created by the growing demand for them.
- Regulatory Compliance: Governments and industry leaders should work hand in hand to establish clear legal frameworks for AI-powered ethical hacking to keep privacy and security pertinently in compliance.

Opportunities for AI in Ethical Hacking

The introduction of AI in ethical hacking holds great promise in modernizing cybersecurity.

Advanced threat detection: AI-powered security systems will become even smarter in detecting complex threats, including those that support the weakness in traditional security measures.

Predictive analytics: AI will also enhance predictive security analytics so that the organizations could predict possible cyberattacks and take preventive measures.

Securing national security: Another powerful application of AI-based ethical hacking is in establishing a protective wall around critical infrastructure and national security against cyberattacks.

Future Prospects of AI in Ethical Hacking

The evolution of the future of AI-driven ethical hacking will be reminiscent of a game changer, given the pace at which technology is evolving now. Organizations need to invest in progressive AI algorithms, automation, and ethical AI frameworks to fortify their security posture, as the threat landscape becomes forever complex. AI-driven ethical hacking will radically change the cybersecurity industry, allowing faster, precise, and even proactive defenses against the modern age of cyber risks. The rise in frequency, sophistication of threats, AI-enabled phishing attacks, and autonomous malware all require security professionals to adapt. With AI ethics malware, the cyber team could do real-time detection of all possible threats, continuous automated tests, and analysing a path for possible attacks is done before they can launch any [13]. AI is no longer a luxury

but now is a need so that such evolving techniques by cybercriminals passionate about AI should be kept under control and cybersecurity could kept ensuring safety to digital environments. Looking ahead, it will be interesting to see how a number of trends will reshape the next generation of AI-driven ethical hacking.

More Advanced AI Algorithms

However, with the development of artificial intelligence, the machine-learning models will become more capable, quicker and more accurate in identifying cyber threats. Future AI-enabled security systems will be able to understand sophisticated attack patterns, detect zero-day exploitations, and autonomously respond to security incidents in real time.

How AI Algorithms Will Improve Ethical Hacking:

- Improved Accuracy in Threat Detection: AI algorithms will separate legitimate user behavior from an actual cyber threat with greater accuracy, hence reducing false positives.
- Self-Learning AI Models: Future AI-driven ethical hacking tools will utilize reinforcement learning to constantly improve on their attack simulations and threat detection capabilities.
- Highly Contextual Cybersecurity: AI systems will start to learn not just from static attack signatures, but are now able to analyze the context of cyber threats.

Real-Life Scenarios: At the most literal level, the AI-driven solutions will detect and block advanced threats which reduce incident response times from hours to milliseconds. It helps security teams track new trends in malware or to stop them from mutating in real time, so they can stay physically ahead of ever-evolving cyber threats. For example, Google's AI-powered Chronicle cybersecurity application processes billions of security events daily from various networks and detects potential threats faster than conventional security software. Such systems would further automate and improve their functionality.

Increased Automation in Ethical Hacking

AI-powered tools will be employed for total autonomy, reducing reliance on manual security assessments and penetration testing. With automation, ethical hacking will be more efficient and cost-effective and scalable.

How Automation Will Change Ethical Hacking:

- All-Automated Penetration Testing: AI-powered tools are projected to simulate an attack, recognize vulnerabilities, and create security reports without human intervention.
- Self-Healing Security Systems: Not only will AI help detect threats, it will also automatically cover vulnerabilities when found, bypassing the waiting period for a human response.
- AI-Powered SOCs (Security Operations Centers): Enterprises will deploy AI-driven SOCs for continuous monitoring, detection, and neutralization of threats in a 24/7 cycle.

Implication in Real Life: Decreased Workload: AI automation will take away the repetitive, manual tasks involved in the security procedure and allow cybersecurity professionals to concentrate on high-level strategic security planning. More Rapid Response to Incidents: AI-driven security orchestration, automation, and response (SOAR) systems will return responses to cyber threats within seconds, thus minimizing financial and operational

damage. Example: IBM Resilient and Palo Alto Cortex XSOAR are among the modern-day examples of AI-powered SOAR platforms that are already automating threat detection and response. AI-driven SOCs will become increasingly dynamic and can finish operations limited for humans [14],[15].

Development of Ethical AI Frameworks

With the integration of AI into ethical hacking's very being, it can be expected for governments, organizations, and policymakers to develop ethical AI frameworks that would establish a mechanism for responsible AI-driven cybersecurity practices. These AI-powered security solutions must be ethical, transparent, and unbiased so that privacy rights are not breached and there is no discrimination against specific groups.

The Major Guiding Principles of Ethical AI in Cybersecurity:

- Transparency & Accountability: AI-driven ethical hacking tools will need to be auditable and explainable so that security teams would understand how decisions were made.
- Privacy Protection: AI has to conform to sound data protection laws, like GDPR, CCPA, and HIPAA, to prevent unethical surveillance practices.
- Deployment of Non-Discriminatory Practices in AI Models: Bias in AI-based security tools will be reduced by training these models on diverse datasets.

The Real-World Implications: Stricter AI Governance: Governments, through legislation, will enforce AI laws to ensure the very existence of fairness and ethicality for cybersecurity tools.

Legality: Organizations will now adopt security practices in tandem with international cybersecurity legislation and data protection mechanisms. An example would be the AI Act enacted by the European Union in 2023 as a regulation to make sure that any AI systems adhered to a set of ethical and transparency standards. Future AI-driven cybersecurity tools will similarly have to comply with similar laws across the globe.

A New Era of Ai-Driven Cybersecurity

AI-based hacking will enable enterprises to develop better, quicker, and more proactive cybersecurity solutions. Next-generation cybersecurity innovation will be driven principally by the rise of ultra-sophisticated AI algorithms increased automation, and the establishment of ethical AI frameworks.

- AI-based ethical hacking will enable organizations to do:
- Detect and eliminate threats in real-time.
- Automate penetration testing and vulnerability assessments.
- Decrease dependence on manual security processes to make security operations more efficient.
- Certify ethical deployment of AI, supervising compliance with guidelines and transparency.

While a gigantic leap into the increasingly complex predicament of cyberattack, strategies has been set into motion with cybercriminals utilizing AI to launch more efficient attacks, cyber defense teams need to act proactively with AI-led cybersecurity defenses. The future of AI in ethical hacking is not just about automation and efficiency; it is about

how organizations will secure their digital assets in the face of a world that is increasingly AI-driven.

CONCLUSION

The adoption of Artificial Intelligence (AI) within ethical hacking heralds a new age of cybersecurity by making the detection of threats faster, smarter, and proactive. AI-enabled ethical hacking increases efficiency, automates processes, and promotes data-driven decision-making. Various organizations are stumbling upon ways to detect vulnerabilities and mitigate cyber threats faster and with greater precision. At the same time, while AI contributes to betterment, it also creates a host of challenging issues to be dealt with. One of the burning topical issues is the ethical aspect of AI in cybersecurity, where the biases of AI models, privacy issues due to AI misuse in surveillance, and the question of fair and accountable conduct arise. At the same time, adversarial attacks have made AI vulnerable, as in, game-like situations, in which cybercriminals manipulate AI models to breach all security measures put forth. This explains the widening skills gap and why it is harder for organizations to find professionals versed in both AI and cybersecurity. For AI-driven ethical hacking to work for the business gigs, proper employment of ethical AI development, training of the workforce, and compliance with international cybersecurity regulations need to be handled. Against the fast-evolving digital landscape of cyberattacks, the collaboration between AI and ethical hacking would be essential in the tussle to protect digital assets, build up the national security, and assure a safe and sound digital future.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Ahmed, H., Haque, M. F. U., Khan, H. R., Nadeem, G., Arshad, K., Assaleh, K., & Santos, P. C. (2024). Selecting the best compiler optimization by adopting natural language processing. *IEEE Access*.

Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

Freitas, S., Kalajdjieski, J., Gharib, A., & McCann, R. (2024). AI-Driven Guided Response for Security Operation Centers with Microsoft Copilot for Security. *arXiv preprint arXiv:2407.09017*.

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*, 2(1), 39-50.

Ismail, I. A., & Aloshi, J. M. R. (2025). Data Privacy in AI-Driven Education: An In-Depth Exploration Into the Data Privacy Concerns and Potential Solutions. In *AI Applications and Strategies in Teacher Education* (pp. 223-252). IGI Global.

Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. *Journal of Information Technology and Cyber Security*, *1*(2), 53-67.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34.

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*.

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International journal of research in business and social science*, *11*(4), 384-396.

Nadeem, G., & Anis, M. I. (2024). Investigation of bovine disease and events through machine learning models. *Pakistan Journal of Agricultural Research*, *37*(2), 102-114.

Nadeem, G., Rehman, Y., Khaliq, A., Khalid, H., & Anis, M. I. (2023, March). Artificial Intelligence based prediction system for General Medicine. In *2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-6). IEEE.

Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. *Nanotechnology Perceptions*, *20*, 332-353.

Saha, D., Mohottalalage, T., & Mailewa, A. B. Decoding the Cyber Battlefield: A Review of Threats, Tactics, and Defensive Strategies in Cyber Warfare.

Solomon, M. G., & Oriyano, S. P. (2022). *Ethical hacking: Techniques, tools, and countermeasures*. Jones & Bartlett Learning.

Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War*, *1*(1), 164-170.