AI in Cyber Security and Ethical Hacking With Advanced Penetration Testing

Jayalakshmi Jayan[1], Angel Mary George[2], Ameena Navas [3]

[1]Assistant Professor, Department of Computer Science, Santhigiri College of Computer Sciences, Vazhithala, Kerala, India, 686662

[2]Student, Department of Computer Science, Santhigiri College of Computer Sciences,Vazhithala, Kerala, India, 686662,

[3] Student, Department of Computer Science, MG University, Santhigiri College of Computer Sciences,Vazhithala, Kerala, India, 686662,

DOI: https://doi.org/10.51584/IJRIAS.2026.11100107

Received: 24 October 2026; Accepted: 29 October 2026; Published: 17 November 2026

ABSTRACT

Cyber security and Ethical Hacking are essential for various sectors like finance, healthcare, education, government, business, and technology, as they provide security for computer systems, confidential data, and networks from online attacks, whereas Ethical Hackers use legal means to provide security by preventing attacks. AI-Driven Cybersecurity and Threat Intelligence provide organizations with automatic detection and prevention of cyber threats, whereas Advanced Penetration Tests, as part of Ethical Hacking, provide organizations with security vulnerabilities that can be resolved before being attacked by hackers. Key technologies include Machine Learning, Natural Language Processing, Security Information and Event Management, Vulnerability Scanning Tools, Social Engineering, and Web Application Testing Tools.

Index Terms: CYBERSECURITY: Aritificial intelligence (AI), Machine learning (ML), Big Data Analysis, Security Information and Event Management (SIEM), Natural Language Processing (NLP), Continuous Exposure Management (CEM). ETHICAL HACKING: Vulnerability Scanning Tool, Exploitation Framework, Network scanning and mapping, Web application testing tools, Red team operating, Agentic AI & Autonomous Pen-Testing Swarms.

INTRODUCTION

Cyber security can be defined as the practice of safeguarding computer systems, networks, and data from cyber attacks and unauthorized access. Artificial Intelligence plays an important role in the practice of cyber security by detecting threats. Ethical hacking can also be related to cyber security, as it helps to identify vulnerabilities in computer systems. Penetration testing can also be related to cyber security, as it helps to improve the strength of the security system by simulating real attacks. Therefore, the practice of cyber security can be related to the modern world, as it can be related to the Indian knowledge system, which includes protection, strategy, and ethics. This study conducts a systematic literature review and theoretical evaluation of AI-enhanced penetration testing, presents a comparative framework of modern defensive and offensive toolsets, and provides actionable guidelines for enterprise compliance under current cybersecurity legislation.

Objectives of the Study

1. To study the role of artificial intelligence in cyber security, as well as advanced penetration testing in the practice of Ethical Hacking.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue X October 2026

2. AI helps to improve the strength of the security system by detecting and predicting cyber threats, which can be stopped immediately. On the other hand, advanced penetration testing helps to improve the strength of the ethically hacked system.

3. To study the challenges that arise due to the combination of defensive AI systems and the practice of ethical hacking.

METHODOLOGY

For the study, the qualitative approach of research will be adopted for the field of Cybersecurity and AI. The research papers, policy, and reports from various organizations, research studies in the field of Cyber security, were reviewed. The information collected is used to analyze the technical impact, challenges, and sustainability of the outcome.

AI Driven Cyber Security

Currently, in 2026, AI-driven cybersecurity is revolutionizing the way the defense of various sectors, such as the finance and health sectors, responds to the ever-increasing threat of highly sophisticated, high-speed, AI-powered cyber attacks. Deep learning (DL), which is a major aspect of AI-driven cybersecurity, makes use of multiple layer neural networks for the analysis of large quantities of complex data for the detection of cyber attacks in real time. Natural language processing technology enables the interaction of the individual with the technology by using their natural language, rather than the need to use programming codes. AI has been incorporated into various cybersecurity tools to make them efficient, for example, AI and cloud security solutions.

Machine Learning In Cyber Security

Machine learning in cybersecurity can be defined as the application of flexible algorithms that analyze information with the aim of identifying, predicting, and responding to various cyber threats in real-time. Machine learning plays a crucial role in improving cybersecurity detection capabilities by Processing huge volumes of information, Enhancing the speed of detection and response capabilities. Machine learning tools in cybersecurity, which improve cybersecurity through AI-powered tools such as endpoint security, network security, code security, etc.

Big Data Analysis

Big data analysis in cybersecurity can be defined as the application of huge volumes, velocity, variety, etc., with the aim of identifying, detecting, and responding to various cyber threats in real-time. This helps in transforming from reactive to proactive cybersecurity detection through machine learning, behavioral analysis, and predictive analysis of hidden and sophisticated attacks. Research on Big Data in Cybersecurity including Research Design, Data Collection, Big Data Framework Implementation, performance valuation, Result Analysis & Conclusion.

Security Information and Event Management (SIEM)

SIEM is a centralized cybersecurity solution that collects and analyzes security-related information in real time to efficiently identify cyber threats. This helps cybersecurity experts to identify cyber threats, investigate security incidents, and ensure compliance with different regulations. This is achieved through a complete understanding of the security posture of the organization. This technology is also improved through the use of AI, which increases the accuracy of cyber threats and minimizes the occurrence of alert fatigue, as well as the ability to respond to cyber threats automatically.

Natural Language Processing (NLP)

Natural Language Processing (NLP) is a technology in artificial intelligence used to process human

language, such as emails, messages, and cybersecurity reports. This technology is used in the field of cybersecurity to identify phishing emails, investigate threat intelligence, and detect suspicious text-based activities. With the use of NLP, AI, and machine learning, cyber threats are efficiently identified.

Continuous Exposure Management (CEM)

Moreover, AI also helps in improving the Continuous Exposure Management system by the intelligent use of assets, predictive prioritization of vulnerabilities, and the mitigation of risks in the digital environment. Additionally, the traditional Continuous Exposure Management system is converted into a predictive and proactive cyber risk management strategy by the use of AI, particularly in the cloud environment. The Continuous Exposure Management system also helps in improving the predictive mitigation of threats and the exploitability windows.

Global Case Studies

Journel Digital Library1: The role of AI in the detection, prevention, and response to threats is discussed in the research paper. The ethical and technological limitations of AI-based security systems are also discussed in the paper. The recommendations for the use of AI in the implementation of cybersecurity strategies are also discussed in the paper.

Journal of Computer and Mathematics Education: The accuracy of the detection system can also be increased by 98 percent by the use of AI, and the proactive role of AI in the identification of threats and the learning process.

METHODOLOGY

Ethical hacking methods such as network scanning, vulnerability assessment, web application testing, etc., are used to identify the vulnerabilities in the system. Exploitation tools are used to test the identified vulnerabilities in a controlled environment. The high-end tools for testing are simulations based on the red team approach and the use of AI-based automated tools for more efficient security testing in an ethical way.

Strengthening Security with Vulnerability Scanners

Vulnerability scanners are tools that are used to automate the discovery of vulnerabilities, misconfigurations, and security issues in the system, network, application, and cloud infrastructure before the attackers exploit them. The tasks performed by the vulnerability scanner are the detection of assets, the identification of running services and software, and the matching of the information with the vulnerability database for the assessment of risk. The best practice recommendations for the use of a vulnerability scanner are the execution of a scan, the prioritization of the critical vulnerabilities, the application of patches, retesting the infrastructure, and the use of the scanner in association with the execution of a penetration test.

Penetration Testing Exploitation Framework

An exploitation framework is a platform used by ethical hackers to test the vulnerabilities of a system. This platform provides tools for the ethical hackers to simulate various cyber attacks to test the vulnerabilities of the system. This will help the ethical hackers to test the vulnerabilities of the system in a controlled environment. The results obtained from this test will help the ethical hackers to know the vulnerabilities of the system. This is one of the practices used by ethical hackers to test the vulnerabilities of the system.

X-Ray Vision for Network

Scanning the network will give the ethical hacker an idea of the various systems, devices, and services available in the network. The network will be scanned using various tools, such as Nmap. This tool will help the ethical hacker to know the vulnerabilities of the network. The network mapping will give the ethical

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue X October 2026

hacker a visual idea of the network. This will help the ethical hacker to know the various vulnerabilities of the network.

Ensuring Web App Quality: Testing Tools and Techniques

Web app testing tools are used to ensure the quality of web applications in terms of performance, security, and functionality. The functional testing tools used for this purpose include Selenium and Cypress. These tools help the developers to work faster using automated test cases. Similarly, the performance testing tools are used to simulate high traffic for testing the stability of the system. The security tools, along with the Burp Suite, are used to identify the vulnerabilities, thus ensuring the quality of the development of high-performance web applications.

Agentic AI and Autonomous Pen-Testing Swarms

Agentic AI is used to design a cybersecurity system to perform various tasks autonomously. The various tasks performed by the cybersecurity system include reconnaissance, vulnerability scanning, exploitation, etc. The minimal involvement of human beings is required in the cybersecurity system. Similarly, the concept of autonomous pen-testing swarms involves the collaborative functioning of various AI agents to perform various tasks such as scanning, exploit testing, reporting, etc. This helps to utilize the potential of AI to the greatest extent, despite the various challenges associated with the concept of AI.

Tool / Platform	Category	Primary Features	AI/ML Capabilities	Operational Pros	Operational Cons
Nessus	Vulnerability Scanner	Asset discovery, configuration auditing, compliance checks	Static signature matching; ML threat prioritization	Extensive CVE library, highly accurate scans	High license cost, non-autonomous remediation
OpenVAS	Vulnerability Scanner	Open-source network scanning, authenticated & unauthenticated tests	Community signature updates; limited heuristic learning	Free/open-source, highly customizable	Requires manual setup, higher false-positive rate
Qualys Guard	Cloud Security / CEM	Cloud-native scanning, patch management, attack surface monitoring	AI-powered vulnerability risk scoring (TruRisk)	Scalable across hybrid clouds, continuous tracking	Bandwidth heavy during deep infrastructure scans
Metasploit Pro	Exploitation Framework	Exploit payload generation, post-exploitation modules, pivoting	Scriptable automation; integration with LLM planners	Industry standard, massive exploit database	High probability of detection by modern EDRs
Cobalt Strike	Red Team Framework	Adversary simulation, beaconing, covert post-exploitation	Custom C2 profiles; machine-assisted evasion	Realistic adversary emulation, advanced command execution	High misuse potential, costly commercial licensing
Splunk	SIEM /	Centralized log	ML Toolkit	Scalable,	High ingest

Enterprise	SOAR	ingestion, real-time alert correlation, SOAR playbooks	(MLTK) for anomaly detection & UEBA	powerful analytics, rich ecosystem	pricing, steep learning curve for SPL
IBM QRadar AI	SIEM / Threat Intel	Security intelligence, risk manager, automated root-cause analysis	Watson AI for automated incident root-cause mapping	Automated investigation, reduced alert fatigue	Complex setup, resource-intensive deployment

Red Team Operations

Red team operations are those that are used to simulate the activities of the real world in order to assess the organization's capacity to respond to the attack. However, this is different from the penetration test in the sense that the latter also includes the assessment of the humans. The process of Red Team includes reconnaissance, exploitation, and reporting, whereby the ethical hackers try to find the vulnerabilities and document them. Red Teaming is a method used in the enhancement of the organization's capacity in the field of cybersecurity.

Global Case Studies

The study discussed ethical hacking methodologies and how organizations make use of ethical hackers to enhance their security and overall cybersecurity environment. Ethical hacking is important in that it helps in the identification of vulnerabilities and security gaps in an organization's cybersecurity environment, and this enhances an organization's overall cybersecurity environment. The study showed that ethical hacking is important in enhancing an organization's security by identifying vulnerabilities, strengthening the organization's systems, and preventing cyber attacks.

Ethical hacking and penetration testing in an organization's security environment help in the protection of an organization's digital assets and enhance the overall cybersecurity environment. The study on ethical hacking and penetration testing, as discussed in the book “Ethical Hacking and Penetration Testing Guide” by Rafay Baloch (2017), discussed the overall process of ethical hacking and introduced the reader to tools such as Nmap, Nessus, Metasploit, Netcat, and BeEF.

Future Directions

The future of AI-driven cybersecurity will involve the prediction, monitoring, and response to threats in real-time to ensure that threats are prevented before they cause damage. AI systems will also learn from global threats, thus making the defenses proactive. In the context of ethical hacking, the use of AI in penetration testing will involve the simulation of complex cyberattacks, thus making them faster and more precise. Also, in the future, the use of AI in penetration testing, also known as autonomous red team testing, will involve continuous scanning of systems for vulnerabilities. Thus, the use of AI in penetration testing in the future will make cybersecurity and ethical hacking smarter, faster, and more continuous.

CONCLUSION

It can, therefore, be concluded that AI-driven technologies have the potential to transform the field of cybersecurity and penetration testing in the context of ethical hacking. AI-driven technologies are advantageous in that they make the detection of threats faster, thus allowing organizations to respond to threats in the most efficient manner. AI-driven penetration testing also allows hackers to simulate real attacks, thus making it possible for them to identify vulnerabilities of systems. Thus, AI-driven cybersecurity and penetration testing are the future of smarter, stronger, and more dynamic cybersecurity.

REFERENCES

2. NIST Special Publications: The language regarding "Integrated Ecosystems" mirrors the NIST Cybersecurity Framework (CSF) 2.0.
3. Priyant Banerjee, Arshad Bhat Eco-Tourism and Sustainable Development 1 (1), 14-26, 2025
4. Jin Wei-Kocsis, Moein Sabounchi, Gihan J Mendis, Praveen Fernando, Baijian Yang, Tonglin Zhang IEEE transactions on education 67 (3), 395-404, 2023
5. Masike Malatji, Alaa Tolah AI and Ethics 5 (2), 883-910, 2025
6. Aya H Salem, Safaa M Azzam, Omar E Emam, Amr A Abohany Journal of Big Data 11 (1), 105, 2024
7. Iqbal H Sarker, Md Hasan Furhad, Raza Nowrozy SN Computer Science 2 (3), 173, 2021
8. Digital threats: research and practice 4 (1), 1-38, 2023
9. The Journal of Defense Modeling and Simulation 19 (1), 57-106, 2022
10. Cybersecurity and Privacy in the Era of Smart Technologies, 301-324, 2026
11. Jack Reid, Donna H Rhodes Monterey, California. Naval Postgraduate School, 2018
12. J. Internet Serv. Inf. Secur. 14 (1), 195-205, 2024
13. Artificial Intelligence for Smart Technology in the Hospitality and Tourism Industry, 265-303, 2024 SN Computer Science 2 (3), 173, 2021
14. Walaa Saber Ismail J. Internet Serv. Inf. Secur. 14 (1), 195-205, 2024https://www.rapid7.com/fundamentals/siem
15. Turkish Journal of Computer and Mathematics Education (TURCOMAT) 9 (3), 10.61841, 2018
16. Selcuk Okdem, Sema Okdem Applied Sciences 14 (22), 10487, 2024
17. Fnu Jimmy, Valley International Journal Digital Library 1 (2), 564-574, 2021
18. Aryendra Dalal, Turkish Journal of Computer and Mathematics Education (TURCOMAT) 9 (3), 10.61841, 2018
19. Jean-Paul A Yaccoub, Hassan N Noura, Ola Salman, Ali Chehab arXiv preprint arXiv:2103.15072, 2021 https://arxiv.org/abs/2103.15072
20. Bogdan Barchuk Authorea Preprints, 2025 https://www.authorea.com/doi/full/10.22541/au.175312505.5835621
21. Supom Roy, Ornab Banik Journel of Computer Science and Technology Studies 7 (3), 1010-1017, 2025 https://al-kindipublishers.org/index.php/jcsts/article/view/9117
22. Avinash Reddy Aitha Deep Science Publishing, 2025 https://www.academia.edu/download/124955496/277_2.pdf
23. Deepak Bhaskar Acharya, Karthigeyan Kuppan, B Divya IEEE Access 13, 18912-18936, 2025 https://www.authorea.com/doi/full/10.22541/au.175312505.58357621