ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

The Role of Ethical Hacking and AI in Proactive Cyber Defense: Current Approaches and Future Perspectives

Mani Gopalsamy[1]; Khader Basha Dastageer[2]

[1]Independent Researcher
[2]Lead Infrastructure and Hybrid Engineer, NCS Pte Ltd.Ang mo Kio. Singapore

Publication Date: 2025/02/24

Abstract: Proactive cyber defense is becoming more reliant on ethical hacking and AI to help organizations foresee, identify, and lessen the impact of security risks. Ethical hackers simulate real-world cyberattacks, uncovering vulnerabilities in systems and networks, while AI enhances these efforts by providing real-time threat detection, anomaly analysis, and predictive insights. Advanced machine learning techniques analyze vast datasets, identifying subtle patterns and deviations that signify potential security breaches. This paper explores the synergistic integration of ethical hacking and AI, presenting current approaches, methodologies, and future opportunities for enhancing cyber defense strategies. By combining human expertise with AI's computational power, a multi-layered defense strategy is achieved to counteract the evolving threat landscape.

Keywords: *Cyber Defense, Cybersecurity, Ethical Hacking, Artificial Intelligence, Machine Learning, Proactive Threat Detection, Vulnerability Assessment, Penetration Testing.*

How to Cite: Mani Gopalsamy; Khader Basha Dastageer. (2025). The Role of Ethical Hacking and AI in Proactive Cyber Defense: Current Approaches and Future Perspectives. *International Journal of Innovative Science and Research Technology*, 10(2), 482-489. https://doi.org/10.5281/zenodo.14916984.

I. INTRODUCTION

A paradigm change has occurred in cybersecurity in recent years due to the incorporation of AI into ethical hacking techniques. The combination of these two areas has improved security in ways never seen before, particularly in the areas of threat identification and vulnerability assessment. Security measures need to be increasingly advanced and adaptable to keep up with the ever-changing cyber threats and the growing complexity of digital ecosystems [1].

Cyber defense is a system for protecting computer networks, which includes safeguarding key infrastructure, responding to attacks, and ensuring the integrity of data for businesses, governments, and other networks[2]. The goal of cyber defense is to keep data and infrastructure safe from harm by detecting and responding quickly to assaults. Cyber defense is crucial for most organizations to protect sensitive data and assets from the increasing number and sophistication of cyber-attacks [3].

Ethical hacking seeks to improve system security by discovering weaknesses from a hacker's perspective [4]. Finding and exploiting security vulnerabilities is the goal of ethical hacking.

Cyber defense gives the much-needed peace of mind to carry out procedures and operations without fear of cyberattacks. This aids in making the most efficient use of resources and boosting the security plan. The objective of cyber defense is to detect, prevent, and react swiftly to attacks and threats in order to preserve infrastructure and data [5]. Most organizations now consider defense to be critical in protecting sensitive data and assets from the ever-increasing number and sophistication of cyberattacks.

Using the same tools, methods, and strategies as hackers, ethical hackers engage in penetration testing or "white hat" hacking. The only distinction is that this kind of hacking is not illegal. Authorization from the target is required for ethical hacking[6].

Cybersecurity techniques rely on AI for proactive cyber threat assessment because hackers are always enhancing their strategies to exploit vulnerabilities in cloud settings [7]. The enormous volumes of data created in real-time inside cloud infrastructures provide a formidable challenge, but AI technologies offer a potent toolbox of ways and tools to tackle this problem. In today's digital world, where many different types of enterprises employ cloud computing, it is crucial to enhance cyber defenses to withstand advanced attacks.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

The integration of AI is causing a dramatic shift in cybersecurity measures [8]. AI provides a potent answer by facilitating data-driven, automated decision-making that improves the accuracy and speed of threat identification, leading to better cyber defense. Integrating AI into cybersecurity has several benefits, one of which is its capacity to analyze massive volumes of data in real-time.

The use of AI in ethical hacking tactics has caused a paradigm change in the cybersecurity profession in recent years[1]. Improved security posture, vulnerability assessment, and threat detection have all seen historic highs because of this integration.

- *Structure of the Paper*

The following paper is organized as follows: Section II provides the role of ethical hacking, Section III provides the leveraging AI for proactive cyber defense, Section IV defines the current approaches for ethical hacking and proactive cyber defense, and Sections V and VI provide Literature Review on this topic and Conclusion with future work.

II. THE ROLE OF ETHICAL HACKING

Since its inception, ethical hacking has seen tremendous change. Hacking as a protective mechanism has been around for a lot longer than the 1995 introduction of the phrase "ethical hacking" by IBM Vice President John Patrick [4]. Ethical hacking uncovers security vulnerabilities in a system. Instead of harming the system, ethical hackers use the same skills and technologies to expose security flaws. To protect sensitive data, ethical hackers execute pen tests to create vulnerability assessment reports for application owners to learn and respond to security vulnerabilities [9]. The term "ethical hacking" refers to a method of conducting security assessments that mimics traditional hacking methods while ensuring that the necessary credentials are obtained from the target organization. The objective is to strengthen a company's defenses against data and security breaches by copying the ideas, tactics, and methods used by cybercriminals.

A. Ethical Hackers and Their Hacking Process

A white hat ethical hacker is a hacker who uses their vulnerabilities for a noble purpose, like safeguarding an organization. In essence, the virtuous people are ethical hackers. These are legally permitted to disrupt other people's programs. Ethical hackers examine websites and ports for vulnerabilities that may be attractive to crackers. Attacks are simple once the device's vulnerabilities are identified [10]. Any user serious about staying safe in this digital realm has to educate themselves on the several entry points hackers might use to breach their network. In order to protect networks and organizations for good reasons, ethical hackers study and use hacking principles. Figure 1 depicts the five levels of ethical hacking [11].

- *Reconnaissance*
- *Maintaining Access*
- *Scanning & Enumeration*
- *Gaining Access*
- *Clearing Tracks*

Fig 1: Ethical Hacking Process

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

➢ *Reconnaissance*

It is a methodical approach to covertly collecting data about the target systems. Here, the ethical hacker follows the seven stages outlined below in an effort to learn as much as they can about the systems under attack.

- Identification of active machines
- Preliminary information collection
- Identification of every port's services
- Network mapping
- Identification of open ports & access points
- OS fingerprinting

➢ *Scanning & Enumeration*

Pen testers often employ scanning as a means to find the open door. It is possible to learn about the port's service providers' vulnerabilities via scanning. It is now necessary to ascertain the topology, operating systems, firewalls, services, intrusion detection, perimeter equipment, and physical network structure of the target organization. As a network assault, enumeration should be your main goal. As it establishes a connection with the target machine and gathers data about it, enumeration transforms into a producer.

➢ *Gaining Access*

The hackers will try to get access using tools and methods after the observation is complete and all vulnerabilities have been evaluated. The recovery of the password is the primary emphasis here. This could be accomplished by a hacker utilizing password-cracking techniques or bypass methods.

➢ *Maintaining Access*

The intruder has two options: either he keeps a low profile and continually exploits the systems without the genuine user knowing what he's doing, or he uses the systems as a springboard to test and destroy additional systems.

➢ *Clearing Tracks*

Everyone who commits a burglary wants to remain undetected; thus, they erase evidence, commonly termed erasing tracks. After an attack, the first thing to do is delete any bogus login credentials or error messages that the victim's system may have received.

B. The Key Role of Ethical Hacking in Cyber Defense

Ethical hacking is essential for proactively finding weaknesses in networks, apps, and systems so that businesses may strengthen their defenses before bad actors take advantage of them. Through the simulation of actual attack scenarios, ethical hackers provide practical insights to reduce risks and enhance security posture. Some key roles are as follows:

- **Identifying Vulnerabilities:** The goal of ethical hackers is to find security flaws in computer systems and software by using a wide range of testing methods. Methods like these include source code examination, social engineering, penetration testing, and network scanning.
- **Assessing and Prioritizing:** Risks After identifying vulnerabilities, ethical hackers evaluate and rank the dangers it provides according to variables like the possibility of exploitation and the possible influence on the company.
- **Recommending and Implementing:** Ethical hackers assess potential security flaws and then advise on and assist with the implementation of procedures to close such gaps. Some examples of such updates include new security measures, configuration tweaks, or software patches[12].

III. LEVERAGING AI FOR PROACTIVE CYBER DEFENSE

The use of AI has become standard practice across many modern businesses. The number of AI-related applications has grown in tandem with the expansion of cyber defense across several sectors. Through its promotion of automation, AI has become more and more embraced by enterprises. A primary goal of automation has been to increase output while decreasing human intervention. Data analysis and security are two areas where AI has started to actively participate [13]. Cybersecurity is becoming more concerned about data security. That the digital revolution has been getting better is what it guarantees.

A. Techniques of AI in Cyber Defense

The capacity of artificial intelligence (AI) to handle massive volumes of data, identify trends, and adapt to new threats has made it an essential component of contemporary cybersecurity measures. Below are some of the current AI techniques used in cyber defense:

- **Machine Learning (ML):** Applied to detect intrusions, spam messages, and malware because it does not require a previous categorization of a set of content. This is because ML helps systems incorporate changes into these areas and become adaptable in relation to new threats.
- **Deep Learning:** A type of ML offering enhancements to the methods of intrusion detection as well as malware categorization by employing neural networks.
- **Natural Language Processing (NLP):** The articles, news, and research are fed through NLP to generate predictive intelligence about possible threats by AI systems.
- **Automated Threat Detection:** AI ensures that risks that are usually not easily noticeable due to their concealment in normal process activities are easily detected and dealt with.
- **Pattern Recognition:** Common Artificial Intelligence systems observe and identify the least features of specific malware and ransomware in order to prevent them from executing their function.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

B. Future Opportunities of AI in Cyber Defense:

➢ *Here are some Potential Future Research Opportunities for Advancing Cyber Security [14]:*

- *Quantum Machine Learning (QML) in Cybersecurity*

A huge step forward in the fight against sophisticated cyber-attacks is the incorporation of QML into cybersecurity, especially for vital facilities. Having domain-specific quantum security protocols would allow for quicker vulnerability discovery and dynamic defense measures using QML's rapid processing capabilities [15].

- *Quantum AI (QAI) in Cybersecurity Education*

One of the most crucial efforts to stay up to date with quantum innovations is integrating QAI into cybersecurity education, particularly in software engineering degrees.

- *Neuro-Symbolic AI for Enhanced Cybersecurity*

Research into improving real-time threat detection to counter advanced adversarial strategies has shown encouraging results, thanks to neurosymbolic AI's integration of neural network pattern recognition with symbolic reasoning.

- *Deep learning for Cyber-Physical Systems Security*

When it comes to protecting cyber-physical systems (CPSs), DL is crucial for detecting intrusions in networks. Researching sophisticated DL architectures and methods, such as federated learning, to circumvent dataset limitations and improve threat detection skills can help in the development of autonomous safety models for complex CPS ecosystems, next-gen networks, and IoT infrastructures.

- *Integrating Humanized AI Insights into Cybersecurity*

Research in psychology, sociology, and law can inform the design of safe and intuitive systems. That sheds light on the whole picture of how well AI cybersecurity solutions take into account all the human elements that influence cyber interactions [16].

- *Explainable AI (XAI) in Cyber Threat Analysis*

Improving threat detection while minimizing false positives is the goal of XAI advancements in cybersecurity, which necessitates fine-tuning algorithms and assessment metrics.

IV. CURRENT APPROACHES FOR ETHICAL HACKING AND PROACTIVE CYBER DEFENSE

In this section, the focus is on the strategies and methodologies that are actively being implemented to enhance cybersecurity through ethical hacking and proactive defense mechanisms[17]. These approaches not only aim to defend against ongoing cyber threats but also anticipate and prevent potential vulnerabilities. Below are some key approaches:

A. Vulnerability Assessment:

A methodical procedure is involved in conducting vulnerability assessments and penetration tests. Assessing a system, piece of software, or network for security flaws is known as a vulnerability scan. By exploiting these vulnerabilities, an assailant may gain access to the victim's system[18]. Vulnerabilities in authentication, configuration weaknesses, input validation, boundary conditions, exception handling, and access control are among those that can affect a system[19].

B. Penetration Testing (Pen Testing):

After determining where a system is vulnerable, penetration testing can be performed. To discover potential vulnerabilities in a system, penetration testing involves trying to exploit it in an authorized way. One of the main goals of penetration testing is to identify potential security flaws in a system by actively probing it for vulnerabilities [20].

C. AI-Powered Threat Detection:

An essential component of AI-powered threat detection is the utilization of ML algorithms, which enable proactive and dynamic responses to cyber-attacks [21]. AI-driven threat detection uses algorithms that can learn from large datasets, identify trends, and adjust to new threats, as opposed to conventional methods that depend on static signatures and patterns [22].

D. Web Application Security Testing:

The purpose of a security test is to determine how well an organization's application security measures function by systematically assessing and verifying their efficacy [23]. Testing the safety of online software is the sole purpose of a web application security audit [24]. Cross-Site Scripting (XSS): Attackers can insert dangerous scripts into websites that other users view due to cross-site scripting vulnerabilities. There are three main types:

- **Stored XSS:** A server can retain malicious code indefinitely, harming any user who visits the compromised website.
- **Reflected XSS:** The harmful script is coded into a URL and runs as soon as the user clicks on the modified link.
- **DOM-based XSS:** A vulnerability lies in the Document Object Model (DOM), enabling attackers to manipulate a page's structure.

E. Bug Bounty Programs:

Individuals such as security researchers and ethical hackers can earn incentives through a crowdsourcing effort known as a bug bounty program, which is also known as a vulnerability rewards program (VRP)[10].

F. Zero Trust Architecture:

It is not possible to rely on location or any traffic in a zero-trust architecture. Alternatively, it is necessary to implement security measures for every access, implement stringent access control with minimum authorization requirements, and visualize and analyze all traffic [25].

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

G. Current Techniques of AI Used in Cyber Defense

➢ *Below are some AI Techniques that are Currently Being used for Cyber Defense[26]:*

- RBAC, or role-based access control, assigns permissions to users according to their job functions. When exceptions or violations are recorded, Benedetti and Mori suggest using AI approaches to update and maintain the access control state. Their primary focus is on streamlining the maintenance process by offering an optimal plan of action to reconfigure the RBAC state.
- A category of software solutions known as intelligent e-mail protection exists to stave against complex cyberattacks that target email specifically. As a marketing strategy, sending unsolicited emails to large lists of people was known as spamming. Unfortunately, malicious software, stolen login passwords, and financial theft are some of the current uses for it. Automated defense against harmful spam emails is being implemented using AI approaches.
- AI-powered backup solutions are becoming available to provide effective backup by backing up important data and software components based on requirements and priorities. Dynamic backup scheduling and optimized backup scheduling are accomplished through the application of AI algorithms.
- AI-driven anti-virus and anti-malware programs are able to examine thousands of files and extract valuable information that helps them be categorized as either malicious or benign. As an input to models in ANNs or RNNs, respectively, researchers have developed antivirus applications that can detect malware based on attributes obtained from executables or dynamic data analysis[27].
- AI-supported device authentication safeguards machine-to-machine connectivity by authenticating devices according to their credentials or network behavior. To guarantee the safety of cyber-physical systems and the automobile industry, researchers are putting a lot of effort into sensor authentication and identification [28].

V. LITERATURE REVIEW

The following is an overview of the literature on ethical hacking and AI in cyber defense:

In, Manoj Varshney (2023) investigates the many contributions that ethical hackers provide to the field of cybersecurity. In proactive defense, ethical hacking is essential because it finds weaknesses before malevolent actors can make use of them. In addition to saving money, this strategy improves an organization's overall security posture. Ethical hacking also aids in mitigating internal threats, raising security awareness, aiding with incident response, and maintaining regulatory compliance[29].

In, Gasmi (2024) proposes a proactive cyber defense framework that leverages the synergistic integration of Artificial Intelligence (AI), specifically evolutionary algorithms, and big data analytics to enhance early threat detection in future networks. The proposed approach utilizes evolutionary algorithms to optimize and adapt detection models continuously, enabling the system to evolve alongside emerging threats. The system is able to anticipate possible security breaches by evaluating massive volumes of heterogeneous data acquired from many network sources in real time and spotting unusual patterns. The incorporation of big data techniques facilitates the handling of high-velocity and high-volume data streams, ensuring timely and accurate threat assessment[30].

In, Istiaque et al. (2021) investigation on the efficacy of cyber defense methods using AI has been initiated. This was achieved by utilizing the KDD'99 data set's multiclass feature. Instance types such as normal, DoS, U2R, R2L, and Probe are included in this dataset. These four broad categories identify multiple forms of cyberattacks. The data set underwent thorough preprocessing prior to commencing testing in the Python lab. There are seven ML algorithms that can identify different types of cyberattacks. Low FPR, sensitivity to detection by different AI models, and good accuracy all attest to the efficacy of the cyber-defense mechanism[31].

In, Rangrez et al. (2024) examine key milestones that have shaped the modern architectures of AI-Powered Cyber Security Defender Systems throughout their historical evolution. It helps in giving a categorization of these systems and explaining how the different kinds of systems work, together with their benefits. These systems, using AI and ML, have the ability to evaluate big data, make diagnoses and counter cyber threats in networks, meaning that the general security is greatly boosted. Thus, the role of AI-Powered Cyber Security Defender Systems is highlighted throughout the research paper as being the primary generators of digital asset and user data protection[32].

In, MacHhindra et al. (2023) examine the use of predictive analytics, anomaly detection, and threat intelligence as possible ways to strengthen cyber security through the utilization of ML. ML applications provide a comprehensive strategy for detecting and reducing cyber risks. Anomaly detection techniques look for out-of-the-ordinary occurrences to help find threats in real-time, while predictive analytics use past data to foresee possible security breaches. Responsible AI practices are emphasized in this analysis, which also covers the difficulties and ethical concerns of using ML for cyber defense [33].

In, Ahmed (2023) processes and challenges inherent in information security, specifically emphasizing the tension between technological progress and data privacies. Using literature surveys, interviews and case studies, the research explores the issues of transparency, equity and ethics in AI-based cybersecurity systems. The conclusions highlight the regulatory legislation, ethical design principles, and integrated stakeholder strategy as the key levers to leverage innovation and ethically relevant factors[34].

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

Below, Table I shows the literature review summary of ethical hacking and artificial intelligence in cyber defense with different papers, methods, dataset used, their key findings and their limitations and future work.

Table 1: Literature review summary for Ethical Hacking and AI in Cyber Defense

Reference	Focus On	Approaches	Key Findings	Challenges	Limitations and Future Work
[29]	Role of ethical hacking in cybersecurity	Proactive defense, vulnerability identification	Ethical hacking enhances security posture, ensures compliance, and mitigates insider threats.	Addressing complex and evolving threats	Expanding frameworks for diverse and complex network environments.
[30]	Proactive cyber defense using AI and big data	Evolutionary algorithms, big data analytics	Enables real-time anomaly detection and prediction of security breaches.	Handling data velocity and volume	Scalability for different network configurations and dynamic security requirements.
[31]	Cyber defense mechanisms using AI	KDD'99 dataset, ML algorithms	High detection accuracy for diverse attack categories with low FPR.	Preprocessing complexity of datasets	Incorporation of more complex datasets for wider application scenarios.
[32]	Evolution of AI-powered cybersecurity systems	AI and ML for large dataset analysis	Significant enhancement in identifying patterns and responding to malicious activities.	Rapidly evolving cyber threats	Continuous development of adaptable models for future needs.
[33]	Machine learning applications in cybersecurity	Predictive analytics, anomaly detection, threat intelligence	Provides multifaceted approaches to identify and mitigate cyber threats effectively.	Ethical concerns in AI practices	Ethical deployment of ML models and addressing bias in predictive systems.
[34]	Ethical implications of AI-driven cybersecurity	Literature review, expert interviews, case studies	Highlights need for transparency, fairness, and adherence to ethical standards in AI systems.	Balancing innovation with privacy	Development of robust regulatory frameworks and collaborative approaches for ethical innovation.

VI. CONCLUSION AND FUTURE WORK

Today, cybersecurity cannot be viewed as effective without ethical hacking and artificial intelligence necessary for risk prediction and management. Ethical hacking provides organizations with the ability to identify vulnerable points in the system and address them before malicious people take advantage of them through real-world attack simulations. AI supports protection from threats, defines malicious events, and performs analytics of all data, providing better detection and reaction rates. In conjunction, these approaches provide a proactive and sustainable means of defense that is fundamental when the threat surfaces have become rapid and innovative. Despite these huge opportunities, there are issues like skill dearth, ethical issues and the increasing complexity of threats, explaining why cybersecurity is one of the fields that should be developing and improving constantly.

Future work should be devoted to enhancing the integration of more intelligent AI with cybersecurity and creating advanced intelligent systems for recognizing and eliminating new threats actively and independently. The breakthrough methods in ML, including quantum ML and neuro-symbolic learning, could provide directions for dealing with complex attacks and enhance the efficiency of cybersecurity solutions. The current methods of ethical hacking should expand on the incorporation of AI models to simulate today's fiercer threat tactics in an endeavor to derive better results for assessments. Also, there are societal probing questions such as ethical use of AI, owning BIG DATA, and compliance issues that will require solutions. Cyber-trust partners among cybersecurity professionals, AI scientists, and policymakers will be at the center of defining the anticipatory global security continuum's strategic future and the rights and wrongs it.

REFERENCES

[1]. P. K. Sambamurthy, "The Integration of Artificial Intelligence in Ethical Hacking: Revolutionizing Cybersecurity Predictive Analytics," 2024.

[2]. D. Galinec and W. Steingartner, "Combining cybersecurity and cyber defense to achieve cyber resilience," in *2017 IEEE 14th International Scientific Conference on Informatics, INFORMATICS 2017 - Proceedings*, 2017. doi: 10.1109/INFORMATICS.2017.8327227.

[3]. A. Immadisetty, S. Engineering, C. Infrastructure, D. Governance, and P. Observability, "MASTERING DATA PLATFORM DESIGN : INDUSTRY-AGNOSTIC," vol. 7, no. 2, pp. 2–5, 2024.

[4]. F. Asif, F. Sohail, Z. H. Butt, F. Nasir, and N. Asgar, "Ethical Hacking and its role in Cybersecurity : A Comprehensive Review," 1995.

[5]. D. Možnik, D. Delija, D. Tulčić, and D. Galinec, "Cybersecurity and Cyber Defense Insights: The Complementary Conceptual model of Cyber resilience," *Entren. - Enterp. Res. Innov.*, 2023, doi: 10.54820/entrenova-2023-0001.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

[6]. S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, 2018. doi: 10.1109/ICPCSI.2017.8391982.

[7]. A. Reddy and P. Reddy, "The role of Artificial Intelligence in proactive cyber threat detection in cloud environments," *NeuroQuantology*, vol. 19, no. 12, pp. 764–773, 2021, doi: 10.48047/nq.2021.19.12.NQ21280.

[8]. M. Cooper, "AI-Driven Early Threat Detection : Strengthening Cybersecurity Ecosystems with AI-Driven Early Threat Detection : Strengthening Cybersecurity Ecosystems with Proactive Cyber Defense Strategies," no. September, 2024, doi: 10.13140/RG.2.2.32615.87202.

[9]. Sivakumar Ponnusamy, "Cybersecurity and Ethical Hacking Harnessing AI," *Proc. - 2019 Int. Conf. Smart Grid Electr. Autom. ICSGEA 2019*, pp. 558–561, 2024, doi: 10.1109/ICSGEA.2019.00131.

[10]. V. KOLLURI, "A Comprehensive Analysis on Explainable and Ethical Machine: Demystifying Advances in Artificial Intelligence," *Int. Res. J.*, vol. 2, no. 7, 2015.

[11]. Fiza Abdul Hafiz Qureshi, Mayur Dube, Komal Ramteke, and Akshay Akhare, "A Review Paper on Ethical Hacking," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 11, no. 12, pp. 779–783, 2023, doi: 10.48175/ijarsct-12786.

[12]. R. C. Kurmi, N. Chaudhary, and S. Khan, "Ethical Hacking and Cyber Security : A Comprehensive Overview," vol. 11, no. 3, pp. 373–376, 2024.

[13]. B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review," *Int. J. Softw. Eng. Appl.*, 2022, doi: 10.5121/ijsea.2022.13502.

[14]. K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Front. Big Data*, vol. 7, 2024, doi: 10.3389/fdata.2024.1497535.

[15]. Venkateswaranaidu Kolluri, "A Thorough Examination of Fortifying Cyber Defenses : AI in Real Time Driving Cyber Defence Strategies Today," *JETIR - Int. J. Emerg. Technol. Innov. Res. (www. jetir. org), ISSN*, p. 32, 2016.

[16]. V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization AI for Cybersecurity Incident Investigations," *Int. J. Res. Anal. Rev.*, vol. 3, no. 3, 2016.

[17]. Mani Gopalsamy, "An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks," *Int. J. Sci. Res. Arch.*, vol. 7, no. 2, pp. 661–671, Dec. 2022, doi: 10.30574/ijsra.2022.7.2.0235.

[18]. V. Kolluri, "AN IN-DEPTH EXPLORATION OF UNVEILING VULNERABILITIES : EXPLORING A N IN - DEPTH EXPLORATION OF U NVEILING V ULNERABILITIES : E XPLORING R ISKS IN AI M ODELS AND A LGORITHMS," no. May, 2024.

[19]. J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," in *Procedia Computer Science*, 2015. doi: 10.1016/j.procs.2015.07.458.

[20]. M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," *Applied Sciences (Switzerland)*. 2023. doi: 10.3390/app13126986.

[21]. M. Gopalsamy, "AI-Driven Solutions for Detecting and Mitigating Cyber Threats on Social Media Networks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, 2023.

[22]. N. K. Et al., "AI in Cybersecurity: Threat Detection and Response with Machine Learning," *Tuijin Jishu/Journal Propuls. Technol.*, 2023, doi: 10.52783/tjjpt.v44.i3.237.

[23]. M. Aydos, Ç. Aldan, E. Coşkun, and A. Soydan, "Security testing of web applications: A systematic mapping of the literature," *Journal of King Saud University - Computer and Information Sciences*. 2022. doi: 10.1016/j.jksuci.2021.09.018.

[24]. V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," *Int. Res. J.*, vol. 11, no. 12, pp. 74–82, 2024.

[25]. R. Bishukarma, "Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1308–1319, 2023, doi: 10.48175/IJARSCT-14000S.

[26]. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, 2023, doi: 10.1016/j.inffus.2023.101804.

[27]. N. Abid, "Empowering Cybersecurity : Optimized Network Intrusion Detection Using Data Balancing and Advanced Machine Learning Models," *TIJER*, vol. 11, no. 12, 2024.

[28]. N. Abid, "A Climbing Artificial Intelligence for Threat Identification in Critical Infrastructure Cyber Security," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, 2022.

[29]. A. K. R. G. S. U. S. S. S. N. M. Manoj Varshney, "Ethical Hacking: Enhancing Cybersecurity Through Offensive Security Practices," *Tuijin Jishu/Journal Propuls. Technol.*, vol. 44, no. 4, pp. 2305–2310, 2023.

[30]. S. Gasmi, "Proactive Cyber Defense with AI : Combining Evolutionary Algorithms and Big Data for Early Threat Detection in Future Networks Proactive Cyber Defense with AI : Combining Evolutionary Algorithms and Big Data for Early Threat Detection in Future Networks," no. August, 2024, doi: 10.13140/RG.2.2.17393.49767.

[31]. S. M. Istiaque, M. T. Tahmid, A. I. Khan, Z. Al Hassan, and S. Waheed, "State-of-the-Art Artificial Intelligence Based Cyber Defense Model," in *2021 IEEE International Conference on Service*

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14916984

Operations and Logistics, and Informatics, SOLI 2021, 2021. doi: 10.1109/SOLI54607.2021.9672393.

[32]. U. S. Rangrez, S. A. Qadri, C. Ashok Kumar, and C. Jothi Kumar, "Cyber-Attack Defense System Enhanced by Artificial Intelligence," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2024, pp. 1–5. doi: 10.1109/ISCS61804.2024.10581124.

[33]. P. A. MacHhindra, B. N. Vijay, B. S. Mahendra, C. A. Rahul, P. A. Anil, and P. R. Sunil, "Enhancing Cyber Security Through Machine Learning: A Comprehensive Analysis," in *2023 4th International Conference on Computation, Automation and Knowledge Management, ICCAKM 2023*, 2023. doi: 10.1109/ICCAKM58659.2023.10449547.

[34]. M. Z. Ahmed, "Revolutionizing Cyber Defense : The Role of Artificial Intelligence in Proactive Threat Detection," vol. 09, no. 01, pp. 121–134, 2023.