Educational Administration: Theory and Practice
2024, 30(6), 251-258
ISSN: 2148-2403
https://kuey.net/

Research Article

Exploring the Impact of AI-based Honeypots on Network Security

Shyamalendu Paul[1], Amitava Podder[2*], Kaustav Roy[3], Anupama Sen[4], Anindita Chakraborty[5]

[1-,2,3,4,5]*Assistant Professor, Department of Computer Science & Engineering, Brainware University, West Bengal, India*
shyamalendupaul992@gmail.com[1], amitavapodder24@gmail.com[2], kaustroy@gmail.com[3], anupamasen2015@gmail.com[4], ani.9012@gmail.com[5]

Citation: Amitava Podder[2] , (2024), Exploring the Impact of AI-based Honeypots on Network Security, *Educational Administration: Theory and Practice*, *30*(6), 251-258, Doi: 10.53555/kuey.v30i6.5155

ARTICLE INFO **ABSTRACT**

Honeypots, utilized for detecting and deflecting unauthorized network access, have evolved with artificial intelligence advancements. This research paper covers AI-based honeypot technology in computer networking, detailing basic concepts and evolution towards AI usage. It explores AI techniques like machine learning and neural networks in honeypots, along with their advantages and limitations in network security. The paper concludes with future directions and challenges of AI-based honeypots, aiming to enhance network security and predict the role of AI in it.

Keywords: Honeypots, Artificial Intelligence, Network Security, Machine Learning, Neural Networks, Natural Language Processing.

Introduction:

In the modern tech-focused world, computer network security is incredibly important. Cybercriminals seek out weaknesses in networks to carry out damaging attacks, highlighting the need for honeypots - a tool that can intercept and detect attacks on various network resources. Honeypots aid in identifying attackers and understanding their goals and tactics. [2] [3]

Conventional honeypot methods face limitations in gathering and analyzing vast amounts of data from network attacks. The utilization of AI has revolutionized honeypots, incorporating machine learning, natural language processing, and neural networks to create advanced deceptions resembling actual computer systems. These adaptive honeypots mimic real systems and applications, offering insight into attackers' strategies and tools. [4]

The objective of this study is to present a thorough examination of AI-driven honeypot technology in computer networking. It discusses the basic principles of honeypots and AI methods like machine learning, neural networks, and NLP, as well as their advantages and drawbacks in improving network security. Furthermore, it delves into the potential of honeypots paired with AI, the obstacles, and possibilities in network security.

Literature Review:

This paper will offer a detailed literature review and an update on AI-based honeypot technology for network security, which mimics attractive targets to deter hackers. Traditional honeypots used real systems to lure attackers into a monitored environment for analysis, despite drawbacks like high costs, complex infrastructure, and visibility to hackers. AI-driven honeypot techniques have been created to enhance the detection and prevention of cyber threats. These honeypots harness machine learning algorithms to establish realistic environments that can detect attack patterns, analyze hacker actions, and predict future attacks. They are adept at identifying advanced persistent threats and zero-day exploits that conventional honeypots may overlook. [8]

The usefulness of AI-driven honeypot approaches in computer networking has been the subject of numerous studies. In order to create fictitious traffic that resembles actual network activity, Huang et al. (2021) developed a deep learning-based honeypot system that used a neural network, attaining a detection rate of 95.8%. A machine learning-driven honeypot system using the Random Forest method was created by Chen et al. (2019). It detected different cyberattacks with a 93.4% rate and identified more attack types than traditional honeypots in real-world scenarios. By automating threat detection and mitigation, AI-enabled honeypots have the potential to significantly improve computer network security. Machine learning techniques are used to build more realistic, adaptive, and accurate honeypots. Nevertheless, more investigation is required to assess these systems' performance in intricate and large-scale network settings. [5]

Honeypots in network security:

Honeypots, in general, are deceptive computer systems that are placed in the network to detect unauthorized access to resources. A honeypot 'honeypot' can be a physical device or virtual machine that appears to be a legitimate device but is, in fact, a trap for attackers. [11] [40] Honeypots can be classified based on their deployment into three categories: low-interaction, medium-interaction, and high-interaction. [30]

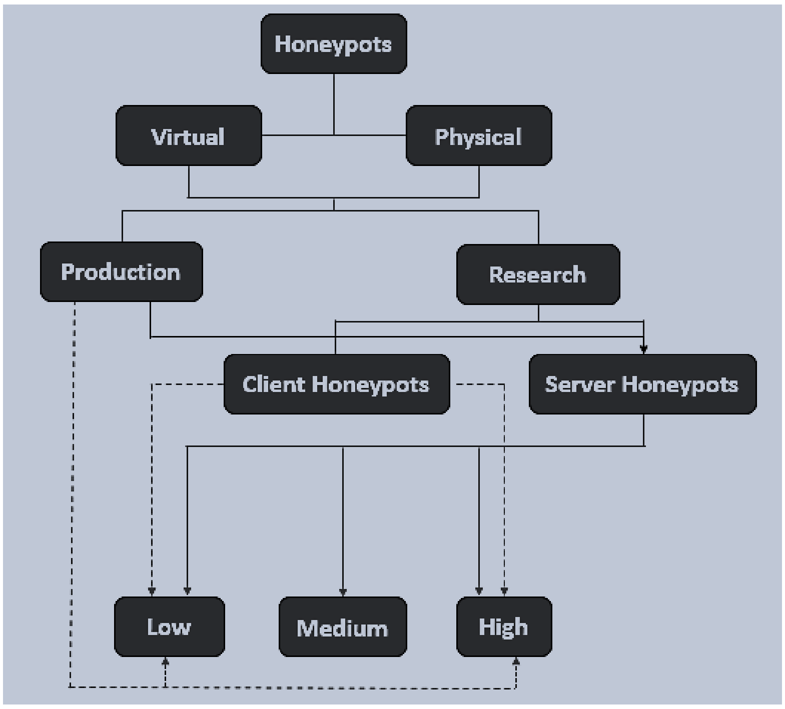

Figure 1: Types of Honeypot [38]

(i) Low-Interaction Honeypots:

A low-interaction honeypot is a security tool that detects and deflects attacks from potential hackers by emulating only a few services or protocols, creating a smaller attack surface. It is also known as a "limited interaction" honeypot due to its reduced functionality and interaction with attackers, often emulating common services like web servers, email servers, and DNS servers. [12]
A low-interaction honeypot is more resource-efficient than a high-interaction honeypot, but still effectively detects and logs attackers exploiting vulnerabilities in services. The choice between the two types depends on the organization's security needs and resources, with low-interaction honeypots being a valuable component of a comprehensive security strategy. Easy to install and with minimal maintenance, low-interaction honeypots safeguard sensitive data and are compatible with various platforms. [31]

(ii) Medium-Interaction Honeypots:

Medium Interaction Honeypots allow interaction between attackers and the environment, simulating real-world scenarios. They provide a more realistic environment for attackers to engage with, offering security analysts valuable insights into attacker methods and techniques. By replicating actual systems, applications, and protocols, attackers are forced to use exploit techniques, instead of just probing for vulnerabilities. This allows for the capture and analysis of attacker activity, aiding in understanding capabilities and motives. Medium interaction honeypots can be used to divert attackers from real systems, preventing attacks and gathering more information about attackers. However, there are associated risks with medium interaction honeypots. Despite this, the benefits of providing a realistic environment for attackers and aiding in the development of effective security measures outweigh the potential risks. [14] If intruders gain access to a honeypot, they can use it to target other systems. Honeypots are part of a larger security strategy with firewalls and other measures, not a complete cybersecurity solution. Medium interaction honeypots offer attackers a realistic setting and help security teams collect valuable information. To effectively combat cybercrime, honeypots must be managed as part of a comprehensive security approach. [15] [32]

(iii) High-Interaction Honeypots:

High-interaction honeypots are a security feature meant to ensnare hackers and thwart their intrusion into a computer network. Unlike low and medium interaction counterparts, high-interaction honeypots offer a realistic system simulation, enabling hackers to engage in typical activities. They are widely utilized in research and educational settings to scrutinize hacker behavior, detect new attack paths, and devise defense tactics. This article delves into high-interaction honeypots, their functionality, and their importance in safeguarding computer networks. [13]

High-interaction honeypots work by creating a realistic environment that simulates a real system. They may include virtual machines, hardcoded applications, and operating systems that have been modified to include security mechanisms that capture any activity performed by a hacker. The primary goal of a high-interaction honeypot is to trick a hacker into believing they have successfully infiltrated a real system. [16] After the hacker falls into the honeypot, administrators can observe their actions, gather information on their methods, and create strategies to avoid future attacks. High-interaction honeypots have an edge over other types due to their stealthiness, as they closely mimic actual systems, making it harder for hackers to identify them. [33] Administrators can enhance their awareness of hacker tactics and find new vulnerabilities with high-interaction honeypots. Such honeypots are essential for both research and practical purposes. Researchers can gather real-time data on hacker activities and evolving tactics. [17] This information helps in understanding cyber threats and creating better security measures. Practically, high-interaction honeypots help in identifying and stopping potential attacks on real systems, enabling preemptive actions to prevent damage. [36] [37]

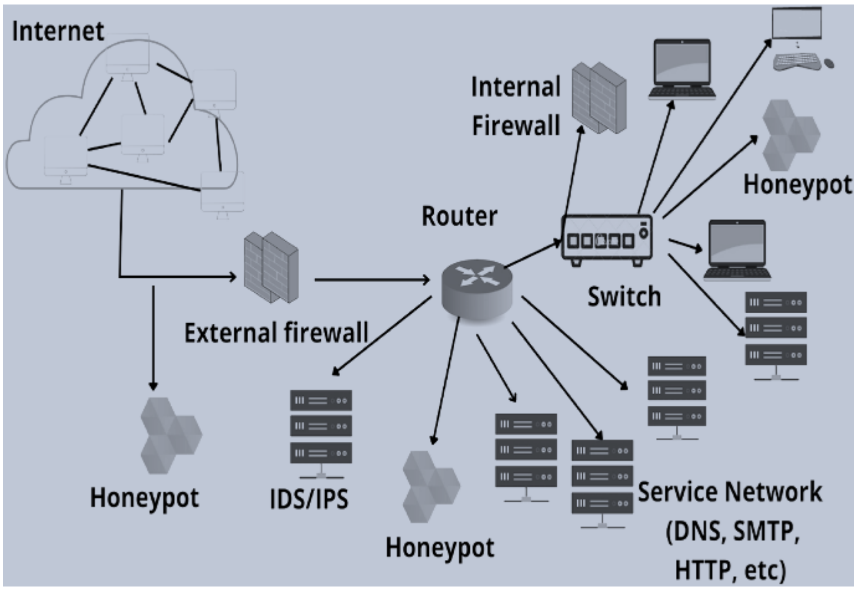

Figure 2: Honeypot for tracking attackers [41]

Artificial Intelligence in Honeypots:

(i) Machine Learning:

Machine learning (ML) is a widely used artificial intelligence approach in honeypots, enabling them to observe and adjust to attackers' tactics. ML can operate in unsupervised mode with a dataset of malicious and benign traffic, or supervised mode to categorize events on a network. [1] The honeypot can then develop a deceptive environment that can attract attackers and harvest data on the attacker's methods based on this knowledge. [6] [7]

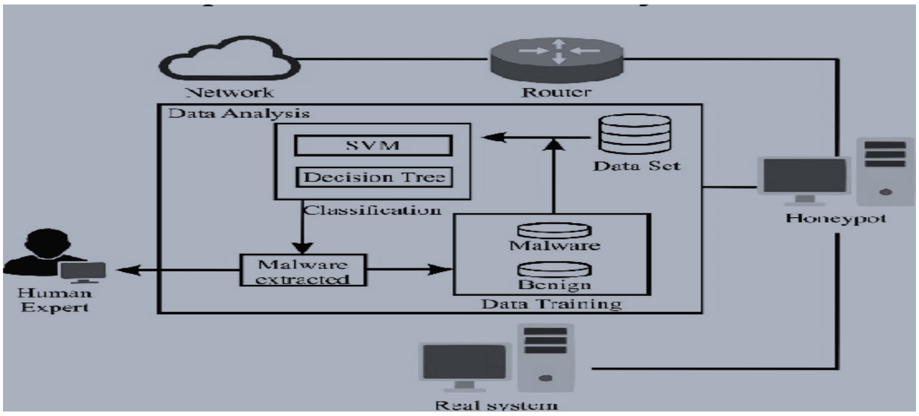

Figure 3: Machine Learning in Honeypots [39]

(ii) Neural Networks:

Honeypot technology employs different methods to lure attackers and monitor their actions for analysis and prevention. Utilizing neural networks in honeypots enhances their ability to detect and forecast attacks by studying attacker patterns and behaviors. Through analyzing data from honeypots, neural networks can recognize typical attack methods like scanning for weak ports, brute-force attacks, and command injection. This knowledge enables neural networks to improve the accuracy of detecting and predicting upcoming attacks. [19] For instance, if an intruder is seen employing a particular set of commands, the neural network can detect this pattern and flag it as a potential attack. Neural networks are also capable of scrutinizing and categorizing the information gathered from honeypots. This helps in distinguishing between valid data flow and malicious actions. Through teaching the neural network about both standard and irregular network behaviors, it can accurately spot suspicious or harmful data flow and react to stop it. Employing neural networks in honeypot technology can result in a more effective and efficient method of identifying and stopping cyber attacks. By utilizing machine learning to assess and predict attack trends, organizations can proactively safeguard their networks and resources. [18] [34]

(iii) Natural Language Processing:

NLP can improve honeypot technology by enabling it to interpret and examine the content of user interactions, aiding in the detection and prevention of novel attacks. NLP can assist in creating a more precise model of standard user behavior to identify and flag any deviations as potentially harmful. [35] For instance, NLP can help to analyze the language used in user communications with the system to establish if the communication could be considered as threatening or malicious. Furthermore, NLP can be used to analyze metadata such as the timestamps of user communications or source IP addresses, to identify unusual patterns that may indicate an ongoing attack. NLP can also be applied in detecting phishing attacks as it can analyze the content of messages sent to users from external sources for malicious intentions. [20] Another way in which NLP can enhance honeypot technology is by analyzing natural language responses to system interaction attempts by attackers to gain further insight into their behavior and motives. This data can be used to better understand the attack process and aid in developing more effective defenses against such attacks. [25]

However, there is a vital point to note that NLP technology has its own limitations- this entails that all outputs from NLP should be verified by human assessment to avoid false positives or zero-day attacks. Also, NLP models trained on limited data sets could unwittingly be biased towards certain attack patterns or miss adequately identify the ever-evolving new cyber attack patterns. [26] [27]

Benefits and Limitations of AI-Based Honeypots:

Benefits:

(i) Proactivity: AI-based honeypots are proactive in identifying and responding to security threats before a human response is necessary. They help to detect unsophisticated attacks, which is not possible with the traditional honeypot approaches.

(ii) Adaptiveness: AI-based honeypots can be programmed to adapt to changing attacker behavior and tactics that can bypass the existing security mechanisms. They can simulate an environment that mimics genuine computer systems and applications, making it difficult for the attacker to distinguish if they are interacting with a real system or a honeypot. [21]

(iii) Insight: AI-based honeypots provide insight into the attacker's actions and behavior, including the tools and methods used for the attack, the attacker's identity, and the attacker's motive.

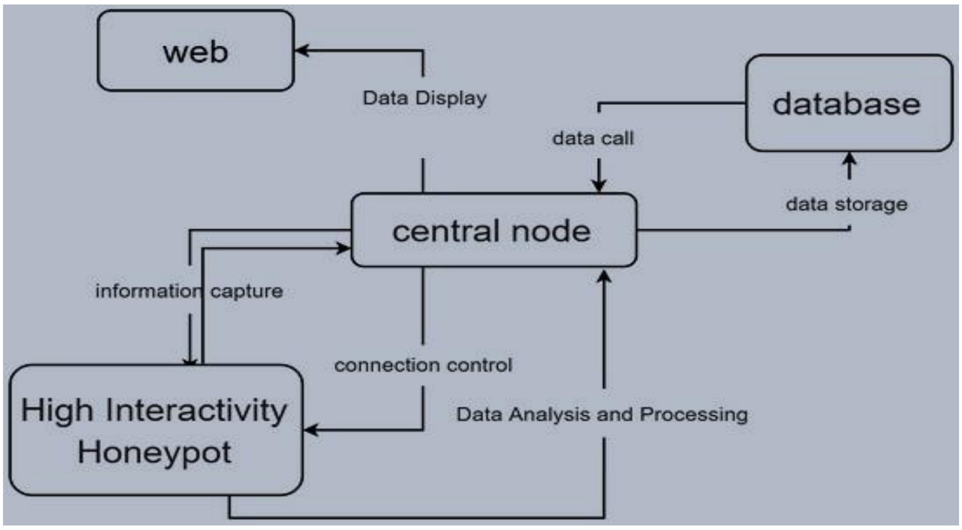

Figure 4: honeypot system framework [42]

Limitations:

(i) **Cost:** The cost of implementing and maintaining an AI-based honeypot can be high since it requires advanced hardware, software, and network resources, which require skilled personnel trained in artificial intelligence, networking, and security.

(ii) False Positives: AI-based honeypots are vulnerable to false positives, which can occur when the honeypot technology triggers an alert for benign traffic or legitimate user activity.

(iii) Privacy: AI-based honeypots record all network traffic passing through the honeypot, which poses potential privacy concerns since personal or sensitive data can be captured and stored.

Future Direction of AI-based Honeypots:

(i) Improved Detection: AI technologies are likely to be developed to improve detection accuracy and take action in real-time to prevent potential attacks successfully.

(ii) Cloud-Based Honeypots: Cloud-based honeypot technology assists organizations in detecting and handling cyber-attacks more effectively by setting up controlled systems to attract cybercriminals and uncover their methods. This technology replicates vulnerable internet-facing systems, applications, and protocols, allowing security teams to learn about attack techniques and motives. The rise of cloud-based honeypots is driven by the need for organizations to cope with complex cyber threats cost-effectively. Unlike traditional honeypots needing specific hardware and software, cloud-based ones use virtualization to deploy multiple honeypots on cloud servers, improving their detection evasion. Moreover, they can be easily adjusted in size to counter varying cyber threats. [9] Cloud-based honeypots offer the benefit of being accessible and monitored worldwide through a web interface, allowing security teams to manage data remotely. Data collected includes detailed logs of attacker interactions, IP addresses, malware payloads, and commands issued, helping identify patterns for proactive defense. These honeypots can integrate with IDS and SIEM platforms for enhanced cybersecurity. [10] Integrations can speed up incident response times by automating cyber threat identification and response. In order to identify and stop cyberattacks, cloud-based honeypots are crucial. They work by mimicking weak points in systems to record attacker activity and provide information about new and developing threats. The use of cloud-based honeypots is anticipated to rise and become an essential component of cybersecurity tactics as cyber attacks become more sophisticated.
[23]

(iii) Quantum-Based Honeypots: Quantum-based honeypot technologies utilize quantum mechanics to identify and prevent cyber attacks, leveraging distinct properties like entanglement, superposition, and measurement for improved security. We will explore the benefits, limitations, and potential of these advanced technologies in protecting computer networks and sensitive data. [22][45] Quantum-based honeypot technologies have a key advantage in detecting attacks that traditional honeypots might miss. Traditional honeypots depend on known attack signatures, while quantum-based ones use quantum encryption and communication protocols to detect new attack forms. This allows them to offer better protection against zero-day attacks by leveraging quantum cryptography for secure communication channels. Additionally, they can enhance security by using decoy data to distract cybercriminals from real information, reducing the risk of sensitive data exposure. Although beneficial, quantum-based honeypots face challenges such as high costs for implementation due to the need for costly hardware and skilled experts. [24][44] Therefore, not every organization can afford to implement this technology as their sole cybersecurity measure. Furthermore, quantum-based honeypot technologies are susceptible to quantum hacking, where hackers with quantum computers can breach these systems and render them useless. This underscores the importance of continuously improving security measures to outpace cybercriminal tactics. While quantum-based honeypot technologies have the potential to transform cybersecurity, it is crucial to consider their limitations and costs before adoption.

(iv) IoT Honeypots: IoT honeypot technology involves linking devices via the Internet of Things to establish a setup for identifying and stopping cyber-attacks. Honeypots are systems crafted to entice attackers, enabling cybersecurity experts to analyze their tactics. [28] IoT honeypots attract attackers using devices like security cameras and smart thermostats, mimicking real environments to help detect and prevent assaults due to the heightened cyber threats posed by the growing number of insecure IoT devices. [29][43] Using real IoT devices, honeypots can simulate authentic situations that are hard to replicate in traditional honeypots, aiding security professionals in pinpointing security weaknesses and enhancing measures. IoT honeypots come in two types: low-interaction and high-interaction. The former imitates a few services to quickly detect and block threats, while high-interaction mimics entire systems for in-depth insight into attackers' tactics but requires more resources and expertise to set up. Apart from thwarting cyber-attacks, IoT honeypots also gather intel on attackers by analyzing their methods and motives. Challenges with IoT honeypots include maintaining secrecy from attackers, as discovery could lead to further attacks or halt attempts, hindering data collection. Additionally, the abundance of IoT devices in a network makes monitoring and analyzing all activities challenging. However, these honeypots are valuable in combating IoT device cyber-attacks by creating realistic attack scenarios to prevent harm. Care must be taken to keep the honeypot hidden from attackers and to monitor and analyze all activity for valuable information.

Proposed Implementations for Artificial Intelligence-Based Honeypots Technology:

(i). Reinforcement Learning-Based Honeypots:

Reinforcement learning algorithms can be used to create honeypots that adapt and evolve over time. These honeypots can use algorithms such as Q-learning to learn from their past experiences and optimize their deception techniques. The mathematical expression for Q-learning can be represented as:

$$Q(s,a) = (1-\alpha) * Q(s,a) + \alpha * [R(s,a) + \gamma * \max(Q(s',a'))]$$

Where:
- Q(s,a): the estimated value of taking action a in state s
- α: the learning rate i.e. $(0 < \alpha < 1)$
- R(s,a): the reward received for taking action a in state s
- γ: the discount factor $(0 < \gamma < 1)$
- max(Q(s',a')): the maximum estimated value from all possible actions a' in state s'

By using this mathematical expression, the honeypot can learn from its interactions with potential attackers and improve its ability to detect and respond to malicious activity.

(ii). Deep Learning-Based Honeypots:

Deep learning techniques, such as neural networks, can be used to create honeypots that are capable of detecting and preventing attacks in real time. These honeypots can be trained on a dataset of known attacks and then use this knowledge to identify and respond to new threats. The mathematical expression for a neural network can be represented as:

$y = f(W * x + b)$

Where:
- y: output of the neural network
- f: the activation function
- W: the weight matrix
- x: the input vector
- b: the bias vector

By training a neural network on a dataset of known attacks, the honeypot can use this mathematical expression to classify incoming network traffic as either benign or malicious.

(iii). Markov Decision Process-Based Honeypots:

MDPs are a tool for developing honeypots that can adapt and respond strategically to threats by analyzing the system's state. The mathematical formulation of an MDP is a way to depict this process.

V(s) = max_aΣ_s' T(s,a,s')[R(s,a,s') + γV(s')]

Where:
- V(s): value function for state s
- T(s,a,s'): the transition function for taking action a in state s and moving to state s'
- R(s,a,s'): the reward received for taking action a in state s and moving to state s'
- γ: discount factor $(0 < \gamma < 1)$

By using this mathematical expression, the honeypot can optimize its responses to ensure that it is effectively deceiving and deterring attackers.

Conclusion:

A review of the development of honeypots, current developments in AI-based honeypot technology, and their advantages and disadvantages in terms of network security were the goals of this survey article. The study discovered that by imitating genuine systems to entice attackers, AI-based honeypots are successful in identifying and evaluating risks. Though they have certain limitations, such price and false positives, AI-based honeypots provide insightful information on how attackers operate. They are anticipated to be essential to network security as AI technology advances.

References:

1. Munjanja and T. de Smedt, "Machine learning based honeypot systems: A review and taxonomy," Journalof Computer Security, vol. 25, no. 2, pp. 147-165, 2017.
2. N. Anand, S. Bhatia, and R. Bhatia, "Artificial intelligence-basedintrusion detection system using honeypots in computer networks," International Journal of Computer Networks and Communications Security, vol. 8, no. 3, pp. 76-86, 2020.

3. M. Jaimes and M. Nascimento, "A classification of honeypots and their use for detecting network attacks," Journal of Information Security, vol. 7, no. 3, pp. 160-175, 2016.
4. R. Khadka, S. Bagale, and S. Raut, "AI-based honeypot for intrusion detection in wireless sensor networks," Journal of Wireless Communications and Mobile Computing, vol. 2019, Article ID 9329498, 9 pages, 2019.
5. V. Gupta, "Honeypots: A review of the evolution of deception-based cyber security," Journal of Network and Cybersecurity, vol. 1, no. 1-2, pp. 1-14, 2016.
6. Y. Jin and A. Lpez-Presa, "A machine learning approach for honeypot-based intrusion detection," Expert Systems with Applications, vol. 42, no. 8, pp. 3863-3874, 2015.
7. D. Kim, M. Kang, and H. Lim, "Using machine learning for detecting advanced persistent threats in honeypot-based environments," Journal of Intelligent Information Systems, vol. 51, no. 2, pp. 193-214, 2018.
8. P. Kelkar, A. S. Nair, and T. Anantharaman, "AI-based honeypots for preventing cyber-attacks in IoT," International Journal of Computer Applications, vol. 181, no. 19, pp. 29-35, 2018.
9. S. Khatkar and N. Singh, "Honeypot-based techniques for detecting and preventing cyber attacks: A survey," International Journal of Computer Applications, vol. 82, no. 15, pp. 37-42, 2013.

A. M. Mahrous and M. A. Mostafa, "Honeypots in cloud computing: A review," Journal of Cloud Computing, vol. 8, no. 1, pp. 1-18, 2019.

10. N. Negi, "An artificial intelligence based approach for honeypot deployment and network security," International Journal of Informatics and Communication Technology, vol. 5, no. 1, pp. 42-50, 2018.
11. S. Nigam, S. R. Pandey, and S. Singh, "Using AI for honeypot-based intrusion detection and prevention," International Journal of Scientific & Engineering Research, vol. 8, no. 2, pp. 952-956, 2017.

A. M. Odeh and A. H. Odeh, "Design and implementation of a hybrid honeypot and IDS for detecting and preventing cyber-attacks," Journal of Security Engineering, vol. 14, no. 6, pp. 431-441, 2017.

B. Pal, "A survey of honeypot systems," International Journal of Information Technology and Computer Science, vol. 6, no. 6, pp. 49-56, 2014.

12. G. Wang and G. Wang, "AI-based honeypot system deployment for network security," Journal of Computer Networks and Communications, vol. 2018, Article ID 5182070, 7 pages, 2018.
13. Wu and Y. Huang, "An effective intrusion detection system based on honeypots and random forest algorithm," Journal of Information Security, vol. 9, no. 1, pp. 17-27, 2018.
14. S. Xu and J. Wu, "AI-based honeypot for detecting network attacks," International Journal of Communication Networks and Distributed Systems, vol. 20, no. 1, pp. 76-84, 2018.
15. R. K. Yadav, R. Pandey, and S. K. Singh, "Artificial intelligence-based honeypot systems for cyber security: A review," Wireless Personal Communications, vol. 104, no. 1, pp. 51-75, 2019.
16. Y. Yang, X. Zhang, and H. Li, "A deep learning-based honeypot framework for network security," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 6, pp. 2271-2282, 2020.
17. R. A. Manteufel and S. H. Gogoi, "A survey on honeypot technology and its different applications," International Journal of Cyber-Security and Digital Forensics, vol. 9, no. 2, pp. 69-81, 2020.
18. Y. Li and Z. Qi, "A novel IoT honeypot system based on artificial intelligence," Journal of Wireless Communications and Mobile Computing, vol. 2020, Article ID 1736340, 11 pages, 2020.
19. J. Li, J. Zeng, and L. Chen, "A survey on honeypot technology and intrusion detection system," International Journal of Security and Its Applications, vol. 13, no. 6, pp. 75-85, 2019.
20. K. S. N. Usha and H. V. Ravindra, "Machine learning-based honeypot for intrusion detection in cloud security," International Journal of Computational Intelligence and Information Security, vol. 7, no. 6, pp. 63-71, 2016.
21. S. Venugopal and S. Vaidya, "A comprehensive review of honeypot systems in cyber security," Journal of Computer Engineering and Information Technology, vol. 6, no. 1, pp. 1-11, 2017.
22. Y. Wang, J. Liu, and J. Wu, "Applying deep learning to honeypot-based intrusion detection," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 4, pp. 1525-1538, 2019.
23. Zhang, "Research on artificial intelligence-based honeypot system," Journal of Intelligent & Fuzzy Systems, vol. 38, no. 2, pp. 1771-1779, 2020.
24. Y. Zhang and H. Duan, "A hybrid malware detection approach based on honeypots and machine learning algorithms," Journal of Cyber Security and Mobility, vol. 7, no. 1, pp. 1-17, 2019.
25. L. Zhao and G. Li, "Using machine learning to optimize honeypot deployments for cyber security," Journal of Cyber Security Technology, vol. 3, no. 1-2, pp. 67-79, 2019.
26. Amitava Podder, Shyamalendu Paul, 2023. Recent Trends of Artificial Intelligence in the Internet of Things ESP Journal of Engineering & Technology Advancements 3(2): 101-109.
27. T. de Smedt and W. Dooms, "A survey of honeypot systems," Journal of Computer Security, vol. 14, no. 1, pp. 13-32, 2006.
28. S. Deshpande and A. Bhise, "Honeypot technology for detecting and preventing network attacks," International Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 4504-4507, 2014.

29. R. Goyal and A. Shekhawat, "A review on honeypots in cyber security," International Journal of Research in Engineering and Technology, vol. 6, no. 4, pp. 11-15, 2017.
30. J. H. Ho, "AI-based cyber defense and its implications," Journal of Forensic Sciences, vol. 65, no. 4, pp. 1096-1106, 2020.
31. L. T. Hwang, S. L. Lin, and K. C. Wang, "A honeynet-based intrusion detection system," International Journal of Network Security, vol. 4, no. 1, pp. 47-55, 2007.
32. Q. Jiang and S. Wang, "Machine learning-based intrusion detection system with hybrid sampling and feature selection for Chinese honeypot data," Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 2, pp. 731-746, 2018.
33. Kataria, "A review of honeypot technology and its effectiveness in cyber security," International Journal of Computer Science and Engineering, vol. 8, no. 3, pp. 89-100, 2020.
34. aul, S. and Podder, A. (2023) A detailed investigation of Artificial Intelligence in Cyber Security, IJESI. Available at: http://www.ijesi.org/Vol12-issue6.html (Accessed: 2023).
35. Vishwakarma, R., & Jain, A. (2020, January 1). A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks | Semantic Scholar. A Honeypot With Machine Learning Based Detection Framework for Defending IoT Based Botnet DDoS Attacks | Semantic Scholar. https://www.semanticscholar.org/paper/A-Honeypot-with-Machine-Learning-based-Detection-Vishwakarma-Jain/ba7c825afaca953187f3fde60a3c2fe0ad7048a1
36. Industrial Honeypots | INCIBE-CERT | INCIBE. (n.d.). Industrial Honeypots | INCIBE-CERT | INCIBE. https://www.incibe.es/en/incibe-cert/blog/industrial-honeypots
37. Paul, S. and Podder, A. (2023b) AI based Computer Network Security, IJCRT. Available at: https://ijcrt.org/viewfull.php?&p_id=IJCRT2306691 (Accessed: 2023).
38. Devi Priya, V. S., & Chakkaravarthy, S. S. (2023, January 25). Containerized cloud-based honeypot deception for tracking attackers - Scientific Reports. Nature. https://doi.org/10.1038/s41598-023-28613-0
39. Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., & Zhao, J. (2023, March 28). A Highly Interactive Honeypot-Based Approach to Network Threat Management. MDPI. https://doi.org/10.3390/fi15040127
40. Dewangan, O., & Sarkar, P. (2022). MACHINE LEARNING & DEEP LEARNING APPLICATIONS. Futuristic Trends in Information Technology, 69-76.
41. Dewangan, O., & Sarkar, P. (2022). A Study on Network Security Using Deep Learning Methods. Advanced Engineering Science, 54(02), 6393 – 6404.
42. Sarkar, S. K., Podder, A., & Roy, P. An Analysis of the Privacy and Security Related Problem with Social Networks. ESP Journal of Engineering and Technology Advancements (ESP-JETA), 3(4), 37-43, (2023).