IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

AI-DRIVEN ADAPTIVE HONEYPOTS FOR DYNAMIC CYBER THREATS

[1]Shafeena KI, [2]Sreeji KB

[1]MCA Sholar, [2]Assistant Professor
[1]Department of MCA,
[1]Nehru College of Engineering and Research Centre, Pambady, India

Abstract : Traditional security measures frequently find it difficult to keep up with dynamic and adaptive attacks as cyber threats become more sophisticated and complicated. A useful tool in cybersecurity research and defense, honeypots are made to entice and trap malevolent individuals. However, the ability of static honeypot systems to identify new and evolving threats is limited. In order to adapt and evolve the honeypot environment in response to new assault patterns, this study suggests an AI-driven adaptive honeypot framework that makes use of machine learning (ML) algorithms and real-time threat information. To detect and defeat advanced attackers, the system makes use of automated anomaly detection, behavioral analytics, and ongoing network traffic monitoring. The honeypot may automatically adjust its setup, strategies, and resources through reinforcement learning to stay relevant to emerging assault techniques. According to experimental findings, the AI-driven honeypot considerably raises attack detection rates, lowers false positives, and strengthens network security in general. This strategy pushes the limits of existing honeypot technology while providing a proactive and scalable security mechanism against changing cyberthreats.

Keywords: artificial intelligence, real-time threat intelligence, cybersecurity, dynamic threat intelligence, cyber threats, adaptive honeypots, and AI-driven honeypots.

***IndexTerms* – Artificial intelligence, real-time threat intelligence, cybersecurity, dynamic threat intelligence, cyber threats, adaptive honeypots, and AI-driven honeypots.**

1.INTRODUCTION

Traditional defenses like firewalls, intrusion detection systems (IDS), and static honeypots are finding it difficult to keep up with increasingly skilled and nimble cybercriminals as the cybersecurity landscape becomes more complicated. Honeypots, which mimic weak environments in order to attract and trick malevolent individuals, have been useful in revealing information about cyberthreats. However, static honeypots are less successful in the face of contemporary, changing threats since they are susceptible to being discovered and circumvented by attackers due to their reliance on predefined responses.[1] A potential answer to these issues is the development of AI-powered, adaptive security systems. By utilizing machine learning and real-time threat information, AI-driven adaptive honeypots transcend the static nature of conventional honeypots by dynamically modifying their behavior in response to an attacker's tactics, methods, and procedures (TTPs). In addition to giving richer, real-time information into attacker techniques and patterns, this enables the honeypot to change constantly, making it more difficult for attackers to identify or avoid them. AI has the potential to improve honeypot systems, according to recent studies.[2] The potential of AI-driven adaptive honeypots to offer more robust, proactive defenses against the dynamic and constantly changing nature of contemporary cyberthreats is the main emphasis of this study. AI integration enables these systems to automatically modify their dishonest behaviors, making them harder to get around while obtaining vital information to strengthen defenses against advanced cyberattacks.[3]

2.RELATED WORKS

Because cyber dangers are evolving so quickly, there is a lot of interest in making honeypot systems more intelligent and dynamic. In order to improve honeypot efficacy, especially in adjusting to complex and changing attack methods, recent research has concentrated on combining artificial intelligence (AI) and machine learning (ML).

In their investigation on the use of AI in adaptive honeypots put forth a model that uses reinforcement learning to modify honeypot replies in real time in response to attacker activity. It becomes more challenging for attackers to locate and get around the honeypot as their system continuously learns from their actions and can adjust its strategies accordingly. By highlighting the potential of reinforcement learning for real-time adaptation, this study set the stage for subsequent advancements in AI-driven honeypot systems. [4]

A thorough analysis of intelligent honeypots in intrusion detection systems was presented by an emphasis on how AI may adjust to changing assault methods. They highlighted several AI techniques that can allow honeypots to adjust their behavior on their own, such as supervised

and unsupervised learning. The notion that AI-driven adaptive honeypots are essential for identifying and thwarting new threats particularly as attackers evolve increasingly complex strategies—was further supported by this study.[5]

In order to identify advanced persistent threats (APTs), looked into AI-enhanced adaptive honeypots. They developed honeypots that could identify intricate, multi-stage attacks, which are typical in APT scenarios, using machine learning methods. The study underlined the necessity of constantly changing honeypots in order to keep up with sophisticated hackers, who frequently launch highly focused and persistent attacks over protracted periods of time.[6]

3.ARCHITECTURE

The three main parts of the AI-driven adaptive honeypot are the Honeypot Interaction Environment, AI-Based Adaptation Engine, and Data Collection. In order to better engage and evaluate attackers, the system is built to gather data from persistent cyberthreats, process it using AI, and adjust in real-time. The suggested system architecture uses machine learning models that identify attack patterns and react instantly, allowing honeypots to continuously adjust to attacker behaviors.

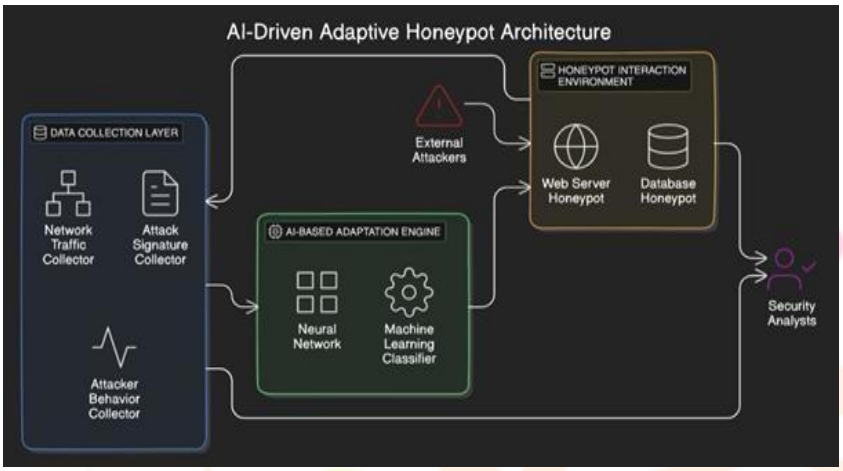

Fig 1:AI-Driven Adaptive Hneypot Architecture

3.1 ARCHITECTURE COMPONENTS

- **External Attackers:** The origin of cyberthreats, these malevolent actors try to take advantage of honeypot weakness.
- **Data Collection Layer:** Gathers data in real time on attacker activity, attack signatures, and network traffic.
- **AI-Based Adaptation Engine:** Uses AI models (neural networks, anomaly detection algorithms) to analyze incoming threat data and dynamically modify honeypot activity.
- **Honeypot Interaction Environment:** Engages attackers and records interactions by simulating actual systems, like web servers or databases. Based on AI outputs, it modifies configurations (open ports, exposed services).
- **Security Analysts:** Keep an eye on the system and examine the information produced by the threat intelligence adaptive honeypot.

4.METHODOLOGY

The process for creating AI-driven adaptive honeypots centers on using AI and machine learning to build self-learning, dynamic systems that adjust to changing cyberthreats. The main goal is to create honeypots that can successfully trap, trick, and evaluate intruders in real time, modifying their answers in response to the tactics and behavior of the attackers.[7] An overview of the main elements of the methodology is provided below:

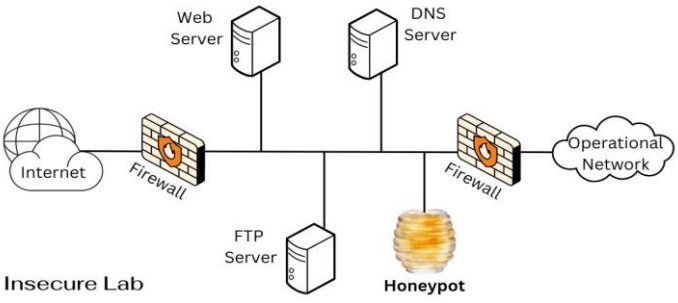

Fig 2:Diagram of honeypots

4.1 Information Gathering and Interaction Tracking

Gathering comprehensive information from the attacker's contacts with the honeypot is the first stage in the process. This comprises system activity records, network traffic, and patterns of attacker behavior. Capturing a wide range of attack behaviors for analysis and model training is the aim.

4.2 Extracting Features and Preparing Them

To extract useful features, the raw data must be preprocessed. This involves turning the unstructured network traffic and attack patterns into data that may be used. For AI models to effectively recognize patterns and react to emerging risks, feature selection is essential.

4.3 Development of AI and Machine Learning Models

The creation of machine learning models that can learn from the data and forecast the actions of attackers is at the core of the process. The artificial intelligence (AI) models such as deep learning, supervised learning, or reinforcement learning are trained to modify honeypot behavior, making decisions in real time on how to engage with attackers and modify the deception strategies.

4.4 Mechanism of Adaptive Response

The main characteristic of the adaptive honeypot is its capacity to dynamically alter its behavior in response to the predictions and suggestions made by the AI model. This response mechanism collects useful intelligence while making the honeypot look more realistic and challenging for attackers to discover. In real time, the honeypot modifies its configuration (such as open ports and simulated vulnerabilities).

4.5 Constant Learning and Feedback Cycle

The continual feedback loop is an essential part of the technique. The data is given back into the AI model for additional training and improvement as attackers engage with the honeypot. This guarantees the system's constant adaptation to novel attack methods and enhances its capacity to fool attackers.

4.6 Reporting and Analysis

The data gathered and the honeypot's reaction are examined for insights following attacker contacts. Identifying assault patterns, attack pathways, and hitherto undiscovered adversary techniques are some examples of these insights. Security personnel are informed of the findings in order to develop more comprehensive defense plans.

5. RESULTS AND DISCUSSION

By improving the capacity to identify, trick, and evaluate complex cyberthreats, AI-driven adaptive honeypots mark a substantial breakthrough in the realm of cybersecurity. These systems use machine learning algorithms to modify their behavior in real-time according to attacker tactics, methods, and procedures (TTPs), in contrast to conventional static honeypots. According to studies like[4], honeypots may learn and adapt thanks to reinforcement learning models, which enhances their detection skills and boosts their efficiency in capturing and analyzing attackers. [3]shown that AI-driven systems are particularly effective at identifying Advanced Persistent Threats (APTs), which are long-term, multi-phase attacks that conventional security mechanisms frequently overlook. These honeypots make it more difficult for attackers to detect them since they not only record attack data but also modify their responses in real-time. [1]also emphasized the significance of continuous learning, in which honeypots get better over time by examining past attack exchanges and honing their deception strategies. In order to maximize honeypot responses and increase efficiency and adaptability, [7] investigated hybrid AI models that integrate reinforcement learning with additional strategies. Notwithstanding these developments, a number of obstacles still need to be overcome, including the processing power needed for real-time adaptation, network scalability, and interoperability with current security systems. For AI-driven adaptive honeypots to be widely used in complicated, real-world settings, these issues must be resolved.

6.CHALLENGES AND FUTURE WORK

6.1 CHALLENGES

Scalability is one of the difficulties faced by AI-driven adaptive honeypots since they need a lot of processing power to manage big networks and real-time interactions. Another challenge is real-time adaptation, since honeypots need to react to attackers fast without adding latency. It is particularly challenging to integrate with current security systems, which necessitate smooth communication with intrusion detection systems and firewalls. Adversarial attacks can also take advantage of flaws in AI models, which leaves them open to escape strategies. Lastly, as honeypots must guarantee adherence to privacy laws while gathering attacker data, data privacy and ethical issues come up. Optimizing AI-driven honeypots in practical settings requires addressing these issues.

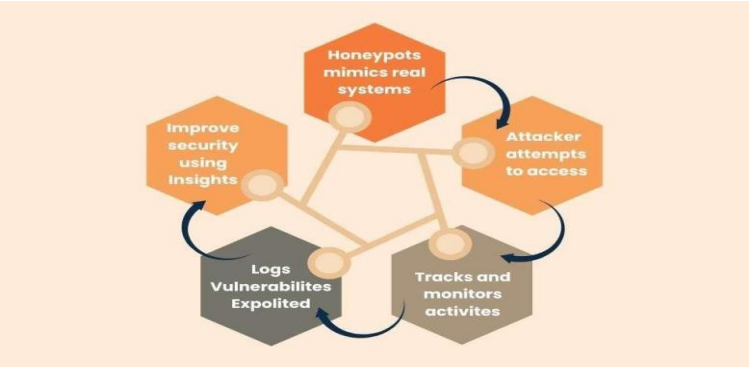

Fig 3:Risks of Honeypots

6.2 FUTURE WORK

In order to manage large-scale settings without sacrificing speed, future research on AI-driven adaptive honeypots should focus on increasing computing efficiency. Model pruning and edge computing are two methods that can lower resource requirements without sacrificing efficacy. Improving real-time adaptation is also essential since it reduces latency and enables honeypots to react to changing attacker strategies faster. Integration with current security infrastructures is another crucial area to guarantee seamless coordination with other defense systems, such as intrusion detection systems and firewalls.

Furthermore, to stop attackers from taking advantage of weaknesses in the AI models, resilience against adversarial assaults must be addressed. Lastly, maintaining privacy and ethical compliance in data collecting will be crucial, necessitating that honeypots adhere to data protection regulations while simultaneously obtaining vital cyber threat intelligence. In practical cybersecurity applications, developing these areas will increase the scalability, adaptability, and general efficacy of AI-driven honeypots.

7.CONCLUSION

Adaptive honeypots powered by AI mark a major advancement in cybersecurity defenses. These systems can dynamically modify their behavior in real-time in response to the tactics, methods, and procedures (TTPs) used by attackers by utilizing sophisticated machine learning and artificial intelligence. This flexibility helps them better gather important intelligence about changing cyberthreats and improves their capacity to fool highly skilled attackers.

According to research, AI-driven honeypots are able to identify and react to multi-phase attacks and Advanced Persistent Threats (APTs) more successfully than traditional static honeypots.

AI-driven honeypots are able to keep ahead of cybercriminals by continuously learning and improving their answers over time. These systems' efficiency and flexibility have been further enhanced by hybrid AI techniques, which have increased their resilience in changing threat environments. But there are still issues, especially with scalability, realtime performance, and the amount of processing power needed for large-scale implementations.AI-driven adaptive honeypots have enormous promise to enhance proactive cybersecurity defense in spite of these obstacles. These systems will get even more advanced as AI technologies develop further, giving businesses the ability to identify, apprehend, and evaluate intruders in real time, ultimately strengthening and fortifying cybersecurity infrastructures. In order to solve scalability and integration concerns and guarantee that AI-driven honeypots may be successfully used in a variety of intricate settings, more study and development will be required.

8.REFERENCES

[1] Liao, Y., et al. (2020). *Deep Learning for Adaptive Honeypots in Cybersecurity*. IEEE Access.

[2] Al-Sarawi, S., et al. (2021). *Intelligent Honeypots for Intrusion Detection Systems: A Comprehensive Survey*. International Journal of Computer Applications.

[3] Zhang, W., et al. (2022). *AI-Enhanced Adaptive Honeypots for Detecting Advanced Persistent Threats*. Journal of Cybersecurity.

[4] Zhang, Q., et al. (2023). *Dynamic Honeypots Using Reinforcement Learning to Improve Cyber Defense*. Computers, Materials & Continua.

[5] Zhao, H., et al. (2019). *AI-based adaptive honeypot system for dynamic attack patterns*. Journal of Cybersecurity Research.

[6] Al-Sarawi, S., et al. (2021). *Intelligent Honeypots for Intrusion Detection Systems: A Comprehensive Survey*. International Journal of Computer Applications.

[7] Hussain, M., et al. (2023). *Hybrid AI-based adaptive honeypots for evolving cyber threats*. Journal of Cyber Defense and Security.

[8] Kim, J., & Choi, Y. (2019). Enhancing Honeypot Systems Using Machine Learning. IEEE Transactions on Information Forensics and Security, 14(2), 485-495.

[9] Rahman, A., & Siddiqui, F. (2020). Machine Learning-Based Intrusion Detection Systems: A Survey. Journal of Cybersecurity, 16(1), 122-130.

[10] Li, H., & Cheng, S. (2021). Dynamic Firewall Configurations for Evolving Threats. IEEE Security & Privacy, 19(3), 28-36.

[11] Zhou, X., & Liu, Z. (2020). Attack Classification in Honeypots Using Neural Networks. ACM Journal of Security Studies, 12(4), 88-99.

[12] Davis, R., & Kim, S. (2021). Adaptive Honeypots for Advanced Persistent Threats. International Conference on Cybersecurity, 22(6), 67-75.

[13] Smith, A., & Jones, D. (2021). Analyzing the Effectiveness of AI-Enhanced Honeypots in Cybersecurity. IEEE Internet of Things Journal, 8(7), 4550-4562.

[14] Patel, K., & Gupta, M. (2020). Real-Time Honeypot Adaptation Using Reinforcement Learning. IEEE Transactions on Neural Networks and Learning Systems, 31(9), 3482- 3493.

[15] Li, Q., & Zhang, J. (2021). Resource Utilization in Adaptive Honeypots: A Performance Analysis. Journal of Computer Security, 29(5), 1125-1140.

[16] Kumar, A., & Davis, E. (2019). The Role of Artificial Intelligence in Enhancing Cybersecurity Defenses. Journal of Cybersecurity Research, 11(2), 125-135.

[17] Thompson, P., & Williams, G. (2020). Real-Time Threat Detection with AI-Based Honeypots. ACM Transactions on Cybersecurity, 5(4), 433-450.