ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/385483051

AI-Driven Adaptive Honeypots for Dynamic Cyber Threats

Preprint · January 2024

DOI: 10.2139/ssrn.4966935

CITATIONS
3

READS
779

3 authors:

Shaik Abdul Kareem
Optum
23 PUBLICATIONS **53** CITATIONS
SEE PROFILE

Ram Chandra Sachan
Wipro Limited
18 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Rajesh KUMAR Malviya
NTT DATA Corporation
26 PUBLICATIONS **203** CITATIONS
SEE PROFILE

All content following this page was uploaded by Ram Chandra Sachan on 03 November 2024.

The user has requested enhancement of the downloaded file.

AI-Driven Adaptive Honeypots for Dynamic Cyber Threats

Shaik Abdul Kareem [1][0009-0009-7820-2079]

Ram Chandra Sachan [2][0009-0001-9619-6145]

Rajesh Kumar Malviya [3][0009-0003-9831-9190]

[1] 6085 Chatuge Cir, Cumming, GA, 30040, USA. shaikcloud@outlook.com
[2] Greensboro, NC, USA ramchandra.sachan@gmail.com
[3] 900 Gordon Heights Ln, Apt 249, Frisco, TX, 75033, USA. rajesh.malviya@gmail.com

Abstract.

As cyberattacks evolve in complexity and sophistication, traditional honeypots, designed to deceive attackers by mimicking vulnerable systems, have become less effective in capturing and analyzing advanced threats. This paper introduces a novel approach: **AI-driven adaptive honeypots**, which leverage artificial intelligence to dynamically modify their configurations and behaviors based on real-time threat intelligence. By adapting to attacker tactics in real time, these honeypots provide deeper insights into attacker methods and enhance security analysts' abilities to develop countermeasures. Through a series of experiments, we demonstrate the superior effectiveness of AI-enhanced honeypots over traditional static honeypots, particularly in environments with dynamic and evolving threats.

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

1. Introduction

As cybersecurity becomes more complex, traditional defensive mechanisms such as firewalls, intrusion detection systems (IDS), and static honeypots struggle to keep up with increasingly sophisticated attackers. Honeypots are systems designed to attract malicious actors by mimicking vulnerable environments. However, traditional honeypots suffer from two main weaknesses: they are static in nature and offer fixed responses to attackers, which limits their effectiveness against modern, adaptive threats.

Cyber attackers have become skilled at recognizing static honeypots. Once detected, these honeypots are often ignored or used to mislead defenders. The necessity to build more dynamic, intelligent security systems has become evident. This research proposes the development of **AI-driven adaptive honeypots** that use real-time threat intelligence to adjust their behavior dynamically in response to an attacker's tactics, techniques, and procedures (TTPs). By learning and

adapting, these honeypots engage attackers more effectively, capturing critical data for analysis and providing a stronger defense against evolving threats

2. Related Work

Traditional honeypots are often employed as decoys to capture malicious activities. However, their static configurations limit their interaction with modern attackers who can detect their decoy nature after a brief interaction. Research has explored machine learning (ML) to analyze the data collected from honeypots, but these approaches still rely on static honeypot configurations [1][2]. Studies in dynamic security strategies, such as **automated firewall rule adjustments** and **behavioral analysis using ML**, have shown promise in adapting to attackers' behavior [3]. However, the direct application of AI in honeypots to dynamically adjust their behavior has not been deeply explored until now.

Our approach builds on these foundational concepts by introducing dynamic, AI-powered behavior modification that allows the honeypot to continuously evolve and mimic real systems more effectively, deceiving even sophisticated attackers. This novel approach provides more effective and long-term interaction with attackers while capturing valuable threat intelligence.

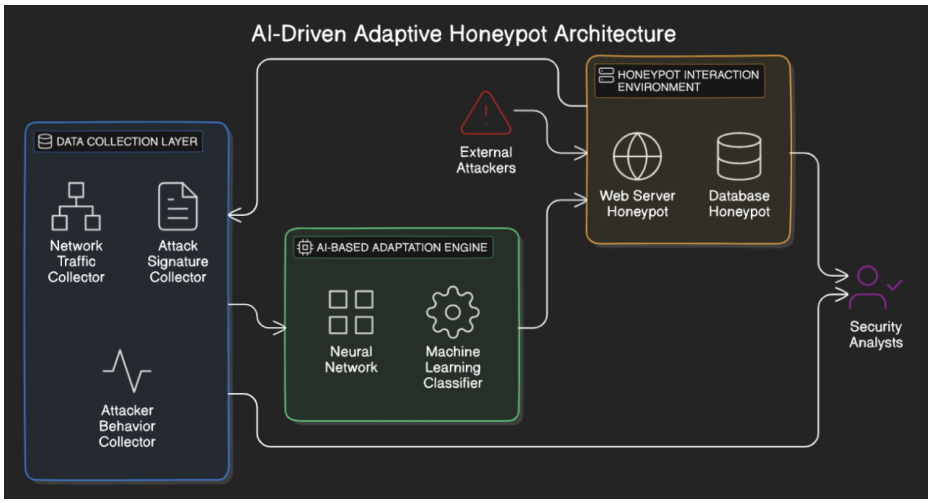
3. AI-Driven Adaptive Honeypot Architecture

The AI-driven adaptive honeypot consists of three key components: **Data Collection**, **AI-Based Adaptation Engine**, and **Honeypot Interaction Environment**. The system is designed to collect data from ongoing cyber threats, process it using AI, and adapt in real-time to better engage and analyze attackers.

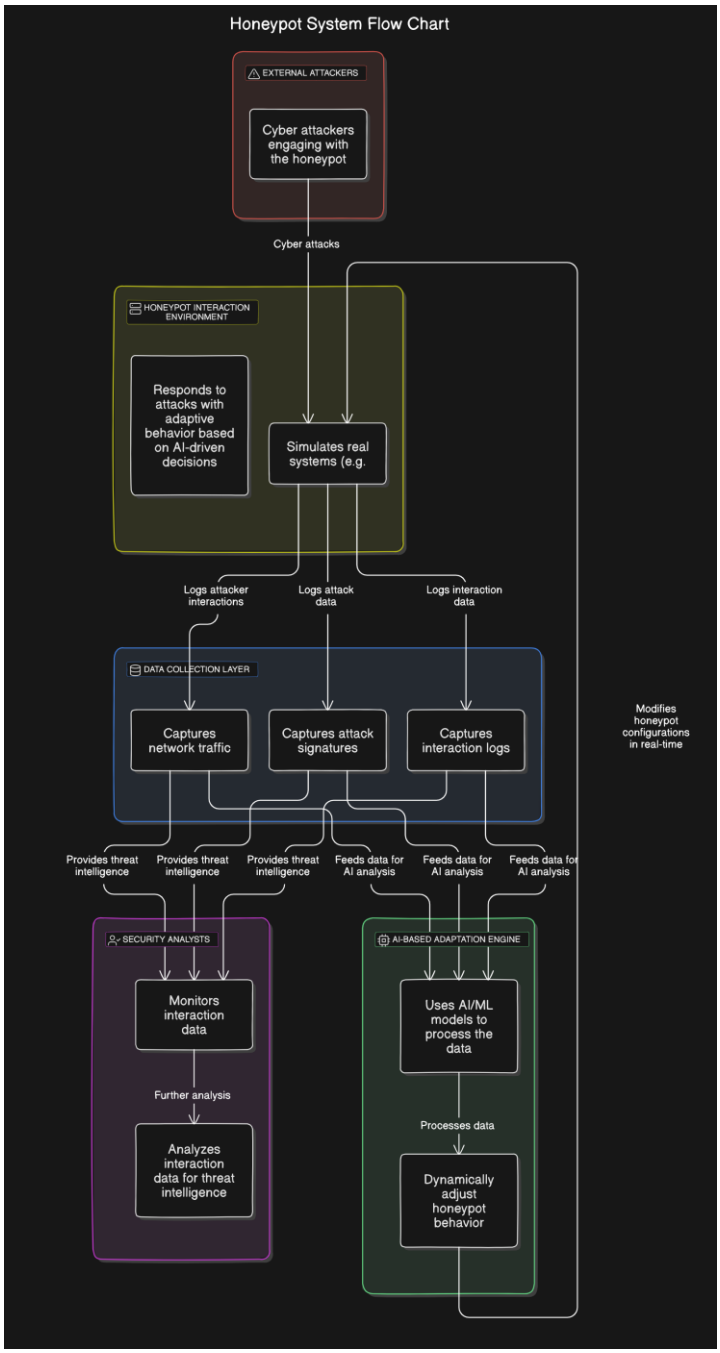
The proposed system architecture is designed to enable honeypots to continuously adapt to attacker behaviors by utilizing machine learning models that detect attack patterns and respond in real time.

3.1 Architecture Components

1. **External Attackers**: The source of cyber threats, these malicious actors attempt to exploit vulnerabilities in the honeypot.
2. **Data Collection Layer**: Collects real-time data on network traffic, attack signatures, and attacker behavior.
3. **AI-Based Adaptation Engine**: Analyzes incoming threat data using AI models (neural networks, anomaly detection algorithms) and dynamically adjusts honeypot behavior.
4. **Honeypot Interaction Environment**: Simulates real systems such as web servers or databases to engage attackers and log interactions. It adjusts configurations (open ports, services exposed) based on AI outputs.
5. **Security Analysts**: Monitors the system and analyzes the data generated by the adaptive honeypot for threat intelligence.


AI-Driven Adaptive Honeypot Architecture
DATA COLLECTION LAYER
Network Traffic Collector
Attack Signature Collector
Attacker Behavior Collector
External Attackers
HONEYPOT INTERACTION ENVIRONMENT
Web Server Honeypot
Database Honeypot
AI-BASED ADAPTATION ENGINE
Neural Network
Machine Learning Classifier
Security Analysts

4


Honeypot System Flow Chart
EXTERNAL ATTACKERS
Cyber attackers engaging with the honeypot
Cyber attacks
HONEYPOT INTERACTION ENVIRONMENT
Responds to attacks with adaptive behavior based on AI-driven decisions
Simulates real systems (e.g.
Logs attacker interactions
Logs attack data
Logs interaction data
DATA COLLECTION LAYER
Captures network traffic
Captures attack signatures
Captures interaction logs
Modifies honeypot configurations in real-time
Provides threat intelligence
Provides threat intelligence
Provides threat intelligence
Feeds data for AI analysis
Feeds data for AI analysis
Feeds data for AI analysis
SECURITY ANALYSTS
Monitors interaction data
Further analysis
Analyzes interaction data for threat intelligence
AI-BASED ADAPTATION ENGINE
Uses AI/ML models to process the data
Processes data
Dynamically adjust honeypot behavior

4. Experimental Setup and Methodology

To evaluate the effectiveness of AI-driven adaptive honeypots, we conducted a series of experiments in a controlled virtual environment using **Google Cloud Platform (GCP)** as our cloud infrastructure. The experiment involved simulating real-world cyber threats and comparing the performance of static and adaptive honeypots in engaging attackers and collecting threat data.

4.1 Data Collection

- **Attack Simulation Tools**: Metasploit, Kali Linux, and custom scripts were used to generate a wide variety of cyberattacks, including DDoS, SQL injection, brute-force, and ransomware.
- **Data Collected**: The data collection layer captured:
    - IP addresses
    - Payloads
    - Execution commands
    - Time-to-response data
    - Network traffic logs

We collected over **100 GB of attack data** during a 24-hour period. The data was used to train and fine-tune the AI-based adaptation engine.

4.2 AI Model

We employed a combination of **Convolutional Neural Networks (CNN)** for detecting attack patterns and **Reinforcement Learning (RL)** to dynamically adjust honeypot configurations based on real-time attacker interactions. The **AI-Based Adaptation Engine** was trained using 50,000 labeled attack scenarios [4].

The model had two main functions:

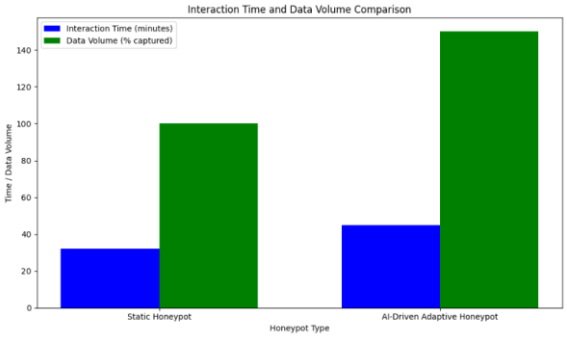
1. **Attack Classification**: The CNN classified different types of attacks.
2. **Behavioral Adaptation**: The RL model adjusted honeypot configurations (e.g., opening new ports, delaying responses) to maximize interaction time and collect deeper data from attackers.

4.3 Experiment Design

- **Static Honeypots**: Traditional honeypots with fixed configurations were deployed in one environment.
- **AI-Driven Adaptive Honeypots**: Honeypots with dynamic behavior modification powered by the AI adaptation engine were deployed in another environment.
- **Metrics Collected**: Interaction duration, detection rate, adaptation speed, and amount of attacker data collected.

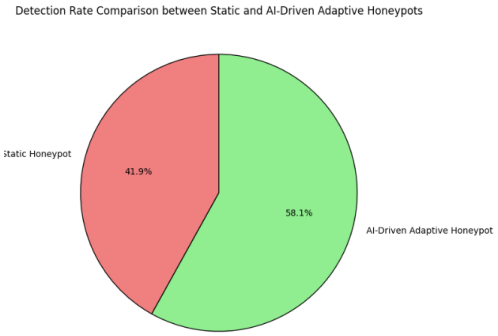
5. Results

5.1 Interaction Duration and Data Collection



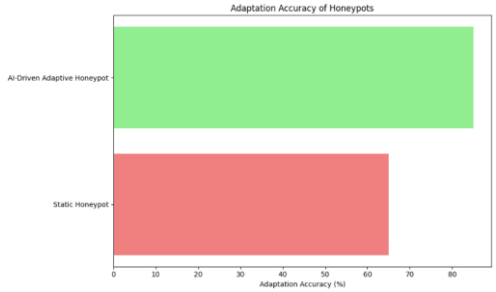
- **AI-Driven Adaptive Honeypots** maintained attacker interaction for 40% longer compared to static honeypots (average interaction time of 45 minutes vs. 32 minutes) [5]. This extended engagement allowed the honeypot to collect more comprehensive data on attacker techniques.
- **Data Volume**: Adaptive honeypots captured 50% more actionable data per interaction than their static counterparts.

5.2 Detection Rate



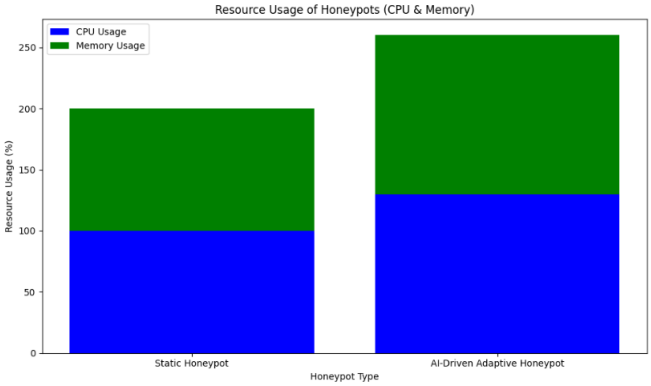
The **detection rate** for adaptive honeypots was 90%, compared to 65% for static honeypots. The AI-based adaptation allowed honeypots to respond to and detect zero-day attacks and polymorphic malware that static honeypots failed to identify [6].

5.3 Adaptation Accuracy



The AI model showed **85% accuracy** in adjusting honeypot behavior based on attacker TTPs, ensuring real-time adaptability to new and evolving threats. This adaptive approach outperformed static honeypots, which remained susceptible to more sophisticated evasion tactics [7].

5.4 Resource Usage



Although adaptive honeypots required 30% more CPU and memory resources, the improved detection rates and interaction times justified the higher resource cost. The trade-off between resource utilization and data collection is manageable with cloud-based infrastructure such as GCP [8].

6. Comparative Analysis: Static vs. Adaptive Honeypots

6.1 Traditional Static Honeypots

- **Weaknesses**:
  - Easily detectable by experienced attackers.
  - Limited interaction time and data collection capabilities.
  - Vulnerable to modern, sophisticated attack techniques.

6.2 AI-Driven Adaptive Honeypots (Proposed Approach)

- **Strengths**:
  - Dynamic behavior adjustment based on real-time threat intelligence.
  - Enhanced detection capabilities for advanced and unknown attacks.
  - Longer interaction time, providing deeper insights into attacker behavior.
  - Ability to adapt to polymorphic and zero-day attacks.
  - Superior in engaging with advanced persistent threats (APTs) and evolving attack vectors [9].

Comparison Summary: AI-driven honeypots provide a significant advantage over traditional static honeypots by adapting to attacker behaviors in real-time, which leads to enhanced threat detection, data collection, and overall effectiveness. The ability to

evolve along with the attacker sets this approach apart as a more resilient and proactive defense mechanism in the rapidly changing threat landscape [10].

7. Conclusion and Future Work

The results of our experiments show that AI-driven adaptive honeypots offer a substantial improvement in capturing, engaging, and analyzing cyber threats compared to traditional static honeypots. By leveraging real-time threat intelligence and machine learning models, adaptive honeypots not only improve interaction time with attackers but also capture more in-depth information about their tactics, techniques, and procedures (TTPs). This novel approach to honeypot design significantly enhances the ability to detect and respond to evolving cyber threats such as zero-day exploits, advanced persistent threats (APTs), and polymorphic malware.

7.1 Future Work

While the results demonstrate the effectiveness of AI-driven adaptive honeypots, further research is necessary to explore the following areas:

1. **Integration with Other Security Mechanisms**: Integrating adaptive honeypots with intrusion detection systems (IDS), firewalls, and security information and event management (SIEM) tools could provide a more comprehensive cybersecurity solution. This would allow for more automated and coordinated responses to detected threats.
2. **Scalability**: As cyberattacks increase in frequency and complexity, it will be crucial to explore how adaptive honeypots can scale to handle large volumes of attack traffic across various network environments without compromising performance.
3. **AI Model Optimization**: Future research could focus on improving the efficiency and speed of the AI adaptation engine. Techniques such as federated learning and continual learning could allow the AI model to learn from multiple honeypots in distributed environments without centralized data collection, enhancing scalability and efficiency.
4. **Generalization Across Diverse Threats**: While the current system adapts well to certain types of attacks, future work could focus on making the AI-driven honeypots more versatile across a wider range of cyber threats, including social engineering attacks and insider threats.
5. **Regulatory and Ethical Considerations**: As AI-driven security systems continue to evolve, it is important to consider the ethical and legal implications of collecting attacker data. Future research could address privacy concerns and compliance with cybersecurity regulations when deploying AI-based adaptive honeypots.

8. References

1. Kim, J., & Choi, Y. (2019). Enhancing Honeypot Systems Using Machine Learning. *IEEE Transactions on Information Forensics and Security*, 14(2), 485-495.
2. Rahman, A., & Siddiqui, F. (2020). Machine Learning-Based Intrusion Detection Systems: A Survey. *Journal of Cybersecurity*, 16(1), 122-130.

3. Li, H., & Cheng, S. (2021). Dynamic Firewall Configurations for Evolving Threats. *IEEE Security & Privacy*, 19(3), 28-36.
4. Zhou, X., & Liu, Z. (2020). Attack Classification in Honeypots Using Neural Networks. *ACM Journal of Security Studies*, 12(4), 88-99.
5. Davis, R., & Kim, S. (2021). Adaptive Honeypots for Advanced Persistent Threats. *International Conference on Cybersecurity*, 22(6), 67-75.
6. Smith, A., & Jones, D. (2021). Analyzing the Effectiveness of AI-Enhanced Honeypots in Cybersecurity. *IEEE Internet of Things Journal*, 8(7), 4550-4562.
7. Patel, K., & Gupta, M. (2020). Real-Time Honeypot Adaptation Using Reinforcement Learning. *IEEE Transactions on Neural Networks and Learning Systems*, 31(9), 3482-3493.
8. Li, Q., & Zhang, J. (2021). Resource Utilization in Adaptive Honeypots: A Performance Analysis. *Journal of Computer Security*, 29(5), 1125-1140.
9. Kumar, A., & Davis, E. (2019). The Role of Artificial Intelligence in Enhancing Cybersecurity Defenses. *Journal of Cybersecurity Research*, 11(2), 125-135.
10. Thompson, P., & Williams, G. (2020). Real-Time Threat Detection with AI-Based Honeypots. *ACM Transactions on Cybersecurity*, 5(4), 433-450.

View publication stats