AI Driven Cloud Honeypot Network

Prof. Shilpa Vishwabhramha[1], Vaishnavi Chavan[2], Yuvraj Dudhal[3], Aniket Patil[4], Akash Wavhal[5]
Department of Computer Engineering
PDEA's College of Engineering Manjri Bk
Pune
84vschavan@gmail.com[1] , dudhalyuvraj@gmail.com[2], ap575819@gmail.com [3] ,wavhalakash44@gmail.com[4]

Abstract – This study presents the development and implementation of an intelligent cloud-based honeypot system designed to enhance cybersecurity through advanced threat detection and analysis. The proposed system uses machine learning algorithms to create a dynamic deception environment that attracts, captures, and analyses malicious activities targeting cloud infrastructure. The system architecture integrates containerized honeypot deployment with comprehensive data collection and analysis capabilities. By utilizing cloud-native services and scalable infrastructure, the honeypot maintains realistic system emulation while ensuring proper isolation from production environments. The research addresses critical challenges in cloud security by providing organizations with actionable threat intelligence and early warning capabilities. The adaptive nature of the system allows continuous learning from attacker behaviour, improving detection effectiveness over time while minimizing false positives.

Keywords—Cybersecurity, Artificial Intelligence, Cloud, Honeypot, Virtual machines

I. INTRODUCTION

Traditional security measures often struggle to keep pace with the dynamic nature of cloud environments. Honeypots have emerged as valuable cybersecurity tools that act as decoy systems to attract, detect, and analyze malicious activities while gathering intelligence about attacker behaviour. However, deploying effective honeypots in cloud environments requires addressing unique challenges including scalability, integration with cloud services, cost management, and maintaining realistic deception. This project develops an intelligent cloud honeypot system that combines traditional deception techniques with artificial intelligence to create an adaptive mechanism.

II. LITERATURE SURVEY

1. The research paper uses Hybrid intrusion detection system combining artificial neural networks (ANN) with honeypot intelligence. The hybrid intrusion detection system combining ANN with honeypot intelligence provides intelligent threat classification with 98.09% accuracy while using honeypots to collect real attack data for continuous learning. It uses Apache Flink for real-time big data processing instead of the traditional batch processing. The hybrid system automatically redirects threats to honeypots while protecting actual systems, enabling both deception-based security and real-time pattern recognition. The project provides real-time processing capabilities and scalable solutions for big data environments with precise attack filtering capabilities. The MQTT Honeypot integrated with Decision and Redirection Engines are used for intelligent traffic filtering and automated threat management which enhances the security.

2. The study presents a comparative analysis of seven honeypot systems (Dionaea, Cowrie, Honeyd, Kippo, Amun, Glastopf, and Thug). It evaluates them by detection range, scalability, reliability, and data integrity. The research proposes a structured framework for assessing honeypots and recommends machine learning and cloud integration for adaptive detection.

3. This paper introduces AI-driven adaptive honeypots as a novel solution for capturing and analyzing advanced cyber threats that bypass less-effective traditional static honeypots. These systems use artificial intelligence to dynamically modify their configurations and behaviors based on real-time threat intelligence. By adapting to attacker tactics in real time, they provide deeper insights into attacker methods and enhance security analysts' ability to develop countermeasures. Experiments demonstrate their superior effectiveness, especially against dynamic and evolving threats.

4. This research introduces an approach to enhance Honeypot systems using the Apache Spark Big Data technique. Honeypots are designed to be compromised to lure and study invaders, but they can be obtuse and sluggish. By integrating Apache Spark, which is known for its speed and ability to process large-scale data quickly, the proposed system aims to improve network security utilization and processing speed. This change would also reduce the number of physical Honeypots needed, saving cost and finance.

5. The paper proposes a Particle Swarm Optimization (PSO)-based method for detecting malicious hubs and determining the cluster head in a Wireless Sensor Network (WSN). The goal is to select a high-potential node as the group leader while simultaneously detecting and removing malicious nodes. This strategy enhances energy proficiency and prevents rogue nodes from becoming the cluster head.

6. This paper presents a systematic review of honeypot data collection, threat intelligence sharing platforms, and the application of AI/ML in cybersecurity. Honeypots (ranging from low to high interaction) are analyzed for effectiveness in capturing attacker behavior and generating actionable threat intelligence. Collaborative threat intelligence frameworks like MISP and STIX are examined for facilitating data sharing. AI techniques, including deep learning and large language models (LLMs), are explored for their potential to improve honeypot performance and real-time anomaly detection. The findings emphasize the transformative potential of integrating AI with honeypots and

threat intelligence to create adaptive, automated, and resilient cybersecurity solutions

7. This article proposes a High-Interaction Honeypot system using Docker containers for detecting network-level and host-level attacks. The system uses open-source tools to ensure it is scalable, dynamic, and secure. It was tested in a real environment and proved effective in capturing malicious data for subsequent analysis using tools like VirusTotal. This solution aims to create more robust, harder-to-detect honeypots compared to easily bypassed low interaction systems.

8. This paper explores how honeypots enhance Network Intrusion Detection Systems (NIDS) by acting as deception-based tools that attract attackers and collect intelligence on their behavior. It provides a detailed review of honeypot classifications, integrations, and implementation challenges, emphasizing their use in modern cybersecurity and IoT environments

9. This research explores AI-powered honeypots as a transformative solution to combat sophisticated cyber threats that bypass traditional security. Traditional, static honeypots have limitations in detecting advanced persistent threats (APTs), automated botnets, and adaptive adversarial tactics. AI-powered systems use machine learning, behavioral analytics, and automated response to dynamically adapt to evolving threats, improve attack attribution, and provide real-time threat intelligence. The findings suggest AI-driven deception technologies offer significant improvements in identifying and neutralizing sophisticated cyber adversaries

III. PROBLEM STATEMENT

Traditional honeypot systems in cloud environments suffer from several critical limitations that reduce their effectiveness against modern cyber threats. Static rule-based detection mechanisms cannot adapt to new attack patterns, resulting in high false positive rates and limited threat intelligence generation.

IV. PROPOSED SYSTEM

Based on the flowchart diagram provided, this appears to be a comprehensive workflow for an **AI-powered cloud honeypot system** that combines cybersecurity monitoring with machine learning analytics. The system begins by listening on multiple ports (2222, 4080, 2121) to capture incoming connection attempts and session metadata including IP addresses, ports, payloads, and timestamps. All captured data is logged locally in honeypot_log.txt files for persistence. The workflow then branches into two parallel processing paths: real-time machine learning analysis and log accumulation. Logs are preprocessed to extract relevant features and stored in a structured dataset for training purposes. The system employs an autoencoder/LSTM/RF (Random Forest) model that undergoes scheduled training cycles to improve anomaly detection capabilities.

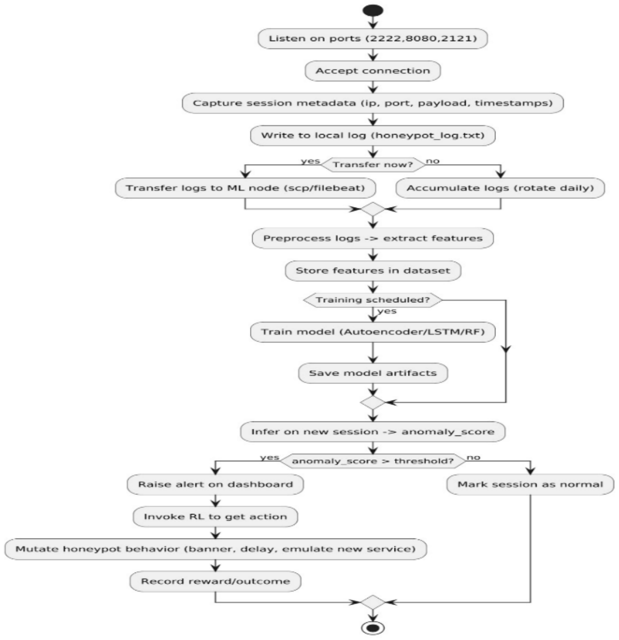
Listen on ports (2222,8080,2121)
Accept connection
Capture session metadata (ip, port, payload, timestamps)
Write to local log (honeypot_log.txt)
Transfer now?
yes
no
Transfer logs to ML node (scp/filebeat)
Accumulate logs (rotate daily)
Preprocess logs -> extract features
Store features in dataset
Training scheduled?
yes
Train model (Autoencoder/LSTM/RF)
Save model artifacts
Infer on new session -> anomaly_score
anomaly_score > threshold?
yes
no
Raise alert on dashboard
Mark session as normal
Invoke RL to get action
Mutate honeypot behavior (banner, delay, emulate new service)
Record reward/outcome

Fig. Activity Diagram

V. PROCESS FLOW

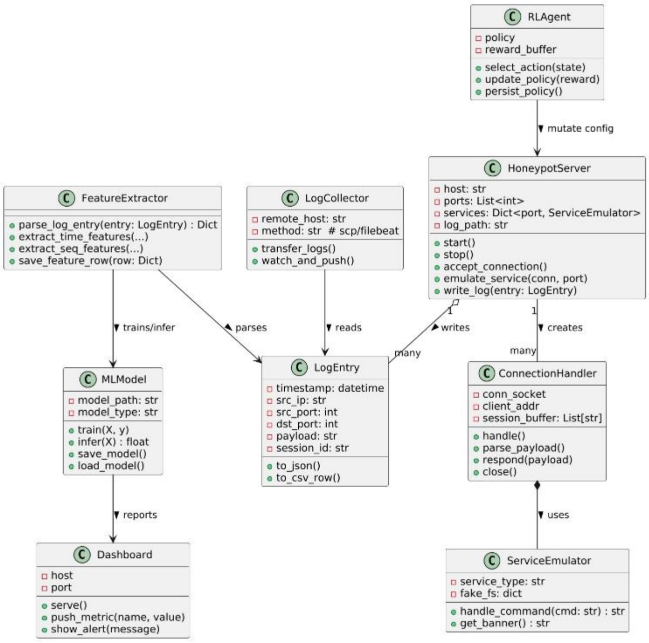

Fig. Class Diagram

VI. CONCLUSION

The AI-Driven Cloud Honeypot Network represents a critical evolution in cybersecurity defense, achieving its aim by developing a scalable and intelligent framework that proactively identifies and analyzes cyber threats. Unlike static, traditional decoys, this system utilizes Machine Learning and AI to dynamically adapt, classify attack behaviors, and detect emerging intrusion tactics in real time. By leveraging the cloud for flexible deployment, it maximizes threat intelligence collection and continuously refines its detection accuracy through an integrated data feedback loop. While facing challenges related to ensuring honeypot realism, managing massive data volumes, and maintaining cost efficiency , its future scope—including expansion to IoT security, integration of advanced deception techniques, and automated self-healing capabilities —firmly establishes this project as a foundational component for next-generation, adaptive, and collaborative threat detection.

REFERENCES

[1] J. Buzzio-Garcia, “Creation of a high-interaction honeypot system based on Docker containers,” in Proc. 5th World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4), 2021.

[2] A. Mudgal and S. Bhatia, “Big data with machine learning enabled intrusion detection with honeypot intelligence system on Apache Flink (BDML-IDHIS),” Springer, 2024.

[3] S. A. Kareem, R. C. Sachan, and R. K. Malviya, “AI-driven adaptive honeypots for dynamic cyber threats,” IEEE, 2024.

[4] A. A. Kubba, O. M. Al Mutasim, M. Abu Talib, and Q. Nasir, "A Systematic Review of Honeypot Data Collection, Threat Intelligence Platforms, and AI/ML Techniques," SSRN Electronic Journal, 2024.

[5] Z. Morić, V. Dakić, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," 2024.

[6] P. Čisar, "The Place and Role of Honeypot Solutions in Network Intrusion Detection Systems," 2025.