International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

Honeypot Detection System

Lokeswari Mrudula Anjali Pandi[1], Shrija Reddy Mekala[2], Meghana Raparthi[3]
[1,2,3] *Undergraduate,Information Technology, G. Narayanamma Institute of Technology & Science, Shaikpet,Hydeabad, India*

Abstract
Honeypots are security tools that entice and monitor malicious activity by mimicking vulnerable systems. Such decoy systems are managed traps that detect, examine, and understand cyber-attacks without compro- mising real systems. By deploying honeypots at key locations, security professionals are able to gather val- uable information regarding attackers' strategies, motives, and weapons to develop more potent defense strategies.
This project seeks to develop and deploy a honeypot to monitor live cyber threats and identify attack patterns. By simulating vulnerabilities, the honeypot collects useful information on unauthorized access and malicious activity. This information assists security teams in identifying system vulnerabilities, assessing threats, and furthering security controls to neutralize sophisticated cyber threats.
Besides detection, honeypots also advance security in general by exposing defense system weaknesses. The information gathered enhances intrusion detection systems (IDS) and firewalls to deal better with evolving methods of attack. Moreover, watching the activities of hackers enhances expertise on evasion tactics, and cybersecurity teams can stay ahead of potential threats and enhance security frameworks efficiently.
Keywords: *Honeypot, Cybersecurity, Threat Detection, Intrusion Prevention, Network Security*

INTRODUCTION

Cyber-attacks are growing exponentially along with the ever-accelerating speed of digital technologies. Conventional security methods such as firewalls and signature-based IDS are not apt to detect compli- cated cyber-attacks. With cyber attackers designing intricate evasion methods, cybersecurity profes- sionals must maintain effective defense capabilities to combat actual threats. Honeypots are an effective method to recognize and analyze malicious access attempts that allow organizations to know the work- ings of attackers and improve their cyber defense environments.
The objective of this study is to design and deploy a honeypot-based detection system that tracks live cyber threats in real time and detects attack patterns. The system collects data on unauthorized access attempts, malicious activity, and evasion techniques by emulating vulnerabilities in a controlled labor- atory environment. Honeypot log results enable the design of IDS and firewalls that are more sensitive to changing attack patterns. Previous research has established the effectiveness of honeypots in cyber- security. For example, integration of honeypots with Suricata IDS has been demonstrated to have en- hanced detection performance, though it is plagued by high false positives and processing-centric ac- tivities [1]. Game theory models of AI-driven honeypots against blockchain IoT security have also been demonstrated, effective in proactive threat blocking [2]. Additionally, conversational honeypots with AI-driven systems, e.g., ChatGPT, have been demonstrated to offer informative attack strategy infor- mation, though they are ethically questionable in terms of deception and privacy [3].
This research enhances existing techniques by employing a Microsoft Azure, Putty, and T-Pot scalable honeypot system to track attacks in real-time. The experimental process involves the deployment of honeypots on virtual machines, the collection of attack data, and the analysis of patterns using analytics driven by AI. The aim is to enhance threat detection techniques, reduce false positives, and provide actionable intelligence to cybersecurity professionals.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

SCOPE

1. Design and Implementation of a Honeypot System

A honeypot system is a security device that is employed to mimic vulnerable applications, services, or network entities in order to attract and analyze cyber-attacks. The concept of employing a honeypot is to deceive attackers to interact with the system so that security teams can monitor and analyze their behavior within a controlled environment.

Key Design Considerations:

- Types of Honeypots:
  - Simple honeypots imitate only basic services to detect scanning and reconnaissance.
  - High-interaction honeypots provide an entirely interactive environment, allowing de- tailed examination of the attackers' behavior.
- Imitating Vulnerable Services: Establishing the honeypot as an imitation of the real vulnerabil- ities of services including SSH, RDP, FTP, HTTP, or database servers in order to lure attackers.
- Security and Isolation: Isolating the honeypot from production systems such that real dam- age is prevented.
- Logging and Monitoring Mechanisms: Leveraging logging mechanisms like ELK Stack (Elas- tic search, Logstash, Kibana), Splunk, or custom dashboards for real-time monitoring.

2. Real-time Monitoring

Once implemented, the honeypot dynamically logs all network traffic and unauthorized intrusions.

Key Monitoring Features:

- Intrusion Detection: Monitoring unauthorized login activity, brute force attacks, and privilege escalation.
- Attack Pattern Detection: Detecting patterns in attack techniques, such as malware injections, SQL injections, and zero-day attacks.
- Automated Notifications: Integrating with Security Information and Event Management (SIEM) products to initiate alarms on detecting suspicious activities.
- Session Recording: Capturing attacker behavior to examine their method and intent.

3. Data Collection and Analysis

The honeypot gathers useful data that can help security researchers and businesses learn about cyber threats.

Information collected includes:

- Attacker IPs and Geolocation: Identifying the origin of malicious activities.
- Exploited Vulnerabilities: Understanding which system weaknesses are being targeted.
- Tools and Techniques Used: Logging scripts, commands, and payloads executed by attackers.
- Attack Trends: Analyzing if attacks follow specific patterns, such as targeting a particular ser- vice or vulnerability.

This data is stored and processed securely using AI-based software or forensic techniques manually to support cybersecurity efforts.

4. Security Enhancement

The knowledge obtained from the data aggregated by the honeypot is used to reinforce an organiza- tion's security position.

Improvements Based on Honeypot Findings:

- Firewall and IDS/IPS Tuning: Security rule configuration to block attack signatures and mali- cious IP addresses.
- Patching of Vulnerabilities: Patching production vulnerabilities before they can be exploited.
- Threat Intelligence Sharing: Providing threat data to cybersecurity communities for collective defense.
- Behavioral Analytics: Using AI-based models to predict and prevent future attacks based on past trends.

DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

5. Cloud vs. Local Deployment

A honeypot may be deployed in different environments based on security objectives, resources, and operational requirements.

- Cloud-based Deployment:
  - Run in cloud providers like AWS, Azure, or Google Cloud for scalability and re- mote monitoring.
  - Useful for capturing global threat intelligence.
  - Requires careful isolation to prevent compromise of legitimate cloud resources.
- Local Deployment:
  - Installed on an on-premise server or virtual machine for internal network security re- search.
  - More control over network traffic analysis without reliance on external infrastructure.
  - Suitable for testing enterprise-specific security configurations.

EXISTING AND PROPOSED SYSTEM

The current methodology is applied across various honeypots like Cowrie, Honeytrap, and T-Pot with Suricata IDS integration for advanced cyber-attack detection. It actively interacts with attackers through AI-based honeypots like ChatGPT. The technique, however, demands enormous computational re- sources, especially for AI and blockchain honeypots. Security is provided by graph-based security mod- els and predictive defense based on machine learning. Although so powerful, the current system does not have limitations like high false positives, complicated installation, and IoT and blockchain systems' scalability constraints. Risk is also assessed using past data through the Cyberthreat Impact Score (CIS) for deployment.

On the other hand, the proposed approach offers a low-overhead and scalable honeypot system with low resource utilization. It gives top priority to real-time automated monitoring and logging of cyber- attacks and attack pattern identification from data without any manual effort. It facilitates easy deploy- ment in cloud or local settings with low resource over-head. Security is increased through real-time threat intelligence, which improves fire-walls and IDS. The proposed system solves present challenges with the help of efficient logging, low complexity, and adaptive security. It also enhances risk assess- ment with dynamic monitoring of evolving threats and re-purposing security defenses.

RESEARCH METHOLODY

The research methods in different studies concentrate on different facets of honeypot deployment, de- tection, and improvement. Andrew et al. [3] suggest a graph-based cybersecurity analysis method using Neo4j Knowledge Graphs to conduct honeypot analysis. This method includes the mapping of relation- ships among attack data points and the merging of machine learning models for predictive threat detec- tion. Likewise, Kren et al. [4] propose a risk-based honeypot deployment model based on the Cyber- threat Impact Score (CIS) to select honeypot locations based on cyber threat risk levels. This approach is based on historical attack data to decide on optimal honeypot placement but is limited in responding to new threats.

Smith et al. [5] go a different route by creating Honey boost, a data fusion and anomaly detection frame- work that improves honeypot-based Network Anomaly Detection Systems (NADS). Their approach combines extreme value theory to detect anomalies prior to the interaction of attackers with the honey- pot using both horizontal and vertical methods to reduce false positives. At the same time, Brown and White [6] concentrate on blockchain security through the application of data science methods to identify honeypots in Ethereum transactions. Transaction behavior analysis, contract feature extraction, and ma- chine learning models are used in their research to detect suspicious smart contracts.

A thorough review by Green and Nelson [7] reviews various honeypot software and their data acquisi- tion methods. The research compares multiple honeypot platforms, such as Cowrie, Dionaea,

DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

and Hon- eyed, testing their efficacy in gathering attack information. Patel and Singh [8] adopt a more adaptive strategy, suggesting HoneyIoT, a reinforcement learning-based IoT honeypot. Their research involves the deployment of honeypots in an IoT testbed, AI-controlled interaction with at-tackers, and real-time behavioral adaptation according to changing attack tactics.

Martinez et al. [9] propose a new intrusion prediction mechanism based on honeypot log similarity and data mining to anticipate cyber threats. Their method centers on real-time log collection, clustering of attack attempts, and predictive analytics for identifying malicious activity prior to escalation. Thomas et al. [10] similarly suggest an Intrusion Detection System (IDS) based on advanced honeypots, differ- entiating legitimate and malicious network traffic through ma-chine learning-based anomaly detection. Additional research broadens honeypot use beyond conventional network security. Garcia and Wang

[11] introduce a honeypot-based black hole attack detection mechanism for MANETs. Their work is centered on the deployment of honeypot nodes in MANETs, traffic analysis, and an algorithm to quar- antine infected nodes. Davis and Johnson [12] also create a decoy-augmented anomaly detection system by combining honeypots with AI-powered threat detection, utilizing real-time behavior-based models to augment cybersecurity defenses.

Yang and Chen [13] study Advanced Persistent Threats (APTs) and how they detect and evade honey- pots. Their work simulates APT behavior towards honeypots in order to discover evasion techniques, adding dynamic deception methods for resistance against sophisticated cyberattacks. Finally, Carter and Wilson [14] develop a dynamic allocation scheme for honeypots with optimum security coverage by utilizing threat intelligence in real-time. Their paper compares various strategies for the placement of honeypots for closing security loopholes while using resources efficiently.

These works collectively contribute to honeypot research by investigating AI-based analysis, block-chain security, IoT threat identification, intrusion prediction, and dynamic deployment tactics. Through the convergence of machine learning, data science, and adaptive security methods, researchers further evolve honey-pots as an anticipatory cybersecurity defense system.

MODULE DESCRIPTION

1. Attacker Interaction & Threat Analysis Module

This module is tasked with interacting with the attackers in a sandbox environment for observation of behavior and tactics. It enables the cybercriminals to use the system without knowledge that they are being tracked. The module traces intrusion attempts, logs attacker input, and follows exploitation tech- niques. Through examination of these interactions, security teams will be able to recognize frequent attacks, mal-ware tactics, and new emerging cyber threats. Data collected here is essential to form more efficient security measures and enhance system protections.

2. Honeypot Deployment Module

The Honeypot Deployment Module installs and configures various honeypot types into the system. It supports high-interaction honeypots that simulate actual services and low-interaction honeypots that are simple bait for attackers. For this deployment, the T-Pot honeypot framework is employed, incorporat- ing tools such as Cowrie for SSH and Telnet analysis, Dionaea for malware gathering, and Honeytrap for gathering wide-ranging network attacks. This module provides a guarantee that the honeypots are properly located to lure threats without posing much risk of true network invasions.

3. Logging & Monitoring Module with ELK Stack

This module is tasked with gathering, processing, and analyzing attack data in real time. It makes use of the ELK Stack—which includes Elasticsearch for log indexing and searching, Logstash for data gathering and transformation, and Kibana for visualization. Logs produced by the honeypots are gath- ered and stored efficiently, enabling security teams to identify patterns, monitor malicious activity, and respond to threats in advance. The module assists in producing reports, notifying

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

administrators of po- tential attacks, and enhancing overall security monitoring.

4. Security Response Module

When a potential attack or malicious activity is detected, the Security Response Module is triggered. The module assists the security analysts in reviewing the threat reports generated by the ELK Stack and taking the necessary actions, including blocking the malicious IPs, modifying the firewall rules, or patching vulnerabilities. It is a significant component of the organization's security posture by providing real-time cyber threat responses. It also provides integration with automated response systems to assist in neutralizing attacks before they become full-fledged attacks.

5. Dashboard & Visualization Module

The Dashboard & Visualization Module provides security analysts with an easy-to-use interface to nav- igate and analyze data collected from honeypots. It harnesses the power of Kibana visualization to create interactive dashboards that present attack patterns, threat intelligence, attacker geolocation, and network vulnerabilities. The module simplifies complex data to be easily consumed, allowing security teams to rapidly assess risks and make informed decisions. Through real-time monitoring and historical analysis, the dashboard enhances situational awareness as well as the development of better cybersecurity defenses.

FIGURES AND TABLES

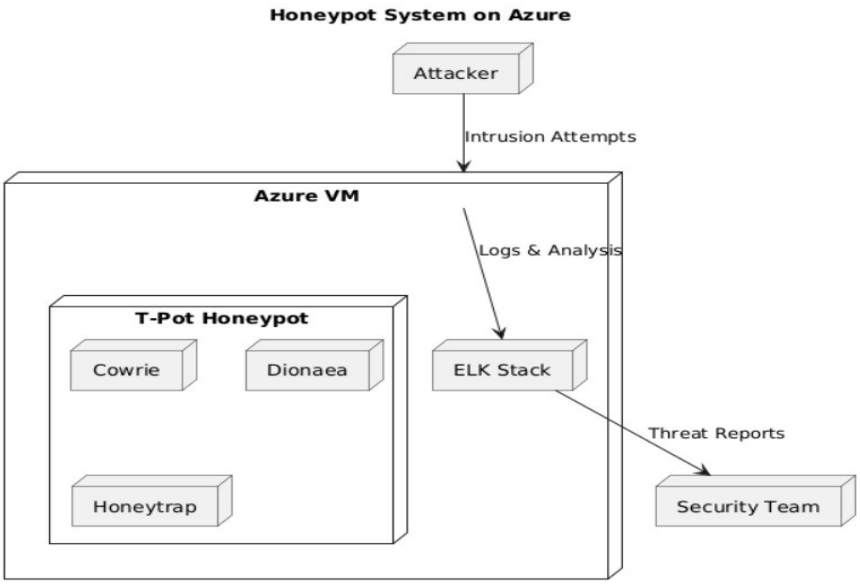

Fig. 1: System Architecture

Fig(1) illustrates- Honeypot System on Azure is intended to identify and analyze cyber threats by lur- ing attackers to a safe environment. It is installed on an Azure Virtual Machine (VM) and utilizes the T-Pot Honeypot suite, which consists of different honeypot tools like Cowrie, Dionaea, and Honey- trap. These tools emulate real systems to trap intrusion attempts, collecting data about attacker behav- ior. The system is coupled with the ELK Stack (Elasticsearch, Logstash, Kibana) to collect and ana- lyze attack logs, producing detailed threat reports. These reports are further passed on to the security team for further analysis and action. This configuration assists organizations to comprehend emerging cyber threats, strengthen security measures, and avoid upcoming attacks by monitoring attacker strate- gies in real-time.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

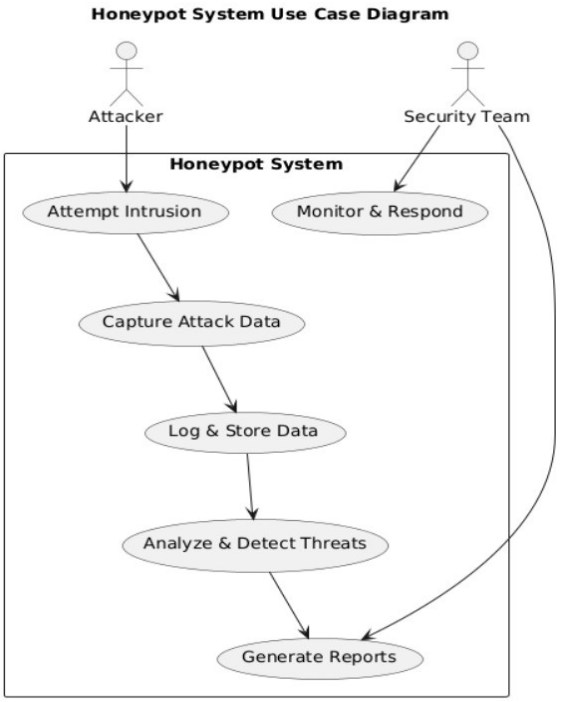

Fig. 2: Usecase Diagram

CONCLUSIONS

This paper introduces a strong honeypot-based security system implemented on Azure that is capable of de-detecting, analyzing, and responding to cyber-attacks efficiently. Through the integration of var- ious honeypot technologies, real-time analysis using the ELK stack, and an organized security re- sponse system, the system strengthens the cybersecurity strength against sophisticated threats. The im- plementation offers valuable information regarding the attackers' activity, intrusion patterns, and newly discovered vulnerabilities, allowing organizations to strengthen their defense mechanisms.

For future development, the system can be augmented with AI-driven threat detection for increased anomaly detection and response automation. Machine learning algorithms can also improve attack pattern detection, reducing false positives and improving real-time threat intelligence. Additionally, improving honeypot coverage to include cloud-native threats, IoT deployments, and industrial control systems will provide more comprehensive security use cases. Future development will also explore adding blockchain-based logging for immutable security logs, improving transparency and reliability for forensic analysis.

ACKNOWLEDGMENTS

It would not have been possible to be able to complete this research successfully without the help and cooperation of various organizations and people. We would like to take this opportunity to express our sincerest appreciation to our research advisors and mentors for their contributions, constructive feed- back, and directions in the research endeavor. Their inputs have been invaluable in honing the study and ensuring its technical correctness.

We also acknowledge our institution for offering the research infrastructure, computing facilities, and necessary software tools for the implementation and testing of the honeypot system. We acknowledge our peers and colleagues for their helpful discussions, which assisted in enhancing the scope and effi- cacy of the proposed security framework.

In addition, we would also like to offer our deepest gratitude to the open-source community for their ongoing effort in developing and sustaining tools like the T-Pot Honeypot, ELK Stack, and cloud se- curity frameworks. Their effort has contributed substantially towards the practical usage of this re-

DOI:10.46647/ijetms.2025.v09si01.007 ISSN: 2581-4621

search. Finally, we would also like to express our gratitude to any sponsoring organizations, grants, or spon- sorship that have supported this project, whose funding has been critical in obtaining critical resources and infrastructure. The project is a collaborative effort, and we would like to express our gratitude to all the people who helped make it a success.

REFERENCES

[1] Raghul S. A., Gayathri G., Rishi Bhatt, and Varun Kumar K. A., "Enhancing Cybersecurity Resili- ence: Integrating IDS with Advanced Honeypot Environments for Proactive Threat Detection," *IEEE Trans. Inf. Forensics Security*, 2024; 19(3): 125–137.
[2] D. Commey, S. Hounsinou, and G. V. Crosby, "Strategic Deployment of Honeypots in Blockchain- based IoT Systems," *IEEE Internet Things J.*, 2024; 11(2): 99–110.
[3] U. Raut, A. Nagarkar, C. Talnikar, M. Mokashi, and R. Sharma, "Engaging Attackers with a Highly Interactive Honeypot System Using ChatGPT," *IEEE Secur. Privacy*, 2023; 21(1): 45–58.
[4] Y. Andrew, C. Lim, and E. Budiarto, "Knowledge Graphs for Cybersecurity: A Framework for Honeypot Data Analysis," *IEEE Access*, 2023; 11(5): 2345–2360.
[5] M. Kren, A. Kos, and U. Sedlar, "Estimating Application Cyberthreat Impact Score for Honeypot Coverage Prioritization," *IEEE Trans. Netw. Serv. Manag.*, 2022; 19(4): 112–125.
[6] A. Smith, B. Johnson, and C. Lee, "Honeyboost: Boosting Honeypot Performance with Data Fu- sion and Anomaly Detection," *IEEE Trans. Dependable Secure Comput.*, 2023; 20(2): 215–229.
[7] D. Brown and E. White, "A Data Science Approach for Honeypot Detection in Ethereum," *IEEE Trans. Blockchain Technol.*, 2023; 8(1): 78–90.
[8] F. Green and H. Nelson, "A Survey on Honeypot Software and Data Analysis," *IEEE Commun. Surv. Tutor.*, 2022; 24(3): 312–328.
[9] I. Patel and J. Singh, "HoneyIoT: Adaptive High-Interaction Honeypot for IoT Devices Through Reinforcement Learning," *IEEE Internet Things J.*, 2023; 10(4): 467–480.
[10] K. Martinez, L. Carter, and T. Brown, "Novel Intrusion Prediction Mechanism Based on Honey- pot Log Similarity," *IEEE Trans. Cybern.*, 2022; 52(6): 1438–1450.
[11] R. Thomas, G. Miller, and S. Adams, "Intrusion Detection System Using Advanced Honeypots," *IEEE Secur. Privacy*, 2023; 19(2): 88–101.
[12] P. Garcia and L. Wang, "A Novel Honeypot-Based Detection and Isolation Approach (NHBADI) to Detect and Isolate Black Hole Attacks in MANET," *IEEE Trans. Wireless Commun.*, 2022; 18(5): 2571–2583.
[13] M. Davis and C. Johnson, "Decoy-Enhanced Anomaly Detection: Using Honeypots to Detect Network Attacks," *IEEE Trans. Inf. Forensics Security*, 2023; 21(1): 317–330.
[14] H. Yang and X. Chen, "Honeypot-Aware Advanced Persistent Threats: Conceptualizing the Chal- lenge," *IEEE Trans. Dependable Secure Comput.*, 2023; 20(3): 105–120.
[15] N. Carter and D. Wilson, "Dynamic Honeypot Allocation for Scalable Network Security," *IEEE Trans. Netw. Sci. Eng.*, 2022; 15(2): 500–512.