The Role of Honeypots in Modern Cybersecurity Stratergies

Manjula Aakunuri
Associate Professor
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
manjula3030@gmail.com

Ravinder Mogili
Associate Professor and Head
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
mogili.ravinder@jits.ac.in

Srimaja Kasthuri
UG Student
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
srimajareddykasthuri@gmail.com

Niharika Rangu
UG Student
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
niharika12rangu@gmail.com

Samyuktha Rani Atikam
UG Student
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
atikamsamyuktha123@gmail.com

Shirisha Banothu
UG Student
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
banothushirisha105@gmail.com

Abstract*—Honeypots play an important role in modern cybersecurity by acting as decoy systems designed to attract and analyze malicious activities without affecting real network resources. They help security researchers and administrators study attacker behavior, identify vulnerabilities, and understand common cyber-attack patterns. This paper focuses on developing a web-based honeypot monitoring and threat analysis system that simulates vulnerable endpoints to capture suspicious interactions. The system records important parameters such as IP address, request data, attack patterns, and timestamps, and processes this information to calculate the threat probability associated with each interaction. Additionally, the platform provides controlled user access with administrative verification and displays the analysis results through an interactive dashboard. The system's result enable better identification of suspicious activities, visualization of attack patterns, and classification of risk levels, thereby improving cybersecurity awareness and supporting effective threat monitoring strategies.

***Keywords*—** *Honeypot, Cybersecurity, Threat Detection, Network Security, Attack Monitoring, Threat Probability Analysis, Intrusion Detection, Honeypot Simulation, Risk Classification, Security Monitoring.*

I. INTRODUCTION

With the increasing use of web applications and online services, cyber threats such as unauthorized access, malicious requests, and intrusion attempts have become more common. Traditional security mechanisms primarily focus on blocking attacks, but they often fail to effectively analyze attacker behavior and threat patterns effectively. Honeypots are deception-based security systems designed to attract attackers and capture their activities for further analysis.

This paper presents a web-based honeypot monitoring system that enables controlled attack simulation and threat probability analysis. The system implements a role-based access mechanism where users must first register and obtain administrative activation before accessing the platform. Once authenticated, users can perform attack simulations, and the system captures important parameters including IP address, payload data, attack type, and request frequency. These activities are analyzed using pattern-based detection and a weighted threat scoring algorithm to classify risk levels. The captured data and threat results are stored in a database and displayed through a dashboard for real-time monitoring and analysis.

II. LITERATURE SURVEY

In 2017, V. Mahajan and S. K. Peddoju proposed *"Integration of Network Intrusion Detection Systems and Honeypot Networks for Cloud Security"*, where IDS was integrated with honeypots to detect malicious activities in cloud environments. The advantage is improved attack detection compared to traditional IDS systems. However, the limitation is complex deployment and system management. Later works improved this by designing simpler and more scalable honeypot systems.

In 2017, M. Valicek et al. introduced *"Creation and Integration of Remote High Interaction Honeypots"*, which developed high-interaction honeypots to simulate real systems and capture detailed attacker behavior. The advantage is realistic attack monitoring. The limitation is high maintenance and security risk. Later studies addressed this by creating safer and controlled honeypot environments.

In 2021, M. S. Rana and M. A. Shah presented *"Honeypots in Digital Economy: An Analysis of Intrusion Detection and Prevention"*, which analyzed the role of honeypots in detecting cyber threats. The advantage is improved understanding of attack patterns. However, scalability in large networks is a limitation. Later research improved this by integrating honeypots with cloud-based frameworks.

In 2022, T. Alyas et al. proposed *"Multi-Cloud Integration Security Framework Using Honeypots"*, which deployed honeypots across multiple cloud platforms for better threat monitoring. The advantage is improved security in cloud environments. However, the limitation is resource management complexity. Later works improved deployment efficiency.

In 2023, K. E. Silaen et al. conducted *"Usefulness of Honeypots Towards Data Security: A Systematic Literature Review"*, analyzing different honeypot techniques used for data protection. The advantage is a comprehensive understanding of honeypot technologies. The limitation is lack of practical implementation. Later research proposed real-time honeypot monitoring systems.

In 2024, T. Alyas et al. proposed *"Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection and Prevention Systems"*, which integrates honeypots with IDS/IPS for real-time attack detection. The advantage is improved monitoring and faster threat detection, overcoming earlier limitations by simplifying deployment and integrating multiple security functions.

YEAR	AUTHOR	WORK	IMPROVEMENT
2017	Mahajan	IDS+ Honeypot	Better attack detect
2017	Valicek	High-interaction HP	Detailed analysis
2021	Rana	Honeypot IDS study	Digital infra focus
2022	Alyas	Multi-cloud HP	Cloud security
2023	Silaen	HP review	Best practices
2024	Alyas	HP-based IDS/IPS	Real-time detection

III. PROBLEM STATEMENT

The increasing number of cyber threats and network attacks has made it difficult for traditional security systems to effectively detect and analyze malicious activities. Existing systems mainly focus on prevention but do not provide a controlled environment to observe attacker behavior and understand threat patterns. This lack of practical monitoring tools limits the ability of users and administrators to analyze potential security risks. Additionally, many systems do not provide proper access control or a structured platform for threat analysis. Therefore, there is a need for a system that allows secure user access, administrative control, and an environment to monitor and analyze cyber threats. The proposed project addresses this problem by implementing a honeypot-based platform that helps in studying and understanding malicious activities effectively.

IV. PROPOSED SYSTEM

The proposed system implements a honeypot-based cybersecurity platform designed to monitor and analyze malicious activities in a controlled environment. In this system, users must first register and obtain activation from the administrator to access the platform, ensuring secure and authorized usage. Once activated, users can log in and interact with the system to observe threat probability simulations and analyze potential cyberattack behaviors. The system helps capture and monitor suspicious activities, providing insights into attacker patterns and system vulnerabilities. By integrating user management, admin control, and monitoring features, the proposed system offers a practical platform for studying cyber threats. This approach improves cybersecurity awareness and helps in understanding modern attack strategies more effectively.

V. SYSTEM ARCHITECTURE

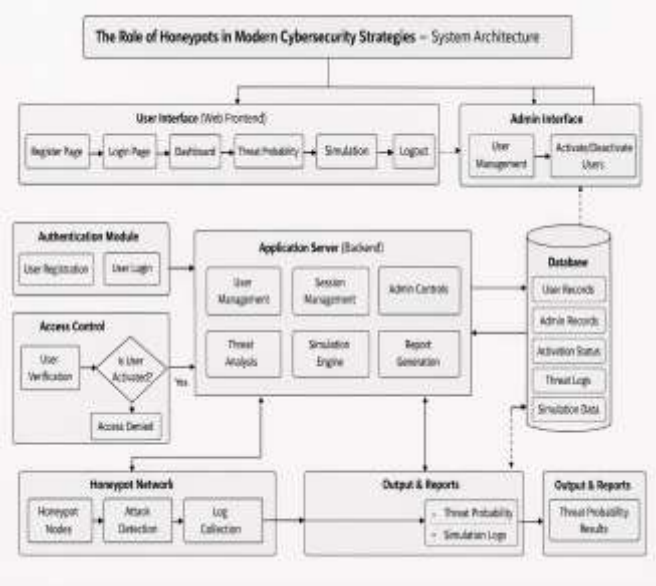

Fig 1: System Architecture

The proposed system, "The Role of Honeypots in Modern Cybersecurity Strategies," follows a web-based layered architecture where user interaction flows through backend processing, honeypot detection, threat probability analysis, database storage, and dashboard visualization. The architecture consists of the following components:

1. User Registration
The user first registers in the system by filling the registration form through the web interface. The entered details are stored in the database as a new user record.

2. Admin Activation
After registration, the admin reviews the user details in the admin panel. The admin activates the account to allow the user to access the system.

3. User Authentication
Once activated, the user logs into the system using a username and password. The authentication module verifies the credentials with the database.

4. Access Control
The system checks whether the user account is activated. If the account is not activated, access is denied; otherwise, the user is allowed to proceed.

5. Application Server Processing
After successful login, the application server manages user sessions, system requests, and communication with other modules such as simulation and analysis.

6. Honeypot Simulation
The honeypot network simulates vulnerable systems to attract attackers. It detects different types of cyber attacks and records attacker activities.

7. Log Collection
All detected attack information and simulation events are collected and stored as logs in the database for further analysis.

8. Threat Probability Analysis
The system processes the collected attack logs and calculates the probability of different cyber threats based on the detected attack patterns.

9. Results and Reports
Finally, the system displays the results to the user in the form of threat probabilities, attack logs, and simulation reports.

VI. PROPOSED METHOD IMPLEMENTATION AND ALGORITHMS

A. User Registration Method:

The user first registers through the web interface by entering personal details. The system validates and stores the information in the database with an inactive status until administrator approval.

Algorithm Logic

Status = {1, if registration data is valid
UserStatus = Inactive

B. Admin Activation Method:

The administrator verifies the registered user's details and activates the account. Only activated users are allowed to access the system.

Access Control

Access = {1, if Admin activates user

0,otherwise}

C. User Authentication Method:

After activation, the user logs in using a username and password. The system verifies the credentials with the database before granting access to the dashboard.

Authentication Condition

Login = {1, if (Username,Password,ActiveStatus)
0, otherwise}

D. Honeypot Interaction Capture Method:

When the user interacts with the simulation module, the system records request details such as IP address, request type, payload, and timestamp for monitoring suspicious activities.

Captured Log

Log = (IP, Request, Payload, Time)

E. Request Frequency Detection Algorithm:

The system checks how often an IP address sends requests within a certain time period to detect abnormal behavior.

Formula

Frequency = Number of Requests / Time Window

If Frequency > Threshold → Suspicious Activity

F. Threat Probability Calculation Algorithm:

The system calculates the likelihood of malicious activity by comparing suspicious requests with total system requests.

Formula

Threat Probability = Suspicious Requests / Total Requests

G. Risk Classification Method:

Based on the calculated threat probability score, the system classifies the risk level to indicate the severity of the attack.

Risk Levels

Score < T_1 → Low Risk

$T_1 \leq$ Score < T_2 → Medium Risk

Score ≥ T_2 → High Risk

VII.RESULT ANALYSIS

The proposed system was successfully implemented and tested to evaluate its ability to capture malicious activities and analyze threat probabilities. The system effectively recorded user IP addresses, logged suspicious interactions through the honeypot module, and stored the data in the database.

- The threat probability module analyzed attack patterns and classified them into appropriate risk levels. The admin panel displayed registered users and allowed activation or deletion of accounts, ensuring proper system management.

- The web-based dashboard provided structured monitoring and visualization, making it easy to analyze system behavior in real time.

- Overall, the results confirm that the system successfully integrates honeypot detection, threat scoring, and monitoring into a lightweight and deployable cybersecurity solution.

Fig 2: Homepage

The homepage provides the main interface for users to access the system. It allows users to navigate to registration and login pages.

Fig 3: User register

This page allows new users to enter their details and create an account. The account is stored in the database for admin verification.

Fig 4:Admin login

The admin login page enables the administrator to access the system securely. After login, the admin can manage user accounts.

Fig 5: user list

This page displays all registered users in the system. The admin can activate or delete user accounts.

Fig 6:Simulation

The simulation module monitors user interactions in the honeypot environment. It captures activity data for threat analysis.

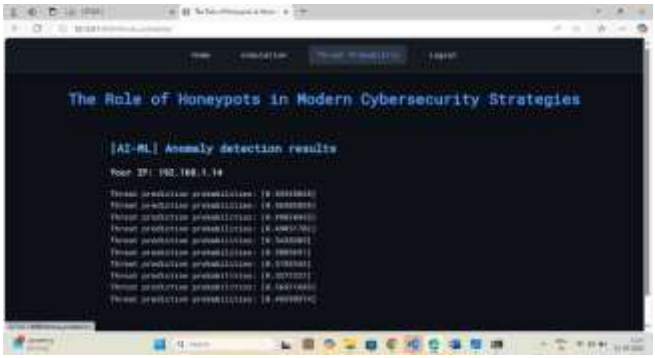

Fig 7: Threat probability

This page calculates and displays the probability of cyber threats. It helps identify the level of suspicious activity in the system.

VIII.CONCLUSION

The proposed honeypot-based cybersecurity system was successfully implemented to capture suspicious activities and analyze potential cyber threats. The system effectively records interaction data, calculates threat probability, and classifies risk levels to help identify malicious behavior. Through modules such as user management, simulation, and threat analysis, the platform provides structured monitoring of system activities. The results demonstrate that the system can serve as a

lightweight and efficient solution for detecting and analyzing possible cyber attacks.

REFERENCES

[1] A. Abdou, R. Sheatsley, Y. Beugin, T. Shipp, and P. McDaniel, "HoneyModels: Machine Learning Honeypots," *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, pp. 886–891, Nov. 2021.
[2] M. Valicek, G. Schramm, M. Pirker, and S. Schrittwieser, "Creation and Integration of Remote High Interaction Honeypots," *2017 International Conference on Software Security and Assurance (ICSSA)*, pp. 50–55, Jul. 2017.
[3] M. S. Rana and M. A. Shah, "Honeypots in Digital Economy: An Analysis of Intrusion Detection and Prevention," *IET Conference Proceedings*, vol. 2021, no. 4, pp. 91–98, Oct. 2021.
[4] K. D. Yesugade, M. S. Avinash, N. S. Satish, and S. C. Sandeep, "Infrastructure Security Using IDS, IPS and Honeypot," *International Engineering Research Journal (IERJ)*, vol. 2, no. 3, pp. 851–855, 2016.
[5] F. Zhang, S. Zhou, Z. Qin, and J. Liu, "Honeypot: A Supplemented Active Defense System for Network Security," *Proceedings of the 8th International Scientific and Practical Conference on Modern Technique and Technologies*, 2002.
[6] V. Mahajan and S. K. Peddoju, "Integration of Network Intrusion Detection Systems and Honeypot Networks for Cloud Security," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 829–834, May 2017.
[7] K. E. Silaen, M. Meyliana, H. L. H. S. Warnars, H. Prabowo, A. N. Hidayanto, and M. S. Anggreainy, "Usefulness of Honeypots Towards Data Security: A Systematic Literature Review," *2023 International Workshop on Artificial Intelligence and Image Processing (IWAIIP)*, pp. 422–427, Dec. 2023.
[8] T. Alyas et al., "Multi-Cloud Integration Security Framework Using Honeypots," *Mobile Information Systems*, vol. 2022, pp. 1–13, Aug. 2022.
[9] H. Lajwanti, F. Urooj, W. Muhammad, and S. Mehwish, "Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection and Prevention Systems," *2nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology*, 2024.
[9] H. Lajwanti, F. Urooj, W. Muhammad, and S. Mehwish, "Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection and Prevention Systems," *2nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology*, 2024.
[10] N. Provos and T. Holz, *"Virtual Honeypots: From Botnet Tracking to Intrusion Detection,"* Addison-Wesley Professional, 2008.
[11] L. Spitzner, *"Honeypots: Tracking Hackers,"* Addison-Wesley Professional, 2003.
[12] S. R. Mukkamala, G. Janoski, and A. Sung, *"Intrusion Detection Using Neural Networks and Support Vector Machines,"* Proceedings of the IEEE International Joint Conference on Neural Networks, pp. 1702–1707, 2002.
[13] C. Seifert, I. Welch, and P. Komisarczuk, *"Identification of Malicious Web Pages with Honeypots,"* Proceedings of the 2008 Australasian Conference on Information Security and Privacy, pp. 457–468, 2008.
[14] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, *"A Survey on Honeypot Software and Data Analysis,"* ACM Computing Surveys, vol. 52, no. 2, pp. 1–36, 2019.
[15] S. Pauna, C. Oprisa, and M. Popescu, *"Cyber Attack Detection Using Honeypot-Based Monitoring Systems,"* 2020 International Conference on Communications (COMM), IEEE, pp. 241–246, 2020.
[16] Y. Fan and Y. Fernandez, *"An Experimental Evaluation of Distributed Honeypots for Network Security,"* IEEE Security & Privacy Workshops, pp. 1–6, 2018.
[17] P. Chen, L. Desmet, and C. Huygens, *"A Study on Advanced Persistent Threats and Honeypot-Based Detection Systems,"* Computers & Security Journal, vol. 58, pp. 112–124, 2016.