IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131128

ADAPTIVE HONEYPOT SYSTEM WITH BEHAVIOUR ANALYSIS FOR WEBSECURITY

Mrs. Latha P[1], Harish Ashok Kalahal[2], Vamshi D[3], R C Vineeth Bhavimane[4]

Assistant Professor, CSE (Cyber Security), RNS Institute of Technology, Bangalore, India[1],

Student, CSE (Cyber Security), RNS Institute of Technology, Bangalore, India[2,3,4]

Abstract: Due to rapidly evolving cybersecurity threats, advanced defence mechanisms are essential. This paper proposes an Adaptive Honeypot System with Behavioural Analysis using the K-Means algorithm to classify threats based on behaviour. By simulating vulnerabilities, the system deceives attackers, collects data, and conducts behavioural analysis. Dynamic configurations adapt to evolving attack patterns. The system efficiently detects and responds to future threats, enhancing web security. Additionally, the system employs lightweight architectures and privacy-preserving mechanisms to comply with regulations like GDPR while maintaining high performance and adaptability. To demonstrate the efficacy of the system, experimental results include statistical trends, accuracy measurements, and graphical analyses of behavioural clustering [3] [4] [7].

Keywords: Adaptive Honeypot, Behavioural Analysis, Web Security, K-Means Algorithm

I. INTRODUCTION

The increasing reliance on internet-based technologies has driven global economic advancements while simultaneously increasing cybercrimes. Conventional safety measures often fail to address the ingenuity of cyber attackers. This necessitates advanced, adaptable defence mechanisms to secure critical infrastructure and sensitive information [1] [2]. The Adaptive Honeypot System simulates vulnerable web services to deceive and monitor malicious actors. It employs Behavioural Analysis and K-Means clustering to classify and analyse attacker behaviours, providing insights into their strategies. By dynamically adapting its configurations, the system anticipates emerging threats and strengthens defences, as evidenced by this study's results [5]. Furthermore, it highlights the significance of integrating machine learning and real-time analytics to create a robust cybersecurity infrastructure capable of addressing complex challenges in dynamic environments [3]. Figures 1 illustrate the system's dynamic configurations Honeypot system

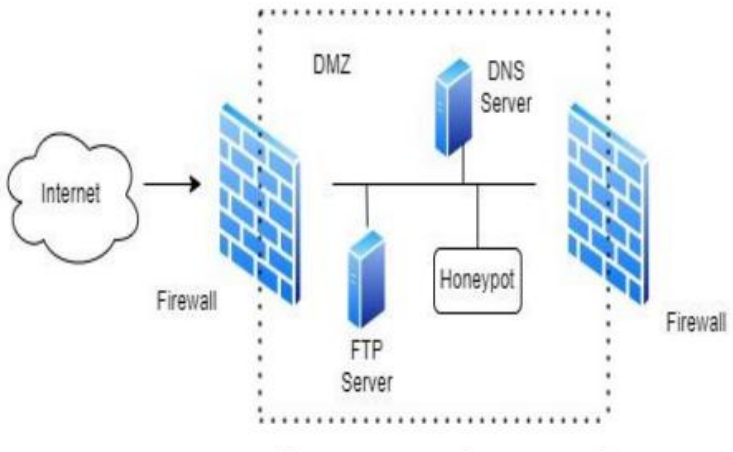

Figure 1.Honeypot

Note: *Location of honeypot in the network. In: Analysis of cyber-attacks using honeypot.* [5]Altunay, H. C. (2024). *Black Sea Journal of Engineering and Science*, 7(5), 954-959.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131128

II. LITERATURE REVIEW

NO	TITLE	AUTHORS	YEAR	ADVANTAGES	DISADVANTAGES	TECHNOLOGIES
1	Honeypot detection systems: A comprehensive survey	Anderson, R., Sallis, M.	2023	-Provides thorough overview of honeypot detection systems - Identifies evolving techniques to bypass honeypots	-Focuses primarily on detection - Limited experimental data	-Survey methodology - Classification algorithms
2	Enhancing web security with adaptive honeypot systems and machine learning-based anomaly detection	Zhang, W., Wang, L., He, X.	2024	-Combines adaptive honeypot systems with machine learning - Demonstrates effectiveness of anomaly detection	-High computational overhead -Potential false positives	-Adaptive honeypot -Machine learning
3	Behavioral analytics for detecting advanced persistent threats using honeypot systems	Yu, H., Li, Y.	2023	- Focuses on advanced persistent threat detection - Leverages behavioral analytics	- Limited dataset for testing - May miss changing tactics	- Behavioral analytics - APT frameworks - Honeypots
4	The k-means algorithm: A comprehensive survey and performance evaluation	Ahmed, M., Seraj, R., Islam, S. M. S.	2020	- Comprehensive overview of K-Means algorithm -Evaluates performance across scenarios	-Lacks cybersecurity specifics - Limited technology integration	- K-Means algorithm - Clustering - Performance evaluation

III. TYPES OF HONEYPOT SYSTEMS

Honeypot systems are categorized according to their function and degree of interaction. Low-interaction honeypots are made to mimic fundamental network functions and are intended to record surface-level assault patterns without disclosing the system itself [8]. Although they are simple to implement and use few resources, they can only gather a limited amount of data. Conversely, high-interaction honeypots simulate entire operating systems and give attackers a realistic environment [10]. Although these systems gather a lot of information about the methods used by attackers, their abuse necessitates significant resources and cautious administration [11].

In academic or experimental contexts, research honeypots are commonly employed to examine new threats and attacker behaviours. The primary goal of these systems is to gather comprehensive data for cybersecurity research and development. Production honeypots are deployed within an organization's infrastructure to enhance security by detecting and mitigating real-world attacks. They are often integrated with other security tools to provide actionable intelligence and improve overall defence mechanisms. By understanding and leveraging these different types of honeypots, organizations can implement targeted solutions that align with their specific security objectives and operational requirements.

IV. PROPOSED WORKING OF ADAPTIVE HONEYPOT SYSTEMS

The Adaptive Honeypot System leverages advanced analytical techniques and real-time monitoring to provide comprehensive security. Using K-Means Behavioural Analysis, the system identifies anomalies and categorizes attacker behaviours by examining their tactics, techniques, and procedures (TTPs) [4]. This information is used to dynamically alter configurations, update decoy services, and modify response strategies, making the system highly adaptive [5].

The system's architecture includes a Python Flask framework and SQLite database for real-time responses, enhancing threat intelligence capture. It employs Python's logging module to meticulously record interactions, enabling detailed post-incident analysis [7]. Captured data is stored securely in SQLite databases, ensuring proper management for subsequent reporting and analysis. Machine learning models based on K-Means clustering are continuously trained on collected data to improve the system's ability to recognize and respond to novel attack patterns and all these are shown in figure 2.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131128

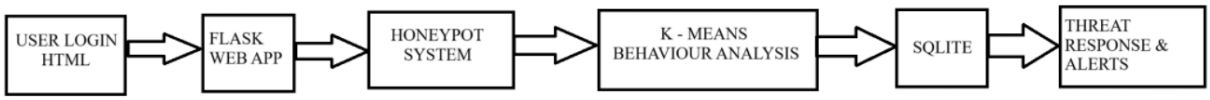

Figure 2. Block Diagram

The Adaptive Honeypot System employs behavioural data collection techniques to capture specific parameters of malicious activities, such as IP addresses, techniques used, and response patterns. This enables the development of a robust database for understanding and countering threats. The integration of dynamic rule engines and machine learning algorithms allows for the detection of anomalies and potential threats, creating a proactive defence mechanism.

Deployment scenarios highlight its versatility, as the system can be implemented in cloud environments, web applications, and IoT networks. Ethical considerations, such as ensuring compliance with privacy regulations and avoiding illegal entrapment, are integral to its design. Applications include safeguarding enterprise systems, mitigating IoT-specific threats, and serving as an educational tool for cybersecurity training. These diverse applications underscore the system's adaptability and importance in various contexts. Statistical comparisons, presented in illustrate the system's performance in different deployment environments.

V. EMERGING TRENDS AND FUTURE WORK

In order to improve danger detection and response mechanisms, adaptive honeypot systems of the future will use cutting-edge AI models such as deep learning and reinforcement learning [4]. Using scalable deployment tools, like Docker, makes it easier to implement across various settings and platforms [9]. Making systems more resistant to attacks is the goal of automated real-time threat mitigation techniques, such as patch deployment and blocking hostile IPs. Privacy-preserving techniques, such as differential privacy and federated learning, are critical for ensuring compliance with data protection regulations like GDPR [8]. These developments promote wider adoption by fostering transparency and confidence. Furthermore, new trends indicate that in order to develop a thorough threat identification framework, multimodal datasets and unified telemetry analysis should be included. This will enhance the accuracy and dependability of the system and enable more complex behavioural analysis.

VI. CONCLUSION

By using dynamic configurations and behavioural analysis to meet changing cyber threats, the Adaptive Honeypot System is a major leap in web security. Its ability to identify and successfully respond to assaults is improved by the combination of machine learning and real-time analytics [3] [4].

The system's capabilities will be strengthened by continued research and development, including AI integration and privacy-preserving mechanisms, even though issues like scalability and false positives still exist. With their creative approaches to countering advanced cyberthreats, adaptive honeypots are set to become a crucial component of contemporary cybersecurity frameworks [2] [7].

REFERENCES

[1]. Anderson, R., Sallis, M. (2023). *Honeypot detection systems: A comprehensive survey.* *International Journal of Computer Science and Security*, 14(5), 543-559.

[2]. Zhang, W., Wang, L., He, X. (2024). *Enhancing web security with adaptive honeypot systems and machine learning-based anomaly detection.* *IEEE Transactions on Information Forensics and Security*, 16(6), 1532-1545.

[3]. Yu, H., Li, Y. (2019). *Behavioural analytics for detecting advanced persistent threats using honeypot systems.* *Journal of Cybersecurity*, 7(2), 98-112.

[4]. Ahmed, M., Seraj, R., Islam, S. M. S. (2020). *The k-means algorithm: A comprehensive survey and performance evaluation*. *Electronics*, 9(8), 1295.

[5]. Altunay, H. C. (2024). *Analysis of cyber-attacks using honeypot. Black Sea Journal of Engineering and Science*, 7(5), 954-959.

[6]. Yao, J., & Chen, J. (2016). *The Design of Website Security Defence System Based on Honeypot Technology. 2nd Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2016)*. Atlantis Press.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024
DOI: 10.17148/IJARCCE.2024.131128

[7]. Jiang, H., Zhu, Z., & Wu, Y. (2018). *Intelligent Honeypot Agent for Web Security*. Journal of Internet Services and Applications, 9(1), 8-15.
[8]. Gupta, B. B., & Conti, M. (2014). *Advanced Honeypot Architecture for Network Threats Quantification and Security Enhancement*. IEEE Transactions on Information Forensics and Security, 9(1), 29-41.
[9]. Al-Shaer, E., & Al-Haj, S. (2007). *Flow-Based Management of Distributed Honeypots*. Proceedings of the 6th ACM Workshop on Recurring Malcode, 31-38.
[10]. Mokube, I., & Adams, M. (2007). *Honeypots: Concepts, Approaches, and Challenges*. Proceedings of the 45th Annual Southeast Regional Conference, 321-326.
[11]. Provos, N., & Holz, T. (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* Addison-Wesley.