International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

Adaptive Honeypot System with Machine Learning for Cyber Attack Detection

Swapnil Anil Koli[1], Prachi Pramod Chavan[2], Aniket Raghuram Menkudle[3], Karan Mahadev Patil[4]

[1,2,3,4]Department of Computer Science & Engineering, Yashoda Technical Campus Satara, Dr. Babasaheb Ambedkar University, Maharashtra, India

ABSTRACT

With the rapid growth of digital technologies and internet-based services, cyberattacks have become increasingly sophisticated and difficult to detect using traditional security mechanisms. Conventional systems such as firewalls and intrusion detection systems primarily focus on identifying and blocking known threats, but they often fail to analyze attacker behavior or detect unknown and evolving attack patterns. This creates a significant gap in modern cybersecurity, where understanding the intent and strategy of attackers is as important as preventing the attack itself.

This research proposes MazeCryptX**, an adaptive honeypot-based cybersecurity framework designed to monitor, analyze, and classify attacker activities in real time. The system deploys multiple deceptive environments, including SSH and web-based honeypots, to attract potential attackers and record their interactions. These interactions are logged and enriched with additional intelligence such as geographic location, network ownership, and potential VPN or cloud usage.**

To enhance analysis, the system integrates machine learning techniques, specifically clustering algorithms, to identify attacker personas based on behavioral patterns such as login attempts, command usage, and session duration. Additionally, suspicious files can be executed in a secure sandbox environment using containerization, allowing safe observation of malicious behavior and extraction of Indicators of Compromise (IoCs). The collected data is visualized through an interactive dashboard, providing real-time insights and enabling forensic analysis.

Keywords: Honeypot, Adaptive Honeypot Systems, Cyber Threat Intelligence, Intrusion Detection, Cybersecurity, Digital Forensics, Machine Learning, Attacker Behavior Analysis, Sandbox Analysis.

INTRODUCTION

In today's digital era, cyber threats are growing rapidly, becoming more advanced and harder to detect. Traditional security systems mainly focus on blocking attacks, but they often fail to understand how attackers behave or why they target certain systems. This lack of insight makes it difficult to predict and prevent future attacks effectively. To address this challenge, the **MazeCryptX** project introduces an intelligent and interactive cybersecurity approach using honeypots. Instead of simply stopping attackers, the system attracts them into a controlled environment where their actions can be safely observed and analyzed. By capturing login attempts, commands, and interaction patterns, the system gains valuable information about attacker behavior. Additionally, MazeCryptX enhances this data with location details, network information, and machine learning techniques to classify different types of attackers. This not only improves threat detection but also helps in understanding attack strategies in a more meaningful way.

LITERATURE REVIEW

Sr. No.	Paper Title & Year	Methodology Used	Key Contribution	Limitations
1	"A Highly Interactive Honeypot-Based Approach to Network Threat Management" (2023)	Interactive Honeypot System	Converts traditional reactive security into proactive defense using honeypots	Limited adaptability for complex real-time attacks
2	"Containerized Cloud-Based Honeypot for Tracking Attackers" (2023)	Cloud + Container-based Honeypot	Uses Docker-based honeypots for scalable attacker tracking and analysis	High resource usage in large-scale deployments
3	"Survey of Open-Source Honeypots and Tools" (2023)	Comparative Survey	Provides architecture and classification of modern honeypots	Does not include real-time adaptive intelligence
4	"Honeypot-Based Threat Detection using Machine Learning" (2023)	Machine Learning (ML) + Honeypot	Uses ML models to classify attacker behavior and detect threats	Limited dataset and real-world deployment challenges
5	"Intelligent Malware Classification using CNN in Honeypot Networks" (2024)	Deep Learning (CNN)	Detects unknown malware using AI and honeypot data	Computational complexity is high

METHODOLOGY

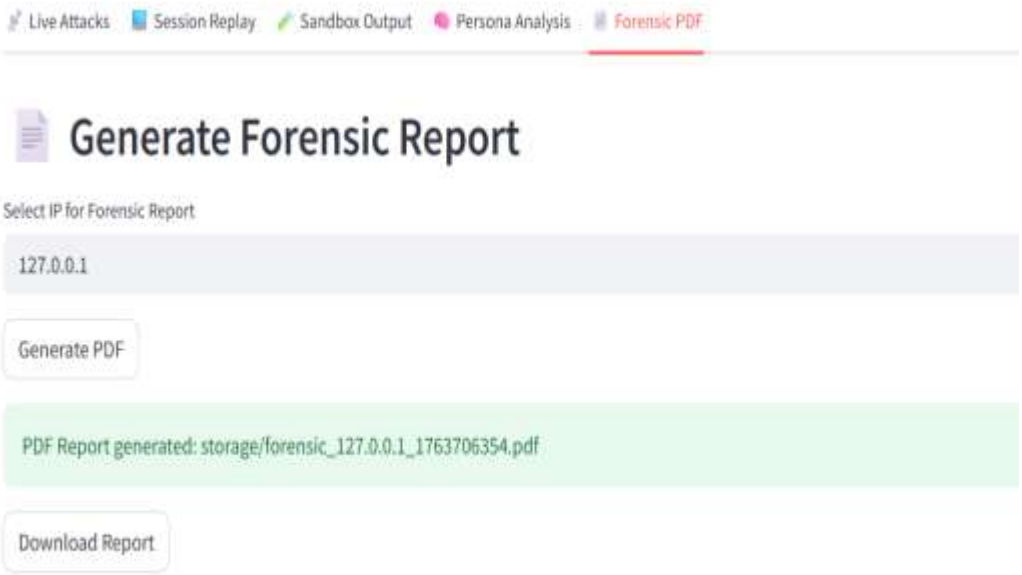
The MazeCryptX system follows a step-by-step approach to capture and analyze cyberattacks in a controlled environment. First, the system initializes and deploys SSH and web honeypots, which act as fake targets to attract attackers. When attackers interact with these honeypots, their activities such as login attempts, commands, and inputs are recorded as events. These events are then enriched with additional information like location (GeoIP), network details (ASN), and detection of VPN or cloud usage. The collected data is processed continuously using an event pipeline and stored for analysis.

To understand attacker behavior, the system applies machine learning (K-Means clustering) to classify attackers into categories such as scanners, brute-force attackers, and interactive intruders. If any suspicious files are detected, they are executed safely inside a Docker-based sandbox to observe their behavior and extract important indicators.

Finally, all the analyzed data is displayed on a Streamlit dashboard for real-time monitoring, and detailed forensic reports can be generated for further investigation. This approach helps convert cyberattacks into useful intelligence for improving security.

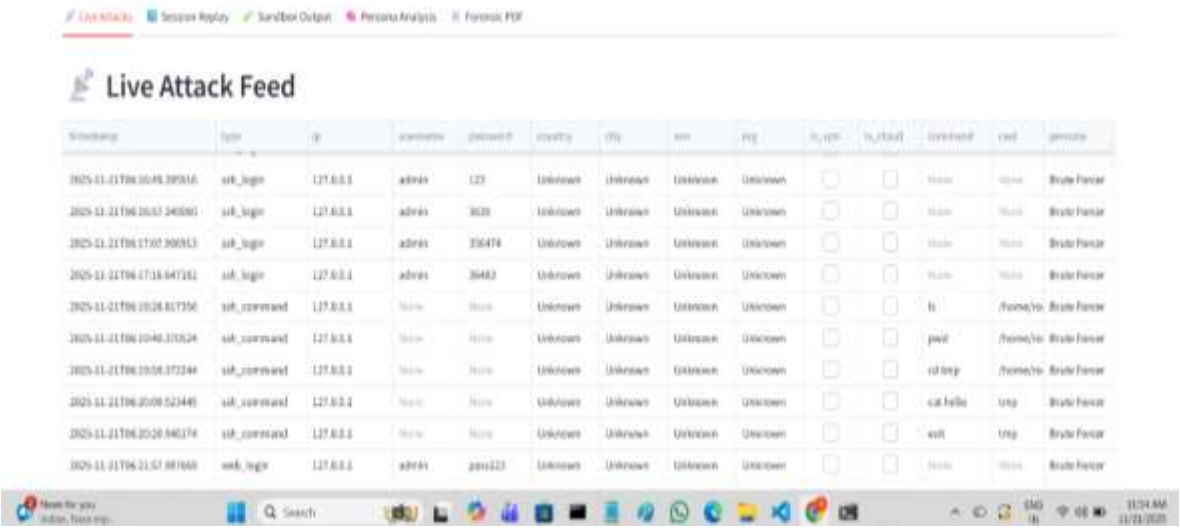
RESULTS AND DISCUSSION

1. The system confirms the report creation and provides an option to download the generated forensic report for further analysis and investigation.



2. This allows investigators to analyze attacker behavior, track system interactions, and understand the sequence of malicious activities for forensic analysis.

3. This feature helps security analysts monitor ongoing attacks, track attacker activities, and identify threat patterns for forensic investigation and threat intelligence.



4. The system successfully predicts the attacker persona as "Brute Forcer," helping analysts understand the attack behavior pattern for improved threat intelligence and response.

CONCLUSION

In conclusion, the MazeCryptX project presents an advanced and practical approach to modern cybersecurity by moving beyond traditional defensive mechanisms. Instead of only blocking attacks, the system focuses on understanding attacker behavior through the use of interactive honeypots, real-time monitoring, and intelligent analysis. By capturing attacker activities such as login attempts, commands, and interaction patterns, the system transforms malicious actions into valuable security insights.

The integration of data enrichment techniques allows the system to provide detailed information about attackers, including their geographic location, network details, and possible use of VPN or cloud services. Additionally, the use of machine learning (K-Means clustering) helps in classifying attackers into meaningful categories, enabling better understanding of their intent and strategies. The inclusion of a sandbox environment further enhances the system by safely analyzing suspicious files and extracting important indicators of compromise.

The Streamlit-based dashboard offers an interactive platform for visualizing attacks, replaying sessions, and generating forensic reports, making the system useful for both real-time monitoring and post-attack analysis. Overall, MazeCryptX successfully demonstrates how combining deception techniques, behavioral analysis, and intelligent technologies can create a more proactive and adaptive cybersecurity solution.

This project not only improves threat detection but also contributes to cybersecurity research by providing a deeper understanding of attacker behavior, making it a valuable tool for future advancements in digital security.

REFERENCES

1. M. Nawrocki, M. Wählisch, T. C. Schmidt, and C. Keil, "A Survey on Honeypot Software and Data Analysis," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1234–1265, 2023.
2. S. Dowling, M. Schukat, and E. Barrett, "A Highly Interactive Honeypot-Based Approach to Network Threat Management," *Future Internet*, vol. 15, no. 4, p. 127, 2023.
3. A. Shaghaghi, M. Rahman, and R. Buyya, "Container-Based Honeypots for Scalable Cybersecurity Monitoring," *Journal of Cloud Computing*, vol. 12, no. 1, pp. 1–15, 2023.
4. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 11, pp. 15000–15015, 2023.
5. P. Casas, J. Mazel, and P. Owezarski, "Machine Learning for Network Traffic Analysis: A Survey," *Computer Networks*, vol. 222, pp. 109512, 2023.
6. N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Boston, MA, USA: Addison-Wesley, 2022.
7. K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST Special Publication 800-94*, National Institute of Standards and Technology, 2022.
8. MaxMind Inc., "GeoLite2 Free Geolocation Data," 2023.