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

# Mazecryptx - Adaptive Honeypot & Forensic Intelligence Platform

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**

**The rapid expansion of internet connectivity and digital systems has led to a significant rise in cyber threats such as unauthorized access, malware, brute-force attacks, and advanced persistent threats, which are often difficult to detect using traditional security tools like firewalls and signature-based intrusion detection systems.**

**Honeypots provide a proactive cybersecurity approach by simulating vulnerable environments to attract attackers and capture their activities for analysis. Modern honeypot systems have evolved into intelligent platforms that integrate machine learning, behavioral analysis, and forensic intelligence to improve threat detection and investigation.**

**This review paper analyzes different honeypot architectures, including low-interaction, high-interaction, and hybrid models, along with detection techniques such as anomaly detection, sandbox analysis, and machine learning-based profiling.**

**It also highlights their benefits and limitations, identifies research gaps like lack of adaptive intelligence and automated forensic reporting, and emphasizes future directions such as AI-driven adaptive honeypots and integrated forensic intelligence platforms for stronger cyber defense.**

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

## INTRODUCTION

The rapid growth of internet and digital communication has increased cybersecurity threats such as malware attacks, unauthorized access, brute-force attacks, and data theft. Traditional security systems like firewalls and signature-based intrusion detection systems are limited because they mainly detect known threats and fail to identify new and advanced attacks. Honeypot systems provide a proactive solution by acting as decoy environments that attract attackers and allow security experts to monitor and analyze malicious activities safely.

They help in collecting important information such as attack patterns, attacker behavior, and system vulnerabilities. Modern honeypots integrated with machine learning, sandboxing, and forensic techniques improve threat detection, automate analysis, and generate detailed forensic reports. These intelligent honeypot systems enhance cybersecurity by providing better threat intelligence and supporting the development of advanced and adaptive security solutions.

## LITERATURE REVIEW

| Reference | Title / Focus | Methodology / Approach | Key Findings / Limitations | Relevance to MazeCryptx |
|---|---|---|---|---|
| Spitzner, 2003 | Honeypots: Tracking Hackers | Passive honeypots to log attacks | Effective in gathering attacker info, but static and non-adaptive | Highlights the need for adaptive honeypots |
| Provos, 2004 | Honeyd: Virtual Honeypots | Creates virtual honeypots to simulate hosts/services | Good for deception, limited forensic reporting | Inspired multi-service honeypot design |
| Pouget et al., 2015 | Adaptive Honeypots | Dynamic honeypot response to attacker behavior | Improved deception, complexity in management | Supports adaptive deception engine in MazeCryptX |
| Singh & Kim, 2017 | ML-based Intrusion Detection | Clustering and classification of attacker activity | Can identify attacker persona, lacks integration with honeypots | Basis for attacker persona clustering in MazeCryptX |
| Ruiu et al., 2018 | Sandbox Analysis of Malware | Executes malware in isolated environment, monitors behavior | Provides IoCs, safe analysis, needs automated report generation | Forms basis of MazeCryptX sandbox module |
| Ghosh et al., 2020 | Forensic Intelligence Platforms | Generates forensic reports from network events | Efficient reporting, integration with honeypots limited | Justifies automated PDF report generation in MazeCryptX |
| Mavroeidis & Bromander, 2017 | Cyber Threat Intelligence & Visualization | Dashboards for threat analysis | Real-time monitoring, visualization improves response | Supports Streamlit dashboard design and session replay |

## METHODOLOGY

This review paper follows a structured research design to analyze and evaluate existing honeypot systems, detection models, machine learning algorithms, and forensic intelligence tools used for cyber threat detection. The research design is based on a systematic review and comparative analysis of IEEE research papers focusing on honeypot-based intrusion detection and adaptive cybersecurity systems.

- **Research Design**

The research design involves collecting and analyzing peer-reviewed IEEE papers related to honeypot architectures, intrusion detection systems, and machine learning-based threat analysis. The review focuses on identifying different honeypot models, detection mechanisms, and forensic analysis techniques used in modern cybersecurity systems.

- **Models Used**

Various honeypot models have been analyzed in this review, including low-interaction, high-interaction, and hybrid honeypots. Low-interaction honeypots simulate basic network services such as SSH or HTTP to capture simple attacks, while high-interaction honeypots provide a real operating system environment to capture detailed attacker behavior. Hybrid honeypots combine both approaches to improve detection capability and reduce risk.

- **Algorithms Used**

Several detection algorithms have been studied in existing research. Rule-based detection algorithms are used to identify suspicious activities based on predefined signatures and patterns. Machine learning algorithms such as Decision Trees, Random Forest, Support Vector Machines (SVM), and Neural Networks are used to classify attacker behavior and detect anomalies. These algorithms analyze features such as attacker commands, session duration, login attempts, and network traffic patterns to identify malicious activities. Anomaly detection algorithms are also used to detect unknown and zero-day attacks by identifying deviations from normal behavior.

- **Tools Used**

Various tools and technologies are used in honeypot systems for data collection, analysis, and forensic investigation. Honeypot tools such as Cowrie and Dionaea are used to capture attacker interactions and malware samples. Malware sandbox environments are used to safely execute and analyze suspicious files. Machine learning frameworks such as

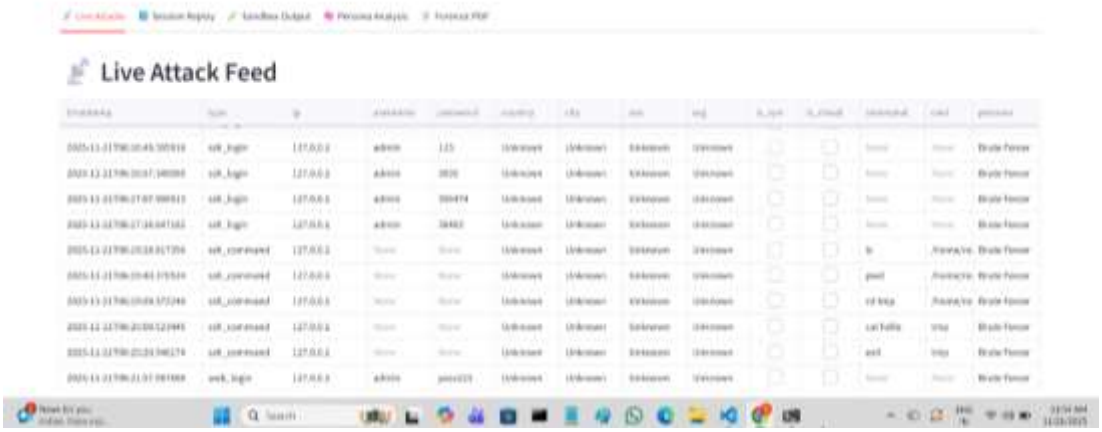
Python, Scikit-learn, and TensorFlow are used to develop attacker classification models. Additionally, forensic intelligence dashboards and monitoring tools are used to visualize attack data, replay attacker sessions, and generate automated forensic reports. These tools help improve threat detection, analysis, and incident response.

## 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

This review paper analyzed the role of honeypot systems in improving cyber threat detection, analysis, and forensic investigation. The findings show that honeypots are effective in attracting attackers and collecting valuable information about attack patterns, malware behavior, and system vulnerabilities. While traditional low-interaction and rule-based honeypots are simple and easy to deploy, they have limitations in detecting advanced and unknown threats. In contrast, high-interaction and machine learning-based honeypots provide better detection accuracy, deeper behavioral insights, and stronger threat intelligence capabilities. Modern adaptive honeypot systems integrated with artificial intelligence, sandbox analysis, and forensic dashboards further enhance automated threat detection and investigation. However, challenges such as high computational requirements, scalability issues, and limited automation still remain. In the future, the development of AI-driven, cloud-based, and fully automated honeypot systems with real-time monitoring and response mechanisms will play a significant role in strengthening cybersecurity and supporting advanced digital forensic investigations.

## REFERENCES

1. An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy Daniel Fraunholz, Marc Zimmermann, Hans D. Schotten Intelligent Networks Research Group, German Research Centre for Artificial Intelligence, Trippstadter Str. 122, 67663 Kaiserslautern, Germany Hans_Dieter.Schotten@dfki.de Daniel.Fraunholz@dfki.de, Marc.Zimmermann@dfki.de,

2. Blind Attack Flaws in Adaptive Honeypot Strategies Muath Obaidat, Senior Member, IEEE Computer Science City University of New York New York, NY 10019 muobaidat@ccny.cuny.edu Joseph Brown Computer Science City University of New York New York, NY 10019 joseph.brown1@jjay.cuny.edu
3. An adaptive honeypot deployment algorithm based on learning automata Yan Zhang, Chong Di, Zhuoran Han, Yichen Li and Shenghong Li Department of Electronic Engineering Shanghai Jiao Tong University Shanghai, {jessiezhang1993,dichong95,hzrtom,liyichen,shli}@sjtu.edu.cn China 200240 Email:
4. D-FRI-Honeypot: A Secure Sting Operation for Hacking the Hackers Using Dynamic Fuzzy Rule Interpolation Nitin Naik , Changjing Shang
5. A Mimic Honeypot Construction Method Based on Incomplete Information Zero-Sum Stochastic Games and Q-Learning Sisi Shao , Zongkai Ji, Xukun Qian, Fei Wu
6. Know Your Enemy: Analysing Cyber-threats Against Industrial Control Systems Using Honeypot S. M. Zia Ur Rashid∗, Mohammad Jalal Uddin† and Ariful Islam‡ Department of Electrical and Electronic Engineering International Islamic University Chittagong, Bangladesh Email: ∗smziaurrashid@gmail.com, †jalaliiuc@gmail.com, ‡smarifulislam.me@gmail.com
7. QRASSH–Aself-adaptive SSH Honeypot driven by Q-Learning Adrian Pauna1 , Andrei Constantin Iacob2,andIonBica3 1 Faculty of Military Electronic and Information Systems, Military Technical Academy, Bucharest, Romania 2 Faculty of Computer Science, A. I. Cu a niversity of IA I, Iasi, Romania 3 Faculty of Military Electronic and Information Systems, Military Technical Academy, adrian.pauna.ro@gmail.com Bucharest, Romania Contact author e-mail:
8. An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy Daniel Fraunholz, Marc Zimmermann, Hans D. Schotten Intelligent Networks Research Group, German Research Centre for Artificial Intelligence, Trippstadter Str. 122, 67663 Kaiserslautern, Germany Hans_Dieter.Schotten@dfki.de Daniel.Fraunholz@dfki.de, Marc.Zimmermann@dfki.de,
9. Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats Phani Lanka *, Khushi Gupta and Cihan Varol