IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, November 2025
Impact Factor: 7.67

INTRUDEX: Intelligent Honeypot-Based Threat Monitoring System

Ingle Ram Vilas, Jadhav Vaishnav Pravin, Wagh Yashraj Kakasaheb, Prof. Bhor. P. G.
Department of Computer Engineering
Samarth College of Engineering and Management, Belhe, Pune

Abstract: *In today's digital era, cyberattacks have become more frequent, sophisticated, and dam-aging. Organizations face continuous threats from malicious actors targeting sensitive data,critical infrastructures, and online services. Traditional defense mechanisms such as fire-walls and intrusion detection systems often fail to provide deep insights into attacker be-havior.To address this challenge, a Cybersecurity Honeypot Simulation System is proposed, whichacts as a decoy environment to attract, detect, and analyze malicious activities in realtime.The system deploys multi-interaction honeypots that emulate real network services such as SSH, HTTP, and database systems. These traps deceive attackers into interacting with decoy systems, allowing detailed monitoring and data capture of their activities. Us-ing advanced log analysis and machine learning techniques, IntrudeX identifies malicious patterns, classifies attack types, and extracts valuable threat intelligence. The enriched data is visualized through dashboards for better understanding and faster response. The system deploys honeypot environments like SSH and Telnet traps (using tools suchas Cowrie) to lure attackers by mimicking real services. All interactions are logged and securely forwarded to a centralized data pipeline, where Logstash performs parsing and enrichment, including GeoIP tagging of attacker IP addresses. This project demonstrates how honeypots not only function as an early-warning system but also as an intelligence-gathering tool, helping security teams understand evolving attack patterns. By simulating realistic targets while ensuring isolation from production networks, the proposed system offers a cost-effective, scalable, and practical approach for improving cyber defense strategies. Enhancing early threat detection and providing actionable insights into attacker tactics, techniques, and procedures (TTPs). By integrating deception technology with analytics, IntrudeX strengthens cybersecurity resilience and contributes toward developing proactive defense strategies for both enterprise and academic environments.*

Keywords: Cybersecurity Honeypot Simulation System

I. INTRODUCTION

The rapid expansion of the digital world has transformed how individuals, organizations, and governments operate. However, this growth has also brought an alarming rise in the number and complexity of cyber threats. Attackers today employ advanced techniques such as brute force, phishing, ransomware, and zero-day exploits to compromise critical systems. Traditional security mechanisms like firewalls, intrusion detection systems (IDS), and an- tivirus solutions are effective to an extent, but they often lack the ability to provide in-depth insights into the motives, tools, and strategies used by adversaries. This creates a strong need for proactive mechanisms that not only defend but also study attacker behavior to strengthen long-term security.

In this context, honeypots have emerged as a powerful cybersecurity mechanism. A hon- eypot is a decoy system or service designed to attract attackers, monitor their activities, and collect intelligence without endangering real assets. By simulating vulnerable targets, honeypots help in detecting early intrusion attempts, analyzing malicious traffic, and gen-erating valuable datasets for improving defense strategies. Their role has become highly relevant in today's scenario where cyberattacks are increasing both in frequency and so-phistication.

The IntrudeX system leverages this concept by deploying a network of multi-interaction honeypots capable of simulating realistic targets. The system captures malicious activities,logs attacker behavior, and enriches the data with

DOI: 10.48175/IJARSCT-29687

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, November 2025 Impact Factor: 7.67

contextual intelligence using analytical tools. Visualization through dashboards enables real-time threat monitoring and proactive decision-making.

Problem Defination

The increase in cyber-attacks has revealed serious limitations in traditional security systems, which are mostly effective at blocking only known threats but fail to provide in-sight into the evolving behavior and techniques of modern attackers.

This leaves a major gap: there isn't an affordable, practical, and educational platform that allows safe observation and analysis of real attacker behavior. Therefore, there is an ur- gent need for a cost-free honeypot-based system that can attract real-world attackers, log their methods in a controlled environment, and transform this data into valuable insights for research, threat intelligence, and cybersecurity training, without requiring significant financial investment or complex infrastructure

- Simulate real network environments safely.
- Record, analyze, and classify attacker activities.
- To detect and log unauthorized network activities in a safe environment.
- To analyze real-time cyberattacks without risking production assets.
- Visualize global attack patterns and identify active threat sources.
- Generate actionable insights for early detection and prevention of threats.
- IntrudeX addresses this by deploying multiple honeypots integrated with real-time analytics to capture and analyze attacker behavior.
- Traditional intrusion detection systems (IDS) and firewalls can generate many false positives and provide only limited insight into attacker intent.
- Real-world collection of malicious cyber activity is often incomplete, scattered, or ethically constrained, leading to gaps in threat understanding.

Hands-on learning and research platform for students, researchers, and organizations, many of whom lack access to expensive commercial security solutions. By deploying a versatile honeypot system, we can capture real-world attack techniques, enrich threat intelligence, and create a valuable training ground for understanding attacker behavior

Objectives

The system aims to comprehensively collect and centralize security event data fromhoneypot interactions, preprocess and enrich this data with contextual information such as geolocation and attack patterns, and efficiently store it using scalable databases. Real-time visualization through advanced dashboards will facilitate the identification of attack trends and techniques, while integration of machine learning models will enable anomaly detec- tion and classification of threats.

- Deploy multiple types of honeypots (e.g., SSH, malware, web application) to actively attract and capture real-world cyber-attacks.
- Log and analyze attacker activity, including IP address, geographic location, attack techniques, submitted commands, and malicious payloads.
- Enrich captured threat data using global intelligence feeds (such as HoneyDB), GeoIP lookup, file hashing, and malware analysis tools.
- Visualize collected data through dynamic, real-time dashboards using the ELK stack and Grafana to simplify log analysis and enable quick threat responses.
- Provide an accessible educational and research platform for students, researchers, and cybersecurity professionals to safely observe and study cyber-attacks.
- Establish a foundation for integrating advanced machine learning models (for anomaly detection, clustering, and threat prediction) to further automate analysis and improve detection capabilities.
- Support ongoing cybersecurity training through interactive labs and simulated attack scenarios to enhance practical defense skills.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, November 2025 Impact Factor: 7.67

• Demonstrate the feasibility of a low-cost, scalable, and extensible honeypot system for organizations and educational institutes without access to expensive commercial alternatives.

II. LITERATURE SURVEY

1. Virtual Honeypots: From Botnet Tracking to Intrusion Detection
AUTHOR NAME :Niels Provos, Thorsten Holz YEAR:2021
SUMMARY :This book details the use of honeypots such as Honeyd in detecting and analyzing worms, malware, and botnets. It reviews multiple real-world de- ployments of honeypot systems and explains how these deceptive environments play a crucial role in identifying attack sources and behavior patterns.

2. Honeypots: Tracking Hackers
• AUTHOR NAME :Lance Spitzner
• YEAR:2013
• SUMMARY: Spitzner introduces the concept of honeypots as intentional security resources designed to attract and be attacked by hackers. The book demonstrates how honeypots reveal attacker tactics, tools, and motives, aiding in proactive de- fense strategies.The author further emphasizes the role of honeypots in threat detection, incident response, and forensic analysis, showing how captured data can be used to strengthen security policies and improve intrusion detection signatures.

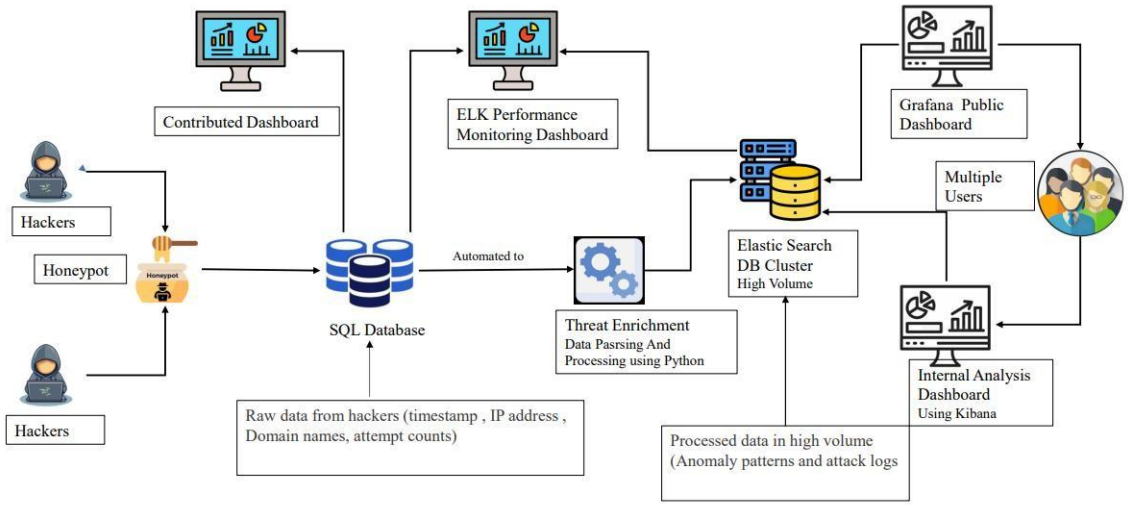
3. Honeypot-Based Forensics
• AUTHOR NAME :F. Pouget, M. Dacier
• YEAR:2020
• SUMMARY: This research emphasizes the forensic application of honeypots, us- ing low- interaction decoy systems to monitor and capture evidence such as wor propagation and attack patterns. Their findings highlight honeypots' roles in dig- ital forensics and attack analysis.

4. Honeypots: Concepts, Approaches, and Challenges
• AUTHOR NAME : I. Mokube, M. Adams
• YEAR:2022
• SUMMARY: Presented at the ACM conference, this paper surveys various types of honeypots, their deployment strategies, strengths, and challenges. It discusses honeypots' effectiveness in research and network defense, while noting chal- lenges in scalability and attacker detection.

5. Research on Honeypot Technology for Network Security
• AUTHOR NAME :Y. Zhang, Y. Jiang, H. Liu
• YEAR:2015
• SUMMARY:This journal paper analyzes the technological developments and applications of honeypots in network security. The authors discuss how hon eypots help collect valuable attacker data, enhance threat intelligence, and adapt to evolving cyber risks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, November 2025
Impact Factor: 7.67

III. SYSTEM ARCHITECTURE



System Models:

1. High-Level Architecture Model:

To decoy honeypot environment (multiple protocols/services like SSH, web, database). Monitoring and logging layer, which captures and securely stores all attacker interactionsand events. Analysis and visualization layer, where data is parsed, enriched with external threat intelli- gence, and displayed through real-time dashboards

2. Functional Workflow Model: All activities access attempts, payloads, commands are logged.Logs are processed, enriched (GeoIP, HoneyDB), and visualized.

3. Data Flow Model:Data flows from the attacker into the honeypot, is collected by monitoring agents, sent the log management system (ELK/Logstash), further enhanced by threat intelligence APIs and finally delivered to the user via dashboards or reports.

4. User Interaction Model: Role-based access allows admins to configure honeypots and review all data, while re-searchers/students can visualize attacks, extract reports, and participate in training labs.

5. Security Isolation Model: All honeypot instances are sandboxed or network-isolated to prevent any impact on actual production systems, and strict authentication controls are enforced across all user interac-tions.

6. Training Simulation Model: Provides a simulated environment where safe attack scenarios and exercises are created foreducational and testing purposes, supporting interactive learning and skills assessment

System Flow and algorithm

Step-by-Step System Flow

1. Attacker Initiates Connection:

The attacker scans and targets open ports exposed intentionally by the honeypot sensors.

2. Honeypot Interaction Captured:

The honeypot records attacker activity including credentials, commands, scripts, and malware payloads.

3. Log Forwarding to Collector:

All raw logs and artifacts are securely forwarded to a centralized Collector module.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, November 2025 Impact Factor: 7.67

4. Data Parsing C Artifact Preservation:
Log Parser normalizes the event data while Artifact Store securely stores malware samples.
5. Threat Analysis:
o Static Analysis: File signatures, strings, metadata, and hash patterns are extracted.
o Dynamic Analysis: Malware is executed inside a controlled sandbox to observe runtime behavior.
6. IOC Extraction C Threat Enrichment:
Host indicators (IP, file hash, domains) are matched with external threat intelligence feeds.
7. Analytics C Alerting:
Dashboard presents visualizations of ongoing attacks, frequency trends, and threat severity levels.
8. Security Response:
Admin/researcher can use the intelligence for firewall rule updates, blacklisting, or incident reporting.
Algorithm: Honeypot-Based Threat Capture and IOC Generation Input:
Incoming connections and payloads from attackers Output:
Extracted and enriched Indicators of Compromise (IOCs) Step 1: Initialize Honeypot Sensor on selected ports.
Step 2: Listen for inbound traffic continuously.
Step 3: If connection request received: Record session metadata (source IP, timestamp, protocol) Log all commands and actions performed by attack If payload is detected: Save artifact to Artifact Store.
Step 4: Send logs and artifacts to Collector Module.
Step 5: Perform Static Analysis: Extract file hash, metadata, signatures.
Step 6: Perform Dynamic Analysis in Sandbox: Execute payload and observe system calls, network behavior, and modifications.
Step 7: Extract Indicators of Compromise (IOCs) from results.
Step 8: Query Threat Intelligence database or API: Compare extracted IOCs with known malicious entities.
Step 9: Store IOCs along with enriched intelligence in Database. Step 10: Update Dashboard with:
- Attack source activity logs
- Behavioral analysis outcomes
- Threat severity and status
Step 11: If new threat detected:
Trigger alert to system administrator.
Step 12: End.

IV. CONCLUSION

The IntrudeX Honeypot-Based Threat Monitoring System successfully demonstrates the potential of using intelligent honeypots for proactive cyber threat detection and analysis. By integrating honeypot-based data collection, machine learning–driven classification, and real-time visualization, the system provides a comprehensive approach to network monitor- ing and intrusion response. It not only helps identify attack sources and behavioral patterns but also contributes to strengthening the organization's cybersecurity posture through con- tinuous intelligence gathering.
The project effectively achieved its objectives of creating a scalable, modular, and adap- tive threat monitoring framework capable of capturing real-world attack data. Through iterative development using the Agile methodology and structured review mechanisms, In- trudeX maintained technical accuracy, efficient performance, and strong documentationintegrity.
The knowledge gained from the development and testing of this system provides a solid foundation for future enhancements, including advanced AI-driven analytics, automated mitigation, and cloud-based integration. From an academic and practical standpoint, the development of IntrudeX provided valu- able insights into cyber threat intelligence collection, honeypot architecture design, and real-time intrusion analysis. The system lays a strong foundation for further research in automated attack classification, AI-driven defense mechanisms, and adaptive honeynet deployment.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, November 2025 Impact Factor: 7.67

In the future, the project can be extended to integrate cloud-based honeypots, federated intelligence sharing, and autonomous incident response, making it scalable and suitable for enterprise-grade security environments. Overall, IntrudeX represents a significant step toward achieving smarter, data-centric, and self-evolving cybersecurity infrastructures

ACKNOWLEDGMENT

The completion of a project is a milestone in student life and its execution is inevitable ithe hands of guide. We are highly indebted the project guide Prof Bhor.P.G and Project Coordinator Prof. Shegar S. R. for there valuable guidance and appreciation for giving form and substance to this report and project. It is due to her enduring efforts, patience and enthusiasm which has given a sense of direction and purposefulness to this project andultimately made it a success. We would like to tender our sincere thanks to the staff members and H.O.D. Prof. Shegar S. R. for their co-operation. We would like to express our deep regards and gratitude to the PRINCIPAL Dr. Narawade N. S. . We are also thankful to our parents for promoting and motivating us regarding our project development. We would wish to thank the non-teaching staffs who have helped us all the way in one way or the other. It is highly impossible to repay the debt of all the people who have directly or indirectly helped us performing the project Finally, we would like to thank to all our staff members of Computer Engineering Depart- ment who helped us directly or indirectly to complete this work successfully.

REFERENCES

[1]. Singh, R. K. Ramajujam, T. "Intrusion Detection System Using Advanced Honey- pots." arXiv, 2009. arxiv.org.
[2]. "Honeypots in network security: a survey." ACM Digital Library. dl.acm.org
[3]. "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems." ResearchGate. ResearchGate
[4]. "Honeypot-based intrusion detection system: A performance analysis." ZIEN Jour- nals. zienjournals.com
[5]. "The effect of using honeypot network on system security." Growing Science. grow- ngscience.com
[6]. "Enriching Honeypot Data Using Cyber Threat Intelligence." Carnegie Mellon SEI.sei.cmu.edu
[7]. "Advancing Cybersecurity with Honeypots and Deception Strategies." MDPI. MDPI
[8]. "A Systematic Review of Honeypot Data Collection, Threat Intelligence Platforms, and AI/ML Techniques." SSRN. papers.ssrn.com+1
[9]. "Dynamic Interactive Honeypot for Web Application Security." ResearchGate. Re- searchGate
[10]. "A Highly Interactive Honeypot-Based Approach to Network Threat Analysis." MDPI. MDPI
[11]. "Honeypot: Intrusion Detection System." IJESTE. lamintang.org
[12]. "Network Intrusion Detection System Using Honeypot in Cloud Computing Environ- ment.JISAE. ijisae.org+1
[13]. "Honeypots – Security by Deceiving Threats." micsymposium.org. micsymposium.org
[14]. "Honeypot-based Secure Network System." ResearchGate. ResearchGate
[15]. "Honeypots: Their Analysis, Evaluation and Future." Preprints. preprints.org