iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80912

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

DecoyShield: A Deception-Based Framework for Proactive Threat Detection and Cyber Defense

Naja Sherin M[1], Nayana N N[2], Sneha N[3], Sujisha M[4], Ms. Anu Treesa George[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering (Cyber Security) Vimal Jyothi Engineering College, Chemperi, Kannur*
[5]*Assistant Professor Department of Computer Science Vimal Jyothi Engineering College, Kannur*

Abstract: ***Modern cybersecurity systems predominantly rely on reactive defense mechanisms that detect threats only af- ter malicious activity has occurred, making them ineffective against advanced and evolving attack techniques such as zero- day exploits, automated scanning and stealthy reconnaissance. Traditional intrusion detection systems struggle to identify early-stage attacks due to their dependence on known signatures and predefined rules. To address these limitations, this work proposes DecoyShield, an intelligent deception-based cybersecu- rity framework designed for proactive threat detection, attacker engagement and real-time analysis. DecoyShield leverages multi- service honeypot environments to simulate realistic network services and lure attackers into controlled decoy systems, en- abling the capture of attacker behavior, commands and interac- tion patterns. The system integrates behavioral analysis, threat intelligence and dynamic risk scoring to classify threats into low, medium and high severity levels. Based on the assessed threat level, an adaptive deception engine selectively deploys fake service banners or interactive sandbox environments to maximize attacker engagement while minimizing risk to real assets. Additionally, DecoyShield provides real-time visualization through a live dashboard, detailed attack logging and automated alert mechanisms for critical incidents. By combining decep- tion technology with intelligent analytics and adaptive response strategies, DecoyShield enhances early threat detection, improves situational awareness and provides valuable insights into attacker tactics, techniques and procedures (TTPs), thereby strengthening overall cybersecurity posture.***

Index Terms: ***Honeypot, Cyber Deception, Threat Detection, Intrusion Detection, Threat Intelligence, Attack Analysis, Net- work Security, Adaptive Defense, Security Monitoring.***

I. INTRODUCTION

The growing reliance on interconnected networks and digital services has significantly increased the exposure of systems to cyber threats. Modern computing environments operate across cloud platforms, enterprise networks and distributed infrastructures, making them more complex and harder to secure. As a result, these systems are increasingly targeted by sophisticated attacks such as automated port scanning, brute-force attempts, zero-day exploits and advanced persistent threats. Traditional security solutions, which primarily depend on signature-based detection and reactive defense mechanisms, are often insufficient to detect and prevent such evolving threats at an early stage.

Recent research proposes a multi-tier honeypot architecture that enhances network security by combining different levels of honeypots with traditional defense mechanisms such as firewalls and intrusion prevention systems. The system redi- rects suspicious traffic into layered honeypot environments, allowing detailed observation of attacker behavior across var- ious stages, including reconnaissance and exploitation. By integrating low, medium and high-interaction honeypots, the approach improves threat detection, supports digital foren- sics and strengthens both proactive and post-attack defense strategies. Experimental results show that this architecture significantly improves intrusion detection performance and effectively mitigates attacks such as DDoS while maintaining system availability [1].

Recent studies in deception-based security highlight ad- vanced honeypot systems for detecting and analyzing net- work attacks. The Ganesha Honeypot System (GHOST) en- hances SSH security by simulating vulnerable environments and capturing attacker activities such as brute-force attempts, improving visibility into intrusion behavior [2]. Building on this, Anwar et al. proposed an adaptive honeypot allocation strategy using game theory and reinforcement learning to dynamically deploy decoys, effectively misleading attackers and strengthening overall network defense [3].

Advancements in system design have been influenced by intelligent interaction technologies and evolving cybersecurity strategies. Das¸demir [4] demonstrated how Brain-Computer Interfaces integrated with Virtual Reality can enhance user interaction by replacing traditional input methods. In the cybersecurity domain, deception-based approaches such as adaptive honeypots play a key role by dynamically adjusting system behavior to engage attackers and collect valuable threat intelligence [5].

©IJRASET: All Rights are Reserved

Despite these developments, there is still a need for integrated solutions that combine adaptive deception with effective monitoring and analysis mechanisms for improved security.

Despite advancements in intelligent systems and cyberse- curity approaches, there is still a lack of a unified solution that integrates adaptive intelligence with proactive security. Existing methods largely depend on signature-based detection and external processing, making them less effective against emerging threats and raising privacy concerns.

II. OVERVIEW OF DECOYSHIELD

DecoyShield is an intelligent deception-based cybersecurity framework designed to enhance proactive threat detection and analysis in modern network environments. Unlike traditional security systems that rely on reactive, signature-based mech- anisms, DecoyShield actively engages potential attackers by deploying realistic honeypot services across multiple ports, thereby luring malicious actors into controlled environments. The system incorporates behavioral analysis to monitor attacker interactions such as scanning patterns, command execution and session activity in real time. Based on this analysis, threats are dynamically classified into low, medium or high levels, enabling adaptive responses such as fake service banners or interactive sandbox environments for deeper inspection. Additionally, DecoyShield integrates threat intel- ligence, centralized logging and real-time dashboard visualization to provide actionable insights and automated alerting. By combining deception techniques with intelligent analysis, DecoyShield offers a secure, scalable and proactive solution for strengthening cybersecurity defense.

A. Key Features

1) Multi-Port Honeypot Engine (Core Deception Mod- ule):
- Deploys multiple fake services across commonly targeted and randomized ports to simulate a realistic network environment.
- Attracts attackers into controlled decoy systems, en- abling safe observation without exposing real assets.

2) Behavioral Analysis Engine:
- Continuously monitors attacker interactions such as connection frequency, port scanning patterns and session behavior.
- Identifies attack intent (e.g., reconnaissance, brute- force, automated scanning) and supports real-time threat classification.

3) Adaptive Threat Scoring and Classification:
- Dynamically calculates risk scores based on attacker behavior, including scan speed and number of tar- geted ports.
- Classifies threats into LOW, MEDIUM and HIGH levels to enable intelligent response decisions.

4) Interactive Sandbox Environment:
- Redirects high-risk attackers into a simulated command-line environment that mimics a real sys- tem.
- Captures attacker commands (e.g., whoami, ls, cat) to analyze behavior while preventing access to ac- tual resources.

5) Deceptive Service Banner System:
- Generates realistic service responses (FTP, SSH, HTTP, etc.) to mislead attackers during initial prob- ing.
- Enhances attacker engagement and prolongs inter- action for deeper intelligence collection.

6) Threat Intelligence and Logging System:
- Enriches attack data using external threat intelli- gence sources (e.g., abuse confidence, geolocation).
- Stores detailed logs including IP, commands, session duration and attack type for analysis and reporting.

7) Real-Time Dashboard and Alerting System:
- Provides live visualization of attack activity, threat distribution and attacker statistics.
- Sends automated alerts (e.g., email notifications) for high-severity threats to ensure rapid response.

DecoyShield integrates deception technology, behavioral an- alytics and adaptive threat response to proactively detect, analyze and mitigate cyber attacks in real time.

III. PROPOSED SYSTEM AND DESIGN

DecoyShield is designed as a proactive cybersecurity system that focuses on detecting, misleading and analyzing attackers in real time rather than simply blocking them. Instead of relying on traditional signature-based detection, the system creates a deceptive network environment that attracts attackers and studies their behavior in a controlled manner. The overall design follows a modular approach where each component works together to identify threats, classify them and respond intelligently.

The system is composed of the following core components:

1) Multi-Port Honeypot Engine: This module forms the foundation of the system by deploying multiple decoy services across commonly targeted and dynamically gen- erated ports. It simulates realistic network environments, attracting attackers into controlled spaces where their activities can be safely monitored without exposing real assets.

2) Behavioral Analysis and Threat Scoring Engine: This component continuously monitors attacker interactions, including connection patterns, scanning behavior and command execution. Based on these parameters, it calcu- lates a dynamic threat score and classifies attackers into low, medium or high threat levels, enabling intelligent decision-making.

3) Adaptive Response and Sandbox Module: Depending on the threat level, the system dynamically responds by presenting fake service banners or redirecting high- risk attackers into an interactive sandbox environment. This sandbox simulates a real system interface, allowing detailed observation of attacker commands while ensuring complete isolation from actual resources.

4) Threat Intelligence Integration Module: DecoyShield enhances detection accuracy by integrating external threat intelligence sources, such as IP reputation services and geolocation analysis. This module provides contextual insights, including abuse confidence scores and historical reports, improving threat assessment.

5) Centralized Logging and Database System: All attack- related data, including IP address, location, commands executed, session duration and threat classification, is securely stored in a centralized database. This enables comprehensive analysis, reporting and long-term tracking of attacker behavior.

6) Real-Time Dashboard and Alerting System The sys- tem provides a live monitoring dashboard that visualizes attack activity, threat distribution and attacker statistics. Additionally, automated alerting mechanisms notify ad- ministrators of high-severity threats, enabling rapid re- sponse and mitigation.

Overall, the DecoyShield framework provides a robust and scalable solution for modern cybersecurity challenges by com- bining deception technology, behavioral analytics and adaptive defense strategies. By shifting from reactive detection to proactive engagement, it improves threat visibility, enhances situational awareness and enables deeper understanding of attacker tactics, techniques and procedures (TTPs), thereby strengthening the overall security posture

A. System Architecture

DecoyShield uses a layered architecture to detect and an- alyze attacks through deception and behavioral monitoring. Incoming traffic first reaches the Network & Access Layer, where multiple decoy ports simulate real services. A port- knocking mechanism allows only authorized users to access the hidden real service, while unauthorized traffic is redirected for analysis.

The Intelligence API Layer enriches incoming data using IP reputation and geolocation services. This data is then pro- cessed by the Analytics & Decision Engine, which evaluates attacker behavior and classifies threats as low, medium or high. Based on the threat level, the Deception Layer generates adaptive responses, such as fake service banners or an interac- tive sandbox for deeper engagement. All activities are stored in the Storage & Alerting Layer, and critical threats trigger alerts. Finally, the UI Layer provides real-time monitoring and visualization through a dashboard.

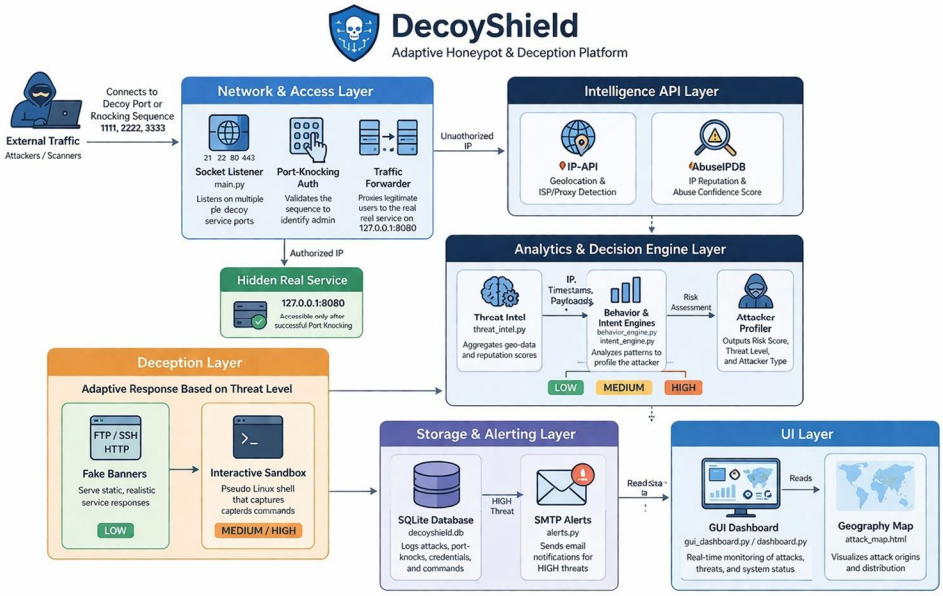


Fig. 1. System Architecture

B. System Design

The DecoyShield system is designed to interact with exter- nal users or attackers through exposed decoy ports. Incoming requests are captured and analyzed instead of directly access- ing real services. The system evaluates behavior using threat intelligence and assigns a risk level (low, medium or high).

Based on this analysis, DecoyShield responds dynamically by either showing fake service banners or redirecting attackers into an interactive sandbox. All activities are logged and visualized in a dashboard, while high-risk actions trigger alerts. This design ensures secure access for legitimate users and controlled engagement for attackers.

The Data Flow Diagram represents how data flows within the DecoyShield system, with the system acting as a central entity between the attacker and the admin. The attacker initi- ates connection attempts or port scans, which are intercepted and analyzed by DecoyShield. Instead of granting real access, the system responds with deceptive outputs such as fake service banners while logging all attack details in the database.

At the same time, the admin or security analyst interacts with the system for monitoring and configuration. DecoyShield provides alerts, threat levels and detailed reports, enabling real-time visibility and effective decision-making. This design ensures continuous monitoring, secure data handling and con- trolled interaction with potential attackers.

- Input: The process begins when the Attacker initiates connection attempts or port scanning activities toward the DecoyShield system.
- Process: The DecoyShield System captures these re- quests, analyzes the traffic and generates deceptive re- sponses such as fake service banners while logging attack details (IP, port, timestamp) into the Attack Log Database.
- Feedback: The system provides fake service responses back to the attacker, while simultaneously sending alerts, threat levels and reports to the Admin/Security Analyst for monitoring and decision-making.

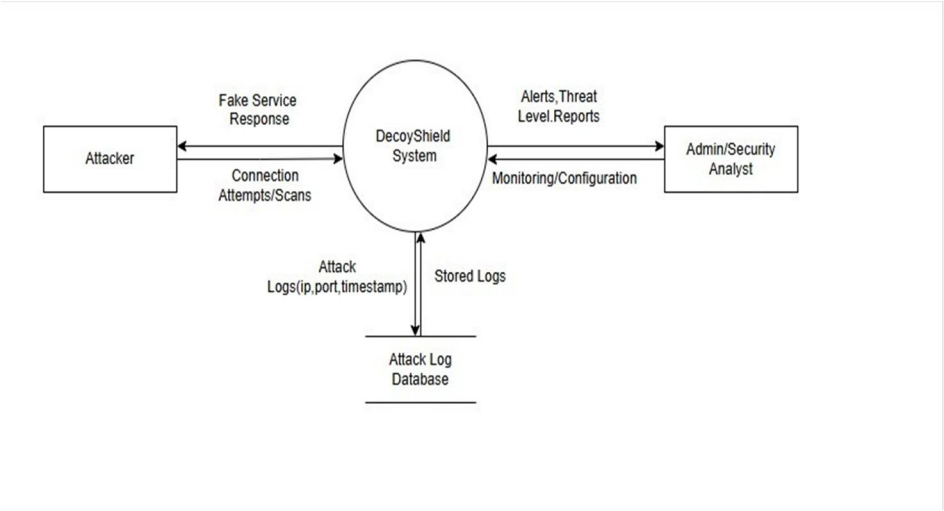


Fig. 2. Data Flow Diagram (Level 0)

The Level 1 Data Flow Diagram expands the DecoyShield system by detailing the interaction between its internal mod- ules, including traffic analysis, threat evaluation, deception mechanisms and the attack log database.

- Traffic Monitoring & Analysis: Incoming suspicious traffic is first processed by the Connection Monitoring module, which detects anomalies and forwards data to Attacker Behavior Analysis. This module evaluates attack patterns using logs and generates insights about attacker intent and activity..
- Deception Control Mechanism: The Decoy Port Man- agement and Adaptive Deception Control modules work together to dynamically respond to threats. Based on the analyzed behavior, the system generates appropriate deception strategies such as fake services or controlled interactions, while updating attacker profiles
- Data Storage & Profiling: Attack details, including logs and session data, are stored in the Attack Log Database, while processed behavioral information is maintained in the Attacker Profile Database. This ensures continuous learning and improved threat detection.
- Alerting & Administration: The Alert and Report Man- agement module sends real-time alerts and reports to the Security Admin, enabling monitoring, configuration and timely response to potential threats.

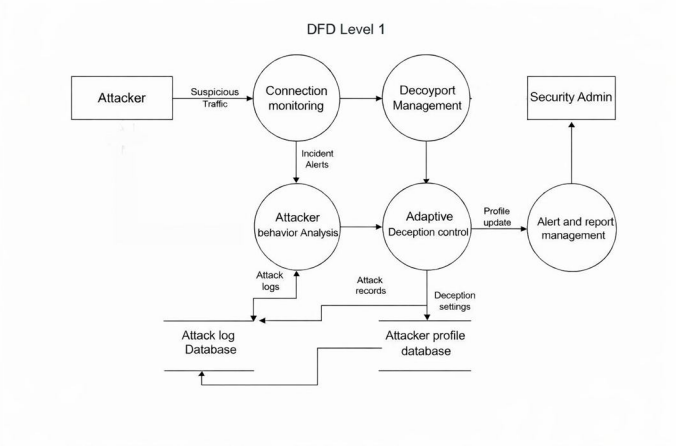


Fig. 3. Data Flow Diagram (Level 1)

IV. IMPLEMENTATION

The development of DecoyShield followed a phased ap- proach to ensure effective threat detection and response. Ini- tially, network monitoring and decoy ports were implemented to capture incoming traffic. This was followed by integrating threat analysis and risk classification modules. Finally, adap- tive deception, logging and alerting components were added to enable dynamic responses and real-time monitoring.

A. *Modules*

1) *Phase 1: System Design and Architecture:* The initial phase focused on designing the layered architecture of DecoyShield, including network access, analysis and deception components. This stage defined system workflows, data flow and integration of core modules.
2) *Phase 2: Network Monitoring and Threat Intelligence:* This phase involved implementing socket listeners, port- knocking mechanisms and traffic monitoring to capture in- coming connections. External threat intelligence APIs were integrated to enrich data with IP reputation and geolocation details.
3) *Phase 3: Behavioral Analysis and Adaptive Deception:* In this phase, behavior analysis and intent evaluation modules were developed to classify threats. Based on risk levels, adaptive deception techniques such as fake service banners and interactive sandbox environments were implemented.
4) *Phase 4: Logging, Alerting and Visualization:* The final phase focused on storing attack data in databases, generating real-time alerts and building a dashboard for monitoring. This ensured effective visualization, reporting and administrative control over detected threats.

B. *Tools And Techniques*

The development of DecoyShield utilizes a combination of network programming, threat intelligence integration and data analysis techniques to enable real-time attack detection and deception. The system leverages efficient programming frameworks, database management and external APIs to en- sure scalable monitoring, intelligent threat classification and effective visualization of cyber threats

1) *Programming Languages*: The implementation of De- coyShield primarily utilizes Python for developing core functionalities such as network monitoring, behavioral analysis and adaptive deception mechanisms, leveraging its strong support for networking and data processing. SQLite is used for efficient data storage and logging, while PyQt is employed for building the graphical dash- board interface. Additionally, standard networking li- braries and API integrations are used to handle real-time communication and threat intelligence enrichment.
2) *Frameworks and Libraries*: The DecoyShield system is developed using Python-based libraries for networking, data processing and GUI development. Core function- alities are implemented using socket programming for real-time connection handling, while external APIs are integrated for threat intelligence and IP analysis. The user interface is built using PyQt, providing an interactive dashboard for monitoring and visualization. Development and testing were carried out using standard Python IDEs, ensuring efficient implementation and system scalability.

3) *Database and Storage*: SQLite is used as the primary database for storing attack logs, including IP details, com- mands, timestamps and threat levels. It enables efficient data retrieval, real-time analysis and seamless integration with the monitoring dashboard for visualization and re- porting.
4) *Development and Monitoring Tools*: The DecoyShield system was developed using Python-based IDEs such as Visual Studio Code for implementing core functionalities, including network monitoring, behavioral analysis and GUI components. Tools like Nmap and Netcat were used to simulate attacks and test system responses. The user interface was designed using PyQt, enabling real- time visualization of threats. The system was tested on Windows and Linux environments to ensure stability, performance and cross-platform compatibility.

V. RESULTS AND DISCUSSION

The implementation of DecoyShield successfully achieved its primary objective of providing proactive threat detection through deception-based techniques and behavioral analysis. The system was evaluated using simulated attack scenarios such as port scanning, service probing and command-based interactions to validate its effectiveness in identifying and engaging potential attackers.

The system demonstrated strong capability in detecting reconnaissance and intrusion attempts in real time. During testing, DecoyShield successfully identified rapid port scan- ning activities (e.g., Nmap scans) and classified them based on intensity and frequency. The behavioral analysis module accurately distinguished between normal and suspicious activ- ity by evaluating connection patterns, scan speed and repeated access attempts.

1) Port Scan Detection: The system detected multiple port scanning attempts and classified them as medium to high threats based on scan rate and number of targeted ports.
2) Deception Effectiveness: Attackers interacting through tools like Netcat were successfully diverted to fake ser- vice banners and sandbox environments, allowing safe observation of commands such as whoami and ls.
3) Threat Classification: The adaptive scoring mechanism effectively categorized threats into low, medium and high levels, enabling appropriate responses.

System Performance and Efficiency: Testing results indicate that DecoyShield runs smoothly with low resource consump- tion. The system was able to manage multiple incoming con- nections simultaneously without noticeable delay, even during continuous scanning activities. Its lightweight design ensures stable operation on standard systems without impacting normal performance.

Logging and Monitoring: DecoyShield effectively records detailed information about each interaction, including attacker IP, targeted ports, executed commands and session duration. The integrated dashboard presents this data in a clear and structured manner, allowing easy tracking of attack patterns and threat levels in real time. Alerting and Response: The system reliably generates alerts when high-risk activity is de- tected, enabling quick response from administrators. Its adap- tive response mechanism ensures that attackers are engaged through deceptive techniques while keeping actual system resources secure.

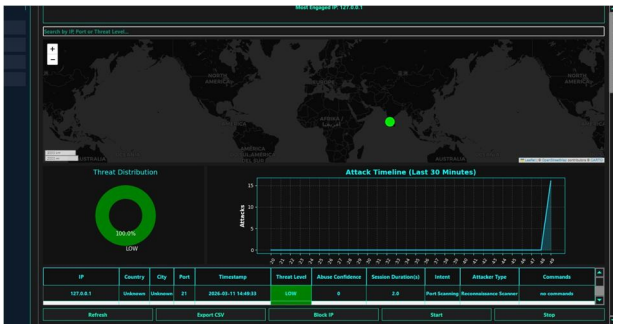


Fig. 4. Critical Threat Alert Notification

Fig. 5. Email Alert for High-Severity Attack

Fig. 6. Attack Details Inspection Window

VI. CONCLUSION AND FUTURE WORK

A. *Conclusion*

The development of DecoyShield demonstrates an effective shift from traditional reactive security methods to a proac- tive and deception-based approach. Instead of only detecting known threats, the system actively engages attackers using simulated environments, allowing real-time monitoring and analysis of their behavior. By combining honeypot techniques, behavioral analysis and adaptive responses, DecoyShield is able to identify suspicious activities, classify threat levels and safely contain potential attacks without affecting real system resources. The integration of logging, alerting and visualiza- tion further improves visibility and helps in understanding attack patterns. Overall, DecoyShield provides a practical and efficient solution for modern cybersecurity challenges by enhancing threat detection, improving situational awareness and enabling better protection of network systems.

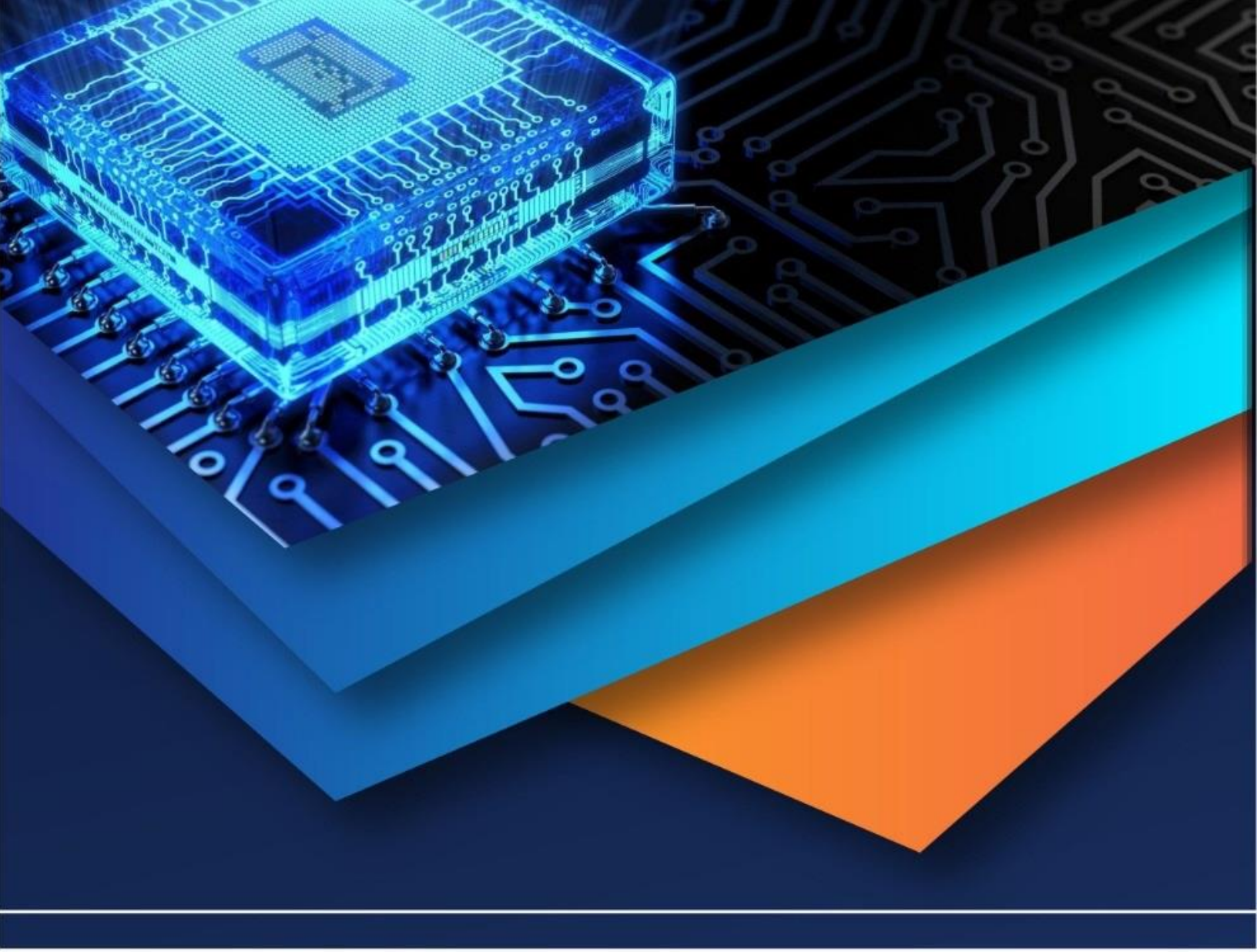
B. *Future Work*

Future enhancements of DecoyShield will focus on im- proving detection accuracy and system scalability. Advanced behavioral analysis techniques and AI-based models can be integrated to better understand attacker patterns and predict potential threats. The system can also be extended with au- tomated response mechanisms, such as dynamic blocking or integration with firewall and SIEM tools for stronger security enforcement. Additionally, deploying DecoyShield in cloud and distributed environments will improve its ability to handle large-scale attacks. Further improvements may include enhanc- ing the dashboard with advanced analytics and visualizations, as well as expanding deception techniques to create more realistic and adaptive environments for attackers.

REFERENCES

[1] K. Salama, N. A. Sedeek, A. Bendary, A. Ashry, and A. D. Elbayoumy, "Multi-tier honeypot for resilient network security," in 2025 15th In- ternational Conference on Electrical Engineering (ICEENG). IEEE, 2025, pp. 1–6.
[2] G. A. J. Saskara, I. K. R. Arthana, and P. B. Megawanta, "Simulation and performance testing of the ganesha honeypot system (ghost) for ssh security," in 2023 1st International Conference on Advanced Engineer- ing and Technologies (ICONNIC). IEEE, 2023, pp. 55–59.
[3] A. H. Anwar, C. A. Kamhoua, N. O. Leslie, and C. Kiekintveld, "Honeypot allocation for cyber deception under uncertainty," IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 3438–3452, 2022.
[4] H. Fan, Q. Tan, R. Tan, and B. Nie, "Honeydecoy: A comprehensive web-based parasitic honeypot system for enhanced cybersecurity," in 2023 IEEE Smart World Congress (SWC). IEEE, 2023, pp. 1–8.
[5] K. I. Iyer, "Adaptive honeypots: Dynamic deception tactics in modern cyber defense," Int. J. Sci. Res. Arch, vol. 4, no. 1, pp. 340–351, 2021.
[6] Z. Moric´, V. Dakic´, and D. Regvart, "Advancing cybersecurity with honeypots and deception strategies. informatics, 12 (1), 14," 2025.
[7] D. S. Morozov, T. A. Vakaliuk, A. A. Yefimenko, T. M. Nikitchuk, and
[8] R. O. Kolomiiets, "Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure." in doors, 2023, pp. 81–96.
[9] A. Ebunoluwa and A. James, "Ai-powered honeypots: Enhancing de- ception technologies for cyber defense," unpublished, 2025.
[10] D. Zielinski and H. A. Kholidy, "An analysis of honeypots and their impact as a cyber deception tactic," arXiv preprint arXiv:2301.00045, 2022.
[11] V. E. Urias, W. M. Stout, J. Luc-Watson, C. Grim, L. Liebrock, and M. Merza, "Technologies to enable cyber deception," in 2017 International Carnahan Conference on Security Technology (ICCST). IEEE, 2017, pp. 1–6.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)