International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Deception-Based Intrusion Prevention Framework for Proactive Network Security Using Behavioral Threat Analysis

Priyanka Shankar Tuppad[1], Vinit Kumar Shukla[2]

[1,2]Assistant Professor, Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, Bengaluru

Abstract

The rapid expansion of networked systems has led to an increase in sophisticated cyber threats that frequently bypass traditional security mechanisms. Conventional defenses largely rely on signature-based or rule-based techniques, which are limited in their ability to detect unknown or advanced attacks. To address these challenges, this paper proposes a Deceptive Intrusion Prevention System (DIPS) that transitions network security from a reactive model to a proactive, intelligence-driven approach. The proposed architecture employs strategically deployed decoy resources and deceptive information to divert attackers away from critical assets while monitoring their behavior within a controlled environment. The framework combines deception, behavioral analysis, and automated mitigation within a unified intrusion prevention architecture. By analyzing attacker interactions with deceptive components, the system accurately identifies malicious activity and enables real-time response actions such as isolation and blocking. Experimental evaluation conducted in a controlled network environment demonstrates that the proposed approach improves detection accuracy, reduces false positives, and enhances overall system resilience. The results further show that deception-based intrusion prevention effectively delays attackers and generates actionable threat intelligence, strengthening proactive network defense.

Keywords: Deception-Based Intrusion Prevention, Cyber Deception, Proactive Network Security, Behavioral Threat Analysis, Honeypot-Based Defense

1. Introduction

The pervasive adoption of digital technologies across sectors such as banking, healthcare, education, industrial control systems, and government infrastructure has made network security a critical priority [1]. Modern organizations increasingly depend on interconnected systems to store, process, and transmit sensitive data [4]. While this interconnectivity enables efficiency and innovation, it also exposes systems to a growing range of cyber threats. Attackers exploit system vulnerabilities to gain unauthorized access, exfiltrate confidential data, disrupt services, or establish persistent footholds within networks [2].

Unlike conventional honeypot-assisted IDS approaches, the proposed DIPS framework integrates cyber deception with behavioral validation and automated intrusion prevention actions.

Traditional network security mechanisms, including firewalls, antivirus software, and intrusion detection systems (IDS), have long served as the first line of defense. These solutions primarily rely on known

attack signatures or predefined rules to detect malicious activity. While signature-based detection is efficient against previously identified threats, it is largely ineffective against zero-day attacks, polymorphic malware, and stealth-based reconnaissance techniques [3]. As attackers increasingly employ adaptive methods to evade detection, conventional defenses struggle to maintain adequate situational awareness. These limitations are extensively documented in established retrospects of cyber defense [6].

Intrusion Prevention Systems (IPS) extend IDS functionality by actively blocking or mitigating detected attacks in real time. Despite this enhancement, IPS solutions remain constrained by high false positive rates and limited behavioral context. Excessive false alerts often overwhelm security teams, leading to alert fatigue and reduced operational effectiveness [5]. Moreover, traditional IPS approaches remain fundamentally reactive, responding only after suspicious activity is detected rather than preventing attackers from progressing through the attack lifecycle. Research into networks of decoy elements has specifically highlighted these visibility gaps [6].

To overcome these challenges, cyber security research has increasingly focused on proactive defense mechanisms capable of anticipating and disrupting adversarial actions before significant damage occurs. One such approach is cyber deception, which deliberately introduces misleading information, decoy systems, and false targets into the network to confuse, delay, and observe attackers [1]. Instead of blocking adversaries immediately, deception-based systems aim to engage them in controlled environments, forcing attackers to reveal tactics, techniques, and procedures (TTPs). This strategy is supported by foundational work in tracking hackers and hybrid frameworks for proactive networks [8].

Recent studies have demonstrated that deception can significantly enhance detection accuracy and threat intelligence generation when integrated with monitoring and analysis components [3]. Systematic surveys indicate that honeypot performance and detection engines are improved through these integrated techniques [6, 7]. However, most existing deception deployments function as auxiliary tools, such as standalone honeypots, rather than being embedded directly within intrusion prevention workflows. This creates a gap between detection and response capabilities [4, 5].

This paper addresses this gap by proposing a Deception-Based Intrusion Prevention System (DIPS) that unifies monitoring, deception, behavioral analysis, and response within a single architecture. By treating interaction with deceptive assets as strong evidence of malicious intent, the proposed framework reduces false positives and enables timely prevention actions. The contributions of this work are threefold:

- **Integrated Architecture:** A layered architecture for integrating deception directly into intrusion prevention systems.
- **Behavior-Driven Decision Model:** A logic-based decision model that utilizes interaction logs to improve detection accuracy and minimize false positives.
- **Empirical Validation:** An experimental evaluation demonstrating the effectiveness of deception-based intrusion prevention in a controlled network environment.

2. Related Work

Current research on cyber deception can be broadly categorized into three categories: modern adaptive deception frameworks, honeypot-assisted detection systems, and foundational deception principles. Table I lists the important literature and its main contributions to give a succinct summary of these research directions and draw attention to the gaps that are currently being filled by this effort.

Table 1: Prior Work on Deception Based Intrusion Defense

Ref.	Focus Area	Key Contribution	Limitation Addressed by DIPS
[1, 2]	Foundational cyber deception	Introduced honeypots and attacker behavior analysis	Lacked automated prevention and integration
[3, 4]	Surveys & challenges	Identified limitations of traditional IDS and deception gaps	No unified prevention framework
[5]	Decoy network analysis	Studied attacker movement within decoy infrastructures	No real-time mitigation
[6, 7]	Honeypot–IDS integration	Improved detection accuracy using honeypots	High false positives, reactive response
[8, 9, 10]	Modern deception frameworks	Decision-making, AI-driven and experimental deception systems	Limited IPS-level enforcement
[11]	Proactive IoT defense	Combined MTD with cyber deception	Not focused on false-positive reduction
[12, 13, 14, 15]	AI / ML-based security	Behavioral analysis and adaptive detection	Deception not tightly coupled with IPS
[16]	Evaluation Data & Implementation	High-fidelity labeled traffic and open-source framework	Realistic, data experimental modern IPS benchmarks

For many years, researchers have examined cyber deception as a defensive tactic to comprehend the actions of attackers. Advanced attackers and new exploit techniques are often missed by traditional defensive measures like firewalls and signature-based intrusion detection or prevention systems (IDS/IPS). As a result, scientists have investigated combining decoy systems, honeypots, and honeytokens.

2.1 Foundations and Evolution of Honeypots

Early foundational work introduced honeypots as deliberately vulnerable or attractive systems designed to lure attackers away from production assets.

- **Research and Analysis:** These systems allowed security analysts to observe attacker behavior and collect forensic data.
- **Informing Defense:** While primarily used for research, honeypots provided foundational knowledge about attacker behavior patterns and informed numerous defense strategies.
- **Distributed Infrastructures:** Subsequent research extended these into honeynets and distributed deception infrastructures capable of capturing large-scale attack data [3, 5].
- **Enhanced Visibility:** Surveys indicate that these systems improve visibility into attacker strategies and support robust forensic analysis.
- **Operational Limitations:** Despite these benefits, early deployments typically operated independently of prevention mechanisms, which limited their overall defensive impact.

2.2 Integration with Intrusion Detection Systems

More recent studies have explored the integration of deception with intrusion detection systems to address the high false positive rates of traditional frameworks.

- **Accuracy Improvements:** Honeypot-assisted IDS frameworks demonstrated improvements in anomaly detection accuracy and reductions in false positives by correlating alerts with honeypot interactions [6, 7].
- **Adaptive Realism:** Adaptive deception frameworks further enhanced realism by dynamically modifying decoy configurations in response to attacker behavior [8, 13].
- **Evasion Difficulty:** This dynamic behavior increases the difficulty for attackers to detect and evade decoy systems.

2.3 AI-Driven Deception and Domain Solutions

Advancements in artificial intelligence (AI) and machine learning (ML) have significantly influenced deception research.

- **Behavioral Classification:** AI-driven deception systems leverage data collected from deceptive environments to classify attacks and automate responses [12, 14].
- **Pattern Recognition:** These approaches show promise in identifying unknown threats and improving pattern recognition.
- **Domain Applications:** Deception methodologies are increasingly applied in specific contexts, such as industrial control systems (ICS) and cloud-containerized environments [7, 11].

Emerging research in 2025 has focused on high-interaction and automated deception mechanisms in the face of evolving threats. For example, the VelLMes framework utilizes high interaction and AI-based deception techniques to generate a high-fidelity environment [9]. On the other hand, the Perry framework tries to provide cyber deception through a quick process of deploying and testing new decoy tactics [10]. Current research also focuses on the need for intelligent intrusion detection methods to secure environments constrained in resources, such as IoT and cyber physical networks, using state-of-the-art machine learning algorithms. Though these papers concentrate on realism and experimentation in deception, the contribution of the DIPS framework is in integrating both into the automation process.

2.4 Comparative Analysis of Approaches

Recent large-scale surveys emphasize the need for unified frameworks that combine deception, behavioral analysis, and automated response. Table II illustrates the shift toward the proposed Deceptive Intrusion Prevention System (DIPS).

Table 2: Comparative Analysis of Existing Approaches

Approach	Deception	Prevention	Behavioral Analysis	False Positive Reduction
Traditional IDS	No	No	Low	Low
Honeypot-Based IDS	Yes	No	Medium	Medium
AI-Based IDS	No	Yes	Medium	Medium
Proposed DIPS	Yes	Yes	High	High

Even though the present-day deception technologies increase the amount of information that is being gained about attackers' activities, most of these systems are independent tools that do not directly integrate into the prevention process of attacks. Additionally, there are various limitations related to their effectiveness as many solutions have problems with high false positives, insufficient behavioral checking, and a lack of automatic actions on the side of prevention.

3. Methodology

The design of the Deceptive Intrusion Prevention System (DIPS) focuses on shifting traditional network defense from a purely reactive model to a proactive and intelligence-driven strategy. Unlike conventional systems that rely on static rules, this architecture integrates deception to actively engage and mislead attackers [8, 10].

3.1 System Architecture

The proposed DIPS framework is organized into five tightly integrated functional layers that manage the lifecycle of an intrusion attempt from initial observation to automated mitigation as depicted in Figure 1. The DIPS architecture consists of five tightly integrated layers [9]:

- Monitoring Layer
- Deception Layer
- Interaction Logging Layer
- Analysis and Decision Layer
- Prevention and Response Layer

Figure 1: Deception Strategies in Modern Cybersecurity

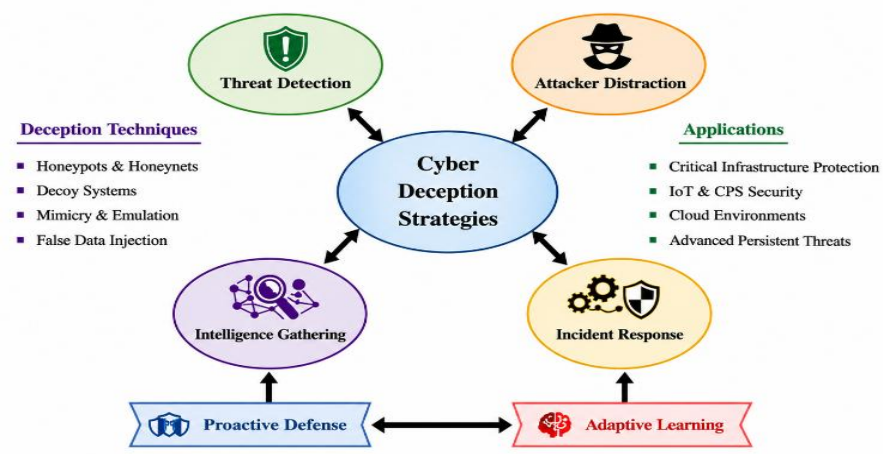


Figure 1 illustrates the integration of deception techniques with threat detection, attacker distraction, intelligence gathering, and incident response to support proactive and adaptive network defense.

3.2 Monitoring Layer

The monitoring layer collects raw data such as packet headers, access logs, and protocol usage patterns while operating with minimal intrusion into normal network operations [16]. Unlike traditional systems that prioritize signature matching, this layer identifies suspicious behavior patterns [5, 6]:

- **Abnormal Access Attempts:** Captures unauthorized or unexpected requests for network services.
- **Reconnaissance Detection:** Identifies unusual port scanning activities and unauthorized service requests.
- **Feeder Mechanism:** Acts as a trigger for the deception layer by identifying potential attacker behavior that requires redirection.

3.3 Deception Layer

The deception layer utilizes assets strategically placed within the network to appear legitimate and attractive to adversaries.

- **High-Fidelity Decoys:** Systems are configured to mimic real production environments, including operating systems and network services, to ensure realism.
- **Dynamic Adaptation:** The layer adjusts its configuration in real-time to closely resemble the current real network environment, making decoys harder to fingerprint [9].
- **Intent Verification:** Since legitimate users have no operational reason to interact with these decoys, any access attempt is treated as highly indicative of malicious intent.

The use of dynamic adaptation in the DIPS architecture helps change the configuration of decoys in real-time to match closely with the configuration in the actual production environment, which makes fingerprinting deceptive assets more difficult [14].

3.4 Behavioral Analysis Model

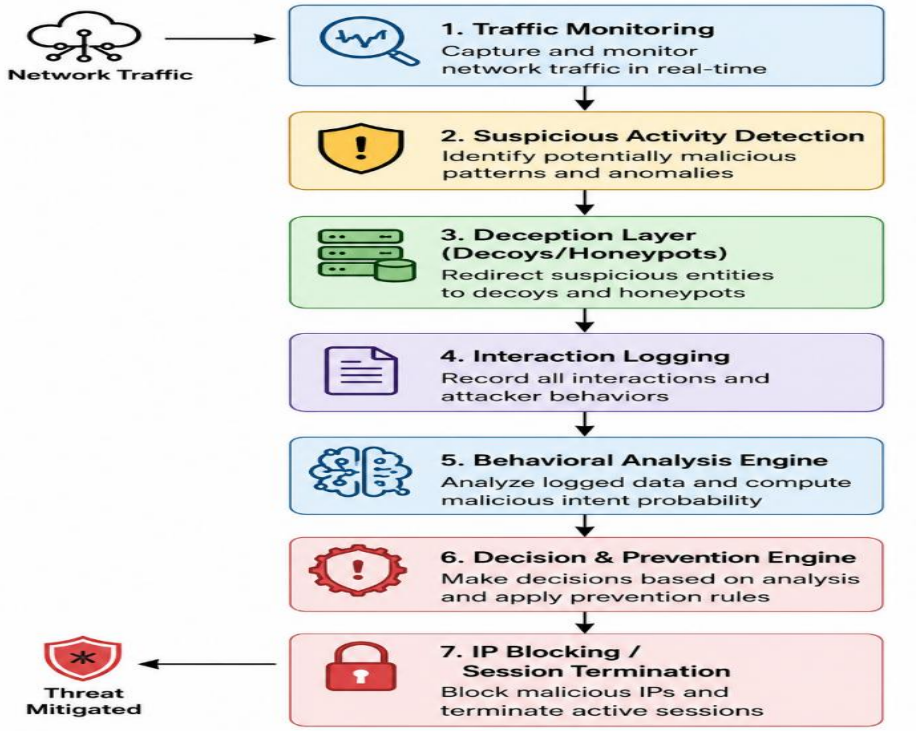
To reduce false positives and improve decision-making accuracy, the system tracks attacker behaviour over time rather than relying on isolated events [8, 12].

- Let L denote legitimate user behavior, D denote interaction with deception assets, and $B(t)$ represent a sequence of observed actions over time.
- **Probabilistic Inference:** Malicious intent is inferred with a high degree of confidence when [8, 13]
  $P(attack\ |D, B(t)\ \gg P(Attack\ |L)$ (1)
  Which is inferred from: P(Malicious | D, A) > θ
  Where θ represents the malicious intent threshold
- **Decision Accuracy:** By treating interaction with deceptive resources as strong evidence, the decision layer can confidently classify malicious activities with higher accuracy than traditional anomaly detection.

3.5 Algorithm – Deception-Based Intrusion Prevention

The operational workflow ensures that suspicious traffic is subtly redirected without alerting the attacker as shown in below Figure 2 [5, 10]

Figure 2: Operational Workflow and Mitigation Lifecycle of the DIPS Framework



Algorithm 1: Deceptive Intrusion Prevention System (DIPS) Workflow

Input: Raw Network Traffic (T)
Output: Prevention Action (A)
Step 1. Monitor incoming network traffic
Step 2. Detect suspicious behavioral patterns
Step 3. Redirect suspicious entities to deception layer
Step 4. Log attacker interactions
Step 5. Analyze attacker behavior
Step 6. Compute malicious intent probability P(Malicious | D, A)
Step 7. If $P(\text{Malicious}|D, A) > \theta$
Step 8. Block attacker IP
Step 9. Terminate Session
Step 10. Store threat intelligence
Step 11. else
Step 12. Continue monitoring
Step 13. end if
Step 14. Return prevention action A

The overall DIPS methodology combines monitoring, deception, and automated response within a five-layer architecture to transition network defense toward a proactive, intelligence-driven model. As illustrated in Figure 2 suspicious entities are tactically redirected to high-fidelity decoys where their interactions are logged and analyzed. This entire working procedure is codified through the Algorithm 1, which utilizes a probabilistic decision model to validate malicious intent and execute real-time mitigation—such as IP blocking and session termination— so, this helps keep threats away from critical assets while collecting useful threat intelligence [15].

4. Results and Experimental Evaluation

The evaluation of the Deceptive Intrusion Prevention System (DIPS) focused on quantifying its effectiveness in enhancing detection accuracy, reducing false alerts, and improving response latency compared to traditional security architectures.

4.1 Experimental Setup

The performance of the system was analyzed within a controlled network environment designed to replicate a real-world enterprise infrastructure [6]. The simulation was implemented using Mininet for network topology management, while high-interaction Cowrie and Dionaea honeypots were deployed as the core assets within the deception layer [7]. Attack simulations were executed using Kali Linux tools (Nmap, Metasploit) and custom Python scripts to generate realistic reconnaissance and brute-force traffic [16].

Network Components: The environment integrated legitimate user traffic, common network services, and strategically deployed deceptive assets, including decoy servers and honeyfiles.

Attack Scenarios: Various attack patterns were simulated to assess the system's resilience, covering the full attack lifecycle:

Reconnaissance: Stealthy port scanning and service enumeration.

Unauthorized Access: Credential brute-forcing and data probing attempts.

Lateral Movement: Attempts to transition between decoy and production nodes.
Workload Conditions: Legitimate user behavior was introduced concurrently to verify that the DIPS could distinguish malicious intent under normal operational conditions without disrupting genuine activities.

4.2 Quantitative Results

The experimental outcomes demonstrate in table III that the integration of deception techniques provides a significant performance advantage over conventional signature-based systems.

Table 3: Comparison of Performance Metrics

Metric	Traditional IPS	Proposed DIPS
Detection Accuracy	78%	92%
False Positive Rate	15%	5%
Average Response Time	420 ms	260 ms
Attacker Engagement Time	Low	High

4.2.1 Detection Accuracy and Reliability

One of the most significant results was the improvement in the system's ability to identify threats that bypassed conventional rule-based detection.

- **Early Detection:** Malicious activities were identified at an early stage because interactions with deceptive resources served as high-confidence indicators of intent [6, 8].
- **Resilience to Stealth:** Attacks utilizing unknown exploit techniques or stealthy scanning were successfully captured once the adversary engaged with the decoys.

4.2.2 False Positive Mitigation

The DIPS achieved a substantial reduction in false alarms, addressing the common challenge of alert fatigue in security operations [6, 12].

- **Workflow Isolation:** Since deceptive components were not part of any legitimate workflow, legitimate users rarely interacted with them.
- **Precise Classification:** Benign anomalies in the production network were correctly identified as non-malicious, allowing security teams to focus exclusively on genuine threats.

4.2.3 Response Effectiveness and Engagement

The system demonstrated efficient real-time mitigation while maximizing the collection of threat intelligence.

- **Timely Mitigation:** Once malicious intent was confirmed, prevention actions—such as IP blocking and session termination—were executed without significant performance delays.
- **Behavioral Visibility:** By allowing attackers to remain within the deception environment for extended periods, the system captured detailed behavioral sequences and exploited vulnerabilities [9, 14].
- **Minimal Performance Impact:** Monitoring and analysis processes handled high traffic volumes without introducing noticeable latency or affecting legitimate user activities.

4.2.4 Performance Comparison Analysis

Figure 3 illustrates a comparative performance analysis between the traditional Intrusion Prevention System (IPS) and the proposed Deceptive Intrusion Prevention System (DIPS) across key evaluation metrics, namely detection accuracy, false positive rate, average response time, and attacker engagement

time. As shown in Figure 3, the proposed DIPS achieves a significantly higher detection accuracy (92%) compared to the traditional IPS (78%), confirming the effectiveness of deception-driven indicators in identifying malicious intent.

Figure 3: Performance Comparison: Traditional IPS vs. Deception-Based IPS

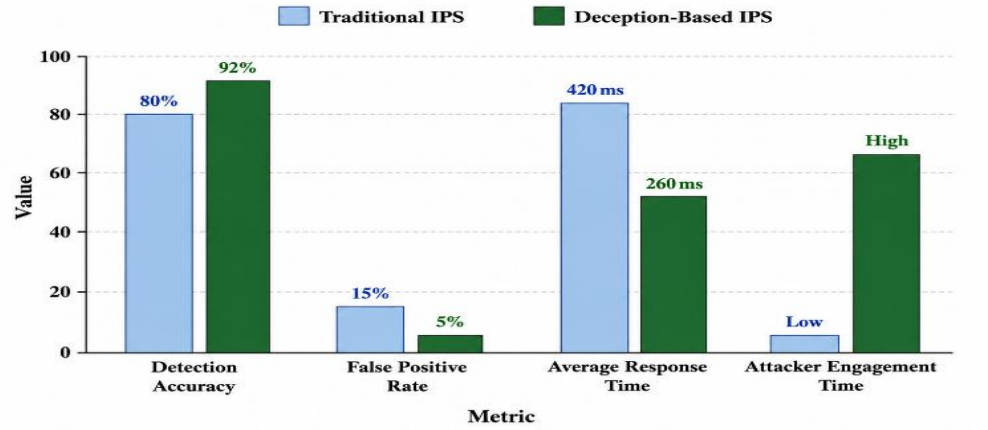


Figure 3 Performance comparison between traditional IPS and the proposed Deceptive Intrusion Prevention System (DIPS) in terms of detection accuracy, false positive rate, response time, and attacker engagement.

The false positive rate is reduced from 15% to 5%, demonstrating improved reliability and reduced alert fatigue. Additionally, the average response time is improved from 420 ms to 260 ms, indicating faster mitigation once malicious behavior is confirmed [7]. Most notably, attacker engagement time is substantially higher in DIPS, highlighting the system's capability to retain attackers within the deception environment for extended behavioral analysis without impacting production assets. These results validate that integrating deception techniques into intrusion prevention enhances both security effectiveness and operational efficiency [11].

5. Discussion

The experimental evaluation confirms that the Deceptive Intrusion Prevention System (DIPS) significantly enhances network security by shifting the defensive paradigm from reactive alerting to proactive engagement. Unlike traditional systems that rely on static signatures or rigid rules, DIPS utilizes interaction with deceptive assets to provide high-confidence indicators of malicious behavior.

5.1 Strategic Advantages of Cyber Deception

The results demonstrate several key advantages of integrating deception into the intrusion prevention workflow:

- High-Confidence Detection: Because deceptive resources are not part of legitimate user workflows, any interaction with them serves as a reliable indicator of malicious intent.
- Resilience Against Advanced Threats: The system successfully identifies stealthy attacks and unknown exploit techniques that typically bypass conventional rule-based detection mechanisms [13, 14].
- Reduction of Alert Fatigue: By achieving a substantial reduction in false positive alerts, DIPS enables security teams to focus their attention on genuine threats rather than being overwhelmed by benign anomalies [3, 6].

- Enhanced Threat Intelligence: The controlled environment allows for the collection of detailed behavioral sequences, providing insights into attacker strategies, tools, and objectives [5, 8].

5.2 Operational Impact and Efficiency

While the deployment and maintenance of decoy systems introduce some architectural overhead, the evaluation shows that the benefits in accuracy and situational awareness justify these costs.

- **System Stability:** The implementation of lightweight, virtualized decoys ensures that the deception layer operates with minimal impact on network performance.
- **Real-Time Mitigation:** The system maintains the ability to execute prevention actions such as blocking IP addresses or terminating sessions in a timely manner once malicious intent is confirmed.
- **Actionable Data:** The intelligence generated regarding attack vectors and exploited vulnerabilities can be used to proactively strengthen existing security policies and incident response planning.

The transition to an intelligence-driven strategy allows for the isolation of attackers from real assets while simultaneously maximizing the intelligence gathered from ongoing attempts. This approach effectively addresses the key limitations of traditional IPS solutions by providing a proactive layer of defense against sophisticated, evolving threats [7, 11].

6. Conclusion and Future Work

This research presents a comprehensive Deception-Based Intrusion Prevention Framework (DIPS) designed to address the critical limitations of traditional, reactive security architectures by integrating cyber deception directly into the intrusion prevention workflow. By leveraging strategically deployed decoy resources and behavioral analysis, the system successfully shifts the defensive paradigm from a passive, signature-dependent model to an active, intelligence-driven strategy. Experimental results confirm that DIPS provides a scalable and practical solution, achieving a detection accuracy of 92% while reducing false positive alerts to 5%. The controlled environment facilitated the collection of detailed behavioral sequences, allowing for the analysis of attacker tactics, techniques, and procedures (TTPs) without risking real production assets.

In future work, efforts will be made to incorporate machine learning techniques to design intelligent learning models that can detect and predict emerging attacks in real time. Future work will focus to automate orchestration that will enable dynamic manipulation of high-fidelity decoy resources inspired by high interaction AI-based platforms such as VelLMes to counter adversarial fingerprinting. Furthermore, there will be plans to expand the scope of the proposed solution in large cloud and IoT environments.

References

1. L. Spitzner, Honeypots: Tracking Hackers. Boston, MA, USA: Addison-Wesley, 2003.
2. Honeynet Project, Know Your Enemy: Learning About Security Threats. Boston, MA, USA: Addison-Wesley, 2004.
3. V. Shirsath, “A survey on current states of honeypots and deception techniques for attack capture,” Int. J. Eng. Res. Technol. (IJERT), vol. 9, no. 3, pp. 1–6, Feb. 2021, doi: 10.17577/IJERTCONV9IS03092.
4. D. Liebowitz et al., “Deception for cyber defence: Challenges and opportunities,” in Proc. IEEE 3rd Int. Conf. Trust, Privacy Security Intell. Syst. Appl. (TPS-ISA), Atlanta, GA, USA, 2021, pp. 173–182, doi: 10.1109/TPSISA52974.2021.00020.

5. D. Reti, D. Fraunholz, J. Zemitis, D. Schneider, and H. D. Schotten, “Deep down the rabbit hole: On references in networks of decoy elements,” in Proc. Int. Conf. Cyber Security Protection Digital Services, Dublin, Ireland, 2020, pp. 1–11, doi: 10.1109/CyberSecurity49315.2020.9138850.
6. M. Baykara and R. Das, “A novel honeypot based security approach for real-time intrusion detection and prevention systems,” J. Inf. Secur. Appl., vol. 41, pp. 103–116, Aug. 2018, doi: 10.1016/j.jisa.2018.06.004.
7. Parineeta and C. S. Dash, “Enhancing cloud server resilience: Honeypots and intrusion detection systems in browser hijacking defense,” in Proc. 2nd Int. Conf. Intell. Cyber Phys. Syst. Internet Things (ICoICI), Coimbatore, India, 2024, pp. 217–222, doi: 10.1109/ICoICI62503.2024.10696630.
8. A. Kashtalian, Ł. Ścisło, R. Rucki, S. Lysenko, A. Sachenko, B. Savenko, O. Savenko, and A. Nicheporuk, “Control and decision-making in deceptive multi-computer systems based on previous experience for cybersecurity of critical infrastructure,” Applied Sciences, vol. 15, no. 22, Art. no. 12286,2025, doi: 10.3390/app152212286.
9. M. Sladić, V. Valeros, C. Catania, and S. Garcia, “VelLMes: A high-interaction AI-based deception framework,” in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Venice, Italy, 2025, pp. 671–679, doi: 10.1109/EuroSPW67616.2025.00082.
10. B. Singer, Y. Saquib, L. Bauer, and V. Sekar, “Perry: A high-level framework for accelerating cyber deception experimentation,” in Proc. 28th Int. Symp. Res. Attacks, Intrusions Defenses (RAID), Gold Coast, Australia, 2025, pp. 158–173, doi: 10.1109/RAID67961.2025.00049.
11. M. Ge, J.-H. Cho, D. Kim, G. Dixit, and I.-R. Chen, “Proactive defense for Internet-of-things: Moving target defense with cyberdeception,” ACM Trans. Internet Technol., vol. 22, no. 1, Art. no. 24, pp. 1–31, Sep. 2021, doi: 10.1145/3467021.
12. M. M. Althobaiti, “Intelligent intrusion detection for IoT and cyber-physical systems using machine learning,” Int. J. Adv. Appl. Sci., vol. 12, no. 6, pp. 92–105, 2025, doi: 10.21833/ijaas.2025.06.009.
13. B. A. Al-Zahrani, “Adaptive deception framework with behavioral analysis for enhanced cybersecurity defense,” arXiv preprint arXiv:2510.02424, Oct. 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2510.02424.
14. C. Guan, J. Zhang, G. Cao, T. F. La Porta, and J. C. Acosta, “Learning-based Internet of Things honeypots for cyber deception,” IEEE Security & Privacy, vol. 23, no. 6, pp. 58–65, Nov.–Dec. 2025,
doi: 10.1109/MSEC.2025.3601986.
15. V. S. S. R. Nallapareddy and S. K. R. Katta, “AI-enhanced cyber security proactive threat detection and response systems,” in Proc. 4th Int. Conf. Sentiment Anal. Deep Learn. (ICSADL), Bhimdatta, Nepal, 2025, pp. 1510–1514, doi: 10.1109/ICSADL65848.2025.10933436.
16. Canadian Institute for Cybersecurity, "Intrusion Detection Evaluation Dataset (CICIDS2017)," University of New Brunswick (UNB), 2017. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html.