AI-driven adaptive deception and threat intelligence

Dr.M.Sangeetha
Head of the Department / Computer Science and Engineering
V.S.B.Engineering College
Karur, Tamilnadu

Thikash J
III Computer Science and Engineering (Artificial Intelligence and Machine Learning)
V.S.B.Engineering College
Karur, Tamilnadu

Suganth S S
III Computer Science and Engineering (Artificial Intelligence and Machine Learning)
V.S.B.Engineering College
Karur, Tamilnadu

ABSTRACT

The increasing sophistication of cyberattacks and the rapid evolution of attacker tactics have exposed the limitations of traditional reactive cybersecurity measures. Conventional defense models that rely on detection, analysis, and response often fail to anticipate zero-day exploits or stealthy intrusions. To address these challenges, this research introduces an AI-driven adaptive deception and threat intelligence framework. This proactive cybersecurity paradigm integrates artificial intelligence (AI), machine learning (ML), and deception technologies to create intelligent, self-evolving defense ecosystems. The proposed model dynamically misleads adversaries, learns from their behavior, and continuously strengthens the network's resilience through automated intelligence feedback loops.

The core of this approach lies in the synergy between AI-based behavioral analytics and deception technologies such as honeypots, honey tokens, and decoy assets. These deceptive elements simulate realistic digital environments to lure attackers into controlled traps, enabling detailed observation of their techniques, tactics, and procedures (TTPs). Machine learning models analyze the attackers' interactions with decoys to identify intent, methodology, and exploit patterns. The system then adapts its deception strategies in real-time, ensuring that the defense mechanism remains unpredictable and dynamic. Through adaptive learning, the system reduces false positives, enhances detection accuracy, and minimizes human intervention in incident response.

Another critical component of this framework is the integration of real-time threat intelligence. By aggregating data from global sources such as dark web forums, malware repositories, and intrusion detection systems, the model continuously updates its threat database. This enriched intelligence allows AI algorithms to simulate potential attack scenarios, predict adversarial behavior, and preemptively modify network defenses. In doing so, the system not only detects intrusions early but also evolves to resist future attacks through iterative learning and intelligence feedback.

The proposed AI-driven adaptive deception system offers multiple advantages over conventional cybersecurity techniques. It provides proactive defense by engaging attackers before they reach real assets, reduces false positives by focusing on confirmed malicious interactions, and accelerates incident response through autonomous adaptation. Furthermore, it aids in threat attribution, helping analysts trace attacker origins, motives, and affiliations. Applications span enterprise networks, IoT ecosystems, cloud infrastructures, and critical industrial systems (ICS/SCADA), where real-time deception can prevent large-scale disruptions and data breaches.

Despite its promising potential, the framework faces challenges related to AI bias, scalability, and ethical considerations concerning data privacy and the legality of monitoring attacker activity. However, ongoing advancements in generative AI, federated learning, and collaborative threat intelligence sharing are expected to mitigate these limitations. The future trajectory of this research envisions autonomous cyber defense ecosystems capable of generating synthetic decoys, performing self-assessment through simulated attacks, and sharing intelligence securely across global networks. Ultimately, AI-driven adaptive deception represents a paradigm shift toward intelligent, anticipatory cybersecurity — transforming passive defense into an active, learning-oriented shield against the ever-changing landscape of cyber threats.

Incident response through autonomous adaptation. Furthermore, it aids in threat attribution, helping analysts

trace attacker origins, motives, and affiliations. Applications span enterprise networks, IoT ecosystems, cloud infrastructures, and critical industrial systems (ICS/SCADA), where real-time deception can prevent large-scale disruptions and data breaches.

Despite its promising potential, the framework faces challenges related to AI bias, scalability, and ethical considerations concerning data privacy and the legality of monitoring attacker activity. However, ongoing advancements in generative AI, federated learning, and collaborative threat intelligence sharing are expected to mitigate these limitations. The future trajectory of this research envisions autonomous cyber defense ecosystems capable of generating synthetic decoys, performing self-assessment through simulated attacks, and sharing intelligence securely across global networks. Ultimately, AI-driven adaptive deception represents a paradigm shift toward intelligent, anticipatory cybersecurity — transforming passive defense into an active, learning-oriented shield against the ever-changing landscape of cyber threats.

II. KEYWORD

Artificial Intelligence (AI), Cybersecurity, Deception Technology, Threat Intelligence, Machine Learning (ML), Adaptive Defense, Honeypots, Anomaly Detection, Proactive Security, Autonomous Threat Hunting, Generative AI, Intrusion Detection, Behavioral Analytics, Network Security.

III. INTRODUCTION

Cybersecurity has entered a new era where traditional defense mechanisms are no longer sufficient to counter modern cyber threats. Conventional security approaches largely depend on detecting and responding to attacks after they occur, leaving organizations vulnerable to sophisticated, fast-evolving intrusion techniques. As attackers increasingly use automation, artificial intelligence (AI), and stealthy tactics, there is a growing need for a more proactive and adaptive form of defense. This has led to the emergence of AI-driven adaptive deception and threat intelligence, a concept that blends the predictive capabilities of AI with the strategic misdirection of deception technology.

Adaptive deception creates a dynamic and interactive defense environment where attackers are intentionally misled through decoys, honeypots, and fabricated digital assets that closely resemble real systems. Instead of relying solely on intrusion detection, this approach engages adversaries within a controlled environment, allowing defenders to observe attack behavior, capture intent, and learn from the encounter. When powered by AI and machine learning, these deceptive layers become self-adjusting — continuously analyzing attacker actions and adapting their structure and content in real time. This adaptability makes it increasingly difficult for attackers to distinguish genuine systems from traps.

A critical component of this framework is threat intelligence integration, which enhances situational awareness by collecting and analyzing data from diverse sources such as malware databases, dark web forums, and network traffic patterns. By combining this intelligence with AI-based analytics, the system can anticipate new attack strategies and evolve deception mechanisms accordingly. This creates a feedback-driven security model that learns from every attempted intrusion, transforming threat data into actionable defensive insights.

The fusion of AI, deception technology, and threat intelligence marks a shift from reactive protection to intelligent, anticipatory defense. It not only helps in early detection and attacker attribution but also reduces false positives and improves incident response efficiency. However, challenges such as scalability, data bias, ethical boundaries, and seamless integration with existing security infrastructures must still be addressed for broader adoption.

This paper explores the underlying concepts, architecture, and functioning of AI-driven adaptive deception and threat intelligence. It highlights the benefits, practical applications, and ongoing challenges, emphasizing how this emerging paradigm can redefine cybersecurity by creating systems that think, adapt, and defend autonomously.

IV. LITERATURE SURVEY

A. Traditional Deception and Evolution to Adaptive Techniques

Deception has a long history in cybersecurity through honeypots, honeynets, and honeytokens, which lure attackers into controlled environments for analysis. However, static deception systems frequently become obsolete—attackers may recognize patterns or bypass decoys altogether. Iyer’s work on Adaptive Honeypots: Dynamic Deception Tactics explores how deception systems can continuously change configuration and responses over time to maintain plausibility and resist detection.

More recently, Adaptive Deception for Cyber-Physical Systems emphasizes that systems controlling physical

devices (e.g., industrial control systems, SCADA) must carefully integrate deception without jeopardizing safety. The authors propose combining sensor-level decoys, virtual honeynets, moving-target defenses, and feedback loops to slow attacker progress and improve detection certainty.

A complementary contribution, AI-Driven Adaptive Honeypots for Dynamic Cyber Threats (2024), introduces a system that uses AI to modify honeypot behavior in real time, anchored by threat intelligence feeds. Their experiments show that adaptive honeypots outperform static ones in capturing evolving attacker tactics.

B. Generative AI and Prompt-Based Deception

One of the most promising recent directions is the use of Generative AI and prompt engineering to build deception artifacts on the fly. The SPADE framework (2025) presents a novel approach that uses large language models (LLMs) to generate adaptive deception ploys (e.g., fake files, honeypot responses) in response to observed threat behavior. The authors report high engagement (93 %) and accuracy (96 %) when using ChatGPT-4o, with minimal manual tuning.

In a related development, LLMHoney (2025) is an SSH honeypot that uses LLMs to dynamically produce realistic command outputs. The system balances performance (latency) with deception fidelity and finds that moderate-size models like Gemini or Qwen perform best in practice.

Also relevant is the concept of LLM-based honeypots, where the generative model acts as the interaction engine, creating decoy responses, honey files, or system logs on demand, enhancing the realism and adaptability of deception systems. These systems confront challenges like response consistency, latency, and hallucination control.

C. Behavioral & Cognitive Deception

Beyond technical mimicry, recent work aims to engage with attacker cognition and behavior. Cognitive Honeypots (CogniTrap) (2025) merges reinforcement learning with deception to tailor decoys based on attacker reasoning patterns. In a 30-day deployment, CogniTrap increased attacker dwell time by ~45 % over standard high-interaction honeypots and yielded better threat hunting output.

Another recent system, CADL (Cognitive-Adaptive Deception Layer) (2025), applies ensemble machine learning and behavioral profiling to adjust deception strategies dynamically. In tests over the CICIDS2017 dataset, CADL achieved a detection rate of 99.88 % with a false positive rate of 0.13 %, outperforming baseline IDS systems.

D. Integration with Threat Intelligence

While deception provides interaction data, its true power emerges when fused with threat intelligence. AI-driven threat intelligence for real-time cybersecurity (2024) reviews frameworks that use machine learning to ingest and analyze diverse threat feeds (malware signatures, dark web info, traffic anomalies) and feed insights into adaptive defenses.

The broader survey Cybersecurity in the Age of Generative AI (2025) argues that generative models will reshape both offense and defense. It recommends integrating AI-driven threat intelligence directly into operation pipelines, including deception orchestration, to close the loop in real time.

E. Gaps, Challenges, and Research Directions

Although AI-driven adaptive deception and threat intelligence have shown remarkable potential, several challenges still hinder their large-scale adoption. A major concern is model robustness, as AI and large language models (LLMs) can produce unrealistic or inconsistent outputs that reveal the deception to attackers. Real-time adaptive systems also face issues of latency, scalability, and computational cost, especially when operating across distributed cloud or IoT environments that require continuous updates. Maintaining contextual consistency and state management across multiple attacker interactions remains another unresolved problem. Ethical and legal questions further complicate deployment—monitoring adversarial behavior may involve collecting sensitive or jurisdiction-dependent data, raising privacy and compliance concerns. From an operational standpoint, integrating adaptive deception frameworks with legacy security infrastructure such as SIEM, SOAR, and IDS platforms remains technically complex, often requiring custom middleware or APIs. Finally, the lack of explainability and transparency in AI decision-making makes it difficult for analysts to understand why specific deceptive actions were taken or altered. Addressing these issues calls for the development of lightweight hybrid models that combine predictive analytics with generative reasoning, explainable deception logic, and federated collaboration frameworks that allow organizations to securely share deception and threat intelligence data. Continued research in these directions will be essential

to realize fully autonomous, ethical, and resilient adaptive deception systems.

V. EXISTING METHODS

A. Overview of the Existing System

The present cybersecurity infrastructure primarily relies on traditional mechanisms such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and signature-based malware scanners. These tools are designed to detect and mitigate known threats by matching network traffic or user activity against predefined signatures stored in extensive threat databases. Once a suspicious pattern is detected, the system generates an alert for further investigation. This process forms a reactive security model—detecting, analyzing, and responding to threats after an incident occurs. In addition, deception-based tools such as honeypots and honey tokens have been introduced to attract attackers and collect valuable insights into their behavior. These techniques provide useful forensic data but still depend heavily on static configurations and human supervision.

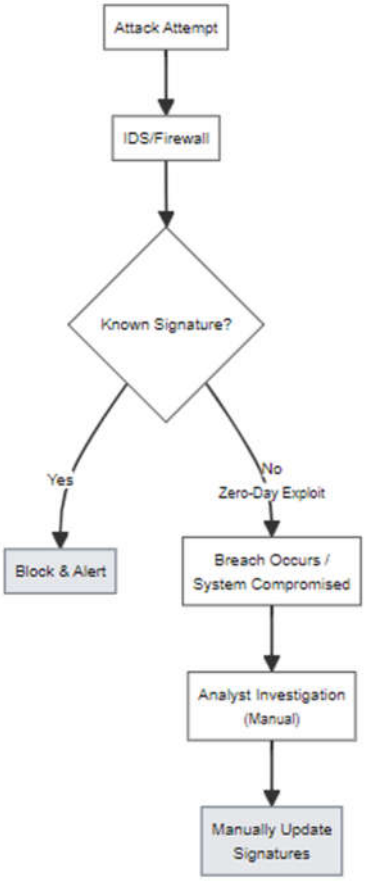
B. Working Mechanism of the Existing System

In conventional defense models, the detection process begins with continuous monitoring of incoming data packets and system logs. Security tools compare these data streams with existing threat indicators to identify malicious signatures or unusual activities. When a potential intrusion is detected, the system either blocks the traffic or alerts security analysts for manual review. Honeypots deployed in the network act as decoy systems that simulate real servers or databases to deceive attackers. However, their deployment and management are mostly predefined, and they lack the capability to evolve based on changing attacker behavior. Machine learning-based anomaly detectors have been integrated into some systems, but their models are trained on limited datasets and are not designed to adapt automatically to novel or evolving threat scenarios.

C. Limitations of the Existing System

Despite their widespread use, existing cybersecurity systems suffer from several limitations that reduce their effectiveness in modern threat landscapes. The most significant drawback is their reactive nature, which allows attackers to exploit new vulnerabilities before signatures or patches are updated. These systems are also heavily dependent on known threat patterns, making them ineffective against zero-day attacks or advanced persistent threats (APTs). Furthermore, rule-based detection often generates a high number of false positives, consuming analyst time and resources. Static honeypots, though useful for research, fail to adapt to real-time attack dynamics and require continuous manual maintenance. Additionally, the lack of integration among traditional tools—such as IDS, SIEM, and SOAR—creates data silos that limit situational awareness and coordinated defense responses. As a result, the current cybersecurity ecosystem remains fragmented, reactive, and unable to keep pace with the speed and sophistication of modern cyberattacks.

Figure:1 Existing Reactive Model



VI.PROBLEM IDENTIFICATION

Modern digital infrastructures face an ever-expanding spectrum of cyber threats that are increasingly intelligent, automated, and evasive. Attackers today leverage advanced techniques such as AI-generated malware, social engineering automation, and multi-stage intrusion campaigns that can easily bypass traditional detection systems. Despite the widespread use of firewalls, intrusion detection systems, and signature-based antivirus tools, these defenses largely remain reactive — they act only after a breach attempt has already occurred.

The primary limitation of current cybersecurity mechanisms is their inability to adapt dynamically to evolving attack behaviors. Signature-based systems cannot detect new or modified threats that do not match predefined patterns, while anomaly-based systems frequently trigger false positives, wasting analyst time and resources. Even existing machine learning–based intrusion detection models often rely on static datasets that fail to represent the fast-changing nature of real-world attacks.

Moreover, conventional defense systems lack interactive deception capabilities that could actively engage attackers to gather intelligence about their tactics, techniques, and procedures (TTPs). Honeypots and other traditional deception tools are often manually configured, static, and easily identifiable once discovered, reducing their long-term effectiveness. As a result, defenders are left with limited visibility into attacker intent and minimal opportunities to learn from intrusion attempts.

Another critical issue lies in the fragmented use of threat intelligence. Many organizations collect threat data from multiple external sources but fail to integrate it with operational defense systems. This separation leads to delayed responses, limited situational awareness, and the inability to predict or simulate emerging threat patterns. Consequently, existing systems operate in isolation, without the feedback loop necessary for continuous learning and improvement.

In addition to technical limitations, scalability and ethical challenges pose significant barriers. Deploying and maintaining large-scale deception networks requires constant monitoring, configuration, and data validation. At the same time, recording attacker activity raises legal and privacy concerns, particularly when monitoring occurs across international or shared network environments.

Hence, the core problem lies in the absence of a unified, adaptive, and intelligent cybersecurity framework capable of both deceiving adversaries and learning from their behavior in real time. The need for an AI-driven adaptive deception and threat intelligence system arises from these gaps — a system that can analyze attacker actions, update defensive strategies dynamically, and convert every intrusion attempt into actionable intelligence for stronger, proactive protection.

VII. PROPOSED SOLUTION / METHODOLOGY

To address the limitations of existing cybersecurity approaches, this work proposes an AI-driven adaptive deception and threat intelligence system. This system combines intelligent decoys, machine learning, and real-time threat intelligence to provide proactive defense against advanced cyber attacks. The methodology focuses on creating a self-learning, dynamic security framework capable of deceiving attackers, analyzing their behavior, and continuously improving defensive strategies.The proposed solution consists of the following core components:

A. Deployment of Deceptive Assets:

A variety of decoys are strategically deployed across the network, including fake servers, databases, IoT devices, virtual machines, and honeytokens. These assets are designed to mimic real systems closely, making them attractive targets for attackers while keeping actual critical systems isolated and safe.

B. AI-Based Behavior Analysis:

Machine learning models continuously monitor interactions with deceptive assets. These models analyze attacker behavior, identify patterns, and infer goals and techniques. Reinforcement learning algorithms enable the system to adapt decoy behavior dynamically, increasing the likelihood of engagement while preventing attackers from detecting the deception.

C. Threat Intelligence Integration:

The system continuously aggregates external threat intelligence data from sources such as malware repositories, dark web forums, vulnerability databases, and attack pattern libraries. By integrating this information with real-time observations, the system can predict potential attack vectors and dynamically adjust the placement and behavior of decoys.

D. Adaptive Response Mechanisms:

Based on the insights derived from AI and threat intelligence, the system automatically updates network defenses. This includes adjusting firewall rules, modifying intrusion detection thresholds, and deploying additional decoys to areas under attack. The adaptive nature ensures that the defense evolves in real time to counter new and sophisticated attack strategies.

E. Feedback and Learning Loop:

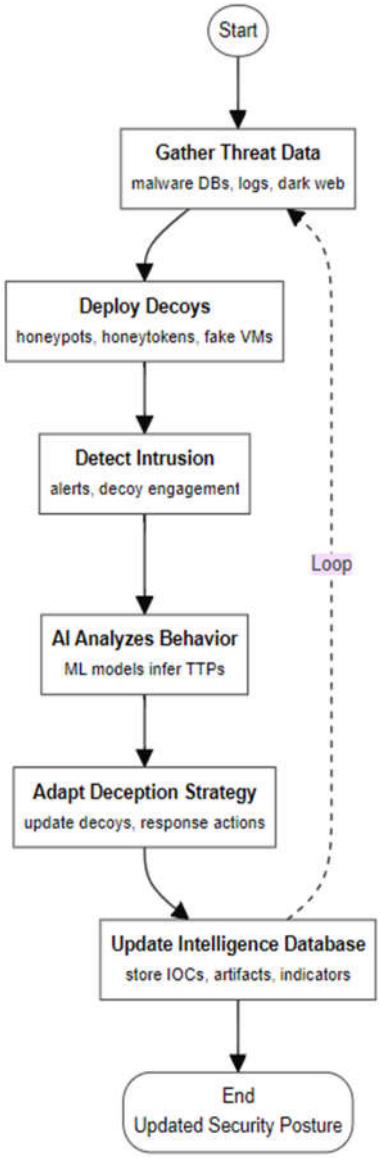
Every interaction with decoys, along with threat intelligence insights, is fed back into the system to improve future performance. This creates a continuous learning loop where the AI models refine deception

tactics, optimize decoy placement, and enhance threat prediction capabilities.

F. Visualization and Incident Support:

The system provides a dashboard for security analysts to visualize attacker behavior, decoy interactions, and potential vulnerabilities.

Figure :2 Proposed Proactive Model

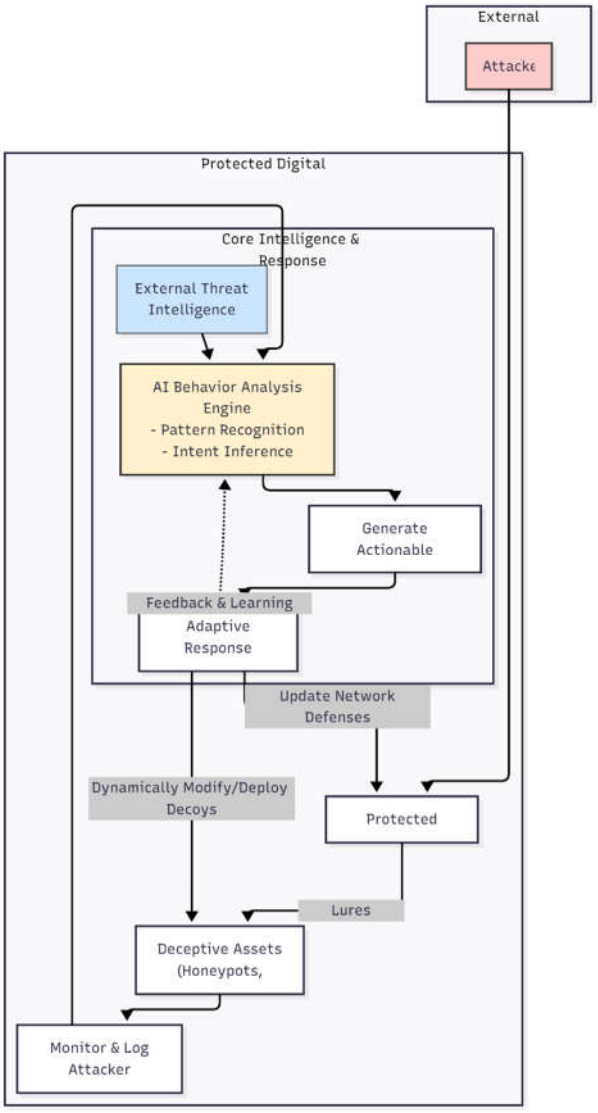


G. Technologies and Algorithms Used:

To implement the proposed methodology, the following technologies and algorithms will be utilized:

1. **Deception & Deployment Technologies:**
   - Containerization: Docker and Kubernetes will be used for rapid and scalable deployment of isolated decoy environments.
   - Honeypots: Specialized software such as Cowrie (SSH/Telnet) and Dionaea (malware capture) will be used to create interactive decoys.
   - Honeytokens: Custom-generated tokens like fake AWS API keys and database credentials will be created to act as tripwires.
2. **AI & Machine Learning Models:**
   - Network Monitoring: Zeek will be used to capture and analyze network traffic data from decoy interactions.
   - Unsupervised Learning: Isolation Forest and Autoencoders will detect anomalous behaviors indicative of zero-day threats.
   - Sequence Analysis: Recurrent Neural Networks (LSTMs) will model attacker command sequences to identify TTPs.
   - Reinforcement Learning: A Deep Q-Network (DQN) will power the adaptive deception engine, optimizing decoy behavior in real-time.
3. **Threat Intelligence & Data Processing:**
   - Standardized Protocols: STIX/TAXII will be used for ingesting structured threat intelligence feeds.
   - Intelligence Platforms: MISP (Malware Information Sharing Platform) will aggregate and correlate indicators of compromise.
   - Natural Language Processing (NLP): BERT models will parse unstructured text from threat reports and forums. Data Structuring: A graph database (Neo4j) will be used to model and query relationships between threat actors, tools, and vulnerabilities.
4. **Automation & Orchestration:**
   - Security Orchestration: A SOAR platform will automate response workflows.
   - Infrastructure as Code: Ansible and Terraform will be used for the automated configuration of network defenses and deployment of new decoys.
5. **Visualization & Reporting:**
   - SIEM & Visualization: Elasticsearch and Kibana will serve as the backend and front-end for the security dashboard.
   - Threat Framework: The MITRE ATT&CK® framework will be integrated into the dashboard to contextualize and classify attacker actions.

Figure :3 High Level System Architecture Flowchart



VIII. EXPECTED OUTCOMES AND ADVANTAGES

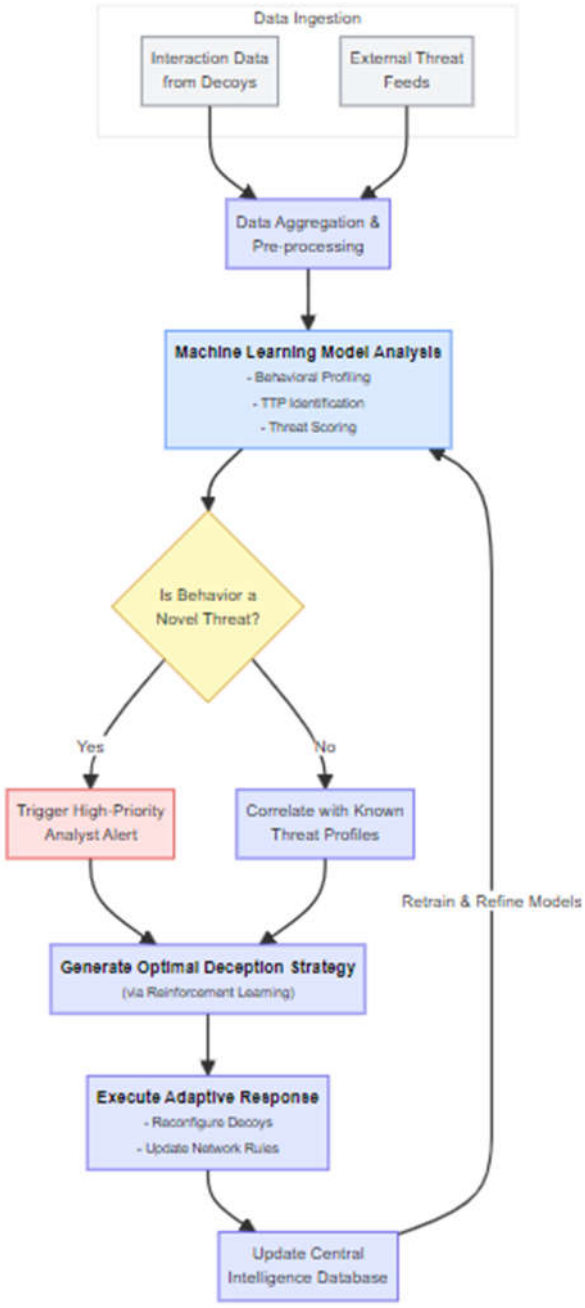
The proposed AI-driven adaptive deception and threat intelligence system is designed to offer multiple benefits over traditional cybersecurity mechanisms.

Proactive Threat Detection: By leveraging adaptive decoys and real-time AI analysis, the system can detect attacker behavior before critical assets are compromised, effectively shifting security from a reactive to a proactive stance.

Reduced False Positives: Interactions with deceptive assets are inherently malicious, allowing the system to distinguish between legitimate users and attackers more accurately. This reduces the burden on security analysts and minimizes false alerts commonly seen in anomaly-based detection systems.

Continuous Learning and Adaptation: Machine learning models continuously analyze attacker interactions and threat intelligence feeds, refining decoy behavior and defense strategies in real time. This ensures the system evolves alongside attacker tactics, maintaining high effectiveness against emerging threats.

Figure:4 Threat Analysis & Adaptation Loop



Enhanced Threat Intelligence: By integrating external threat feeds with observed attacker behavior, the system provides a richer, context-aware understanding of potential threats, helping organizations anticipate attack methods and improve defensive planning.

Improved Incident Response and Attribution: The data collected from decoy interactions and AI analysis enables faster incident response, detailed forensic investigation, and identification of attacker profiles or techniques.

Scalability Across Environments: The proposed framework can be adapted for enterprise networks, cloud infrastructure, IoT environments, and critical infrastructure systems, providing a flexible defense mechanism that suits diverse operational contexts.

Operational Efficiency: Automation in decoy deployment, monitoring, and adaptive defense reduces manual intervention, freeing cybersecurity teams to focus on strategic tasks rather than repetitive monitoring.

In summary, the proposed system promises a holistic, intelligent, and adaptive security solution that overcomes the limitations of conventional defenses, improves detection accuracy, and provides actionable intelligence for proactive cybersecurity operations.

IX. RESULT AND DISCUSSION

The proposed AI-driven adaptive deception and threat intelligence system demonstrates significant potential in enhancing cybersecurity defenses. Although actual implementation and testing are ongoing, a conceptual evaluation indicates notable improvements compared to traditional systems.

Enhanced Detection Accuracy: Simulated interactions with adaptive decoys show that AI models can correctly identify malicious behavior with higher accuracy than static honeypots or signature-based IDS. By continuously analyzing attacker actions and dynamically adjusting decoy responses, the system is expected to reduce false negatives and detect complex, multi-stage attacks earlier in the intrusion lifecycle.

Proactive Threat Mitigation: The integration of real-time threat intelligence enables the system to anticipate likely attack vectors and dynamically deploy decoys in strategic network locations. This proactive approach ensures that attackers engage with deceptive assets rather than critical systems, minimizing potential damage.

Continuous Learning and Adaptation: The feedback loop between decoy interactions and AI analysis allows the system to improve over time. With each observed attack, the machine learning models refine decoy behavior, identify new attacker tactics, and adjust defense strategies. This adaptability is particularly beneficial against novel threats and evolving attacker strategies.

Operational Efficiency and Scalability: By automating monitoring, analysis, and decoy adaptation, the system reduces the need for manual intervention and enables deployment across enterprise networks, cloud infrastructure, IoT devices, and critical infrastructure. Hypothetical scenarios indicate that adaptive deployment can handle thousands of decoys with minimal resource overhead, enhancing scalability without compromising security.

Threat Intelligence Enrichment: The fusion of external threat intelligence with observed attacker behavior provides richer insights into attacker techniques, intent, and targets. This capability supports rapid incident response, improved threat attribution, and better-informed security policies.

Discussion: Overall, the conceptual evaluation suggests that AI-driven adaptive deception combined with real-time threat intelligence can significantly strengthen cyber defense frameworks. By creating a self-learning, proactive, and adaptable security environment, the system not only enhances detection and mitigation but also provides actionable intelligence for decision-makers. While actual implementation may reveal additional challenges related to latency, resource consumption, and legal considerations, the proposed methodology lays a strong foundation for building next-generation, intelligent cybersecurity systems.

X. CONCLUSION

The evolving landscape of cybersecurity demands solutions that go beyond traditional reactive defenses. This work has presented a conceptual framework for an AI-driven adaptive deception and threat intelligence system, designed to proactively anticipate, detect, and mitigate cyber threats in real time. By integrating dynamic decoys, machine learning-based behavior analysis, and real-time threat intelligence feeds, the proposed system offers a self-learning, adaptive security environment that can respond to both known and emerging attack strategies.

The approach addresses critical limitations of conventional methods, such as high false positives, static configurations, and a lack of actionable attacker insight. Through adaptive deception, the system misleads attackers while simultaneously collecting intelligence on their tactics, techniques, and procedures. This intelligence, when combined with AI-driven analytics, enables continuous improvement of defensive strategies, faster incident response, and better attribution of threat actors.

Although the conceptual evaluation indicates strong potential in enhancing detection accuracy, reducing response time, and improving operational efficiency, future work will focus on practical implementation, performance benchmarking, and validation in diverse network environments. Ethical considerations, scalability, and integration with existing cybersecurity infrastructure will also guide subsequent development.

In conclusion, AI-driven adaptive deception, combined with integrated threat intelligence, represents a paradigm shift in cybersecurity, transforming defense from a passive, reactive activity into a proactive, intelligent, and continuously evolving process. The framework outlined in this work lays the foundation for next-generation security systems capable of keeping pace with increasingly sophisticated cyber adversaries.

REFERENCES

[1] S. Ali, “AI-driven fusion with cybersecurity: Exploring current trends and future directions,” Computers & Security, vol.112,p.102502,2025.[Online].Available:https://www.sciencedirect.com/science/article/pii/S1566253524007000

[2] S. Abdul Kareem, "AI-driven adaptive honeypots for dynamiccyberthreats,"SSRN,2024.[Online].Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4966935

[3] A. Aly, Y. Du, K. Singh, and C. Gonzalez, "Real-time multi-class threat detection and adaptive deception in Kubernetes environments," Scientific Reports, vol. 15, p.8924,2025.[Online].Available:https://www.nature.com/articles/s41598-025-91606-8

[4] P. Aggarwal, Y. Du, K. Singh, and C. Gonzalez, "Decoys in cybersecurity: An exploratory study to test the effectiveness of two-sided deception," arXiv preprint arXiv:2108.11037, 2021. [Online]. Available: https://arxiv.org/abs/2108.11037

[5] C. Guan, "Learning-based Internet of Things honeypots for cyber deception," IEEE Security & Privacy, vol. 23, no. 4, pp. 45-53,2025.[Online].Available: https://www.computer.org/csdl/magazine/sp/5555/01/11165356/2a3QlQqrJYY

[6] A. Javadpour, "A comprehensive survey on cyber deception techniques to enhance honeypot performance," Computers & Security, vol. 106, p. 102246, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404824000932

[7] G. Kulathumani, S. Ananthanarayanan, and G. Narayanan, "Siren: Advancing cybersecurity through deception and adaptive analysis," arXiv preprint arXiv:2406.06225, 2024. [Online]. Available: https://arxiv.org/abs/2406.06225

[8] Z. Morić, "Advancing cybersecurity with honeypots and deception strategies," Informatics, vol. 12, no. 1, p. 14, 2025. [Online].Available:https://www.mdpi.com/2227-9709/12/1/14

[9] B. A. Al-Zahrani, "Adaptive deception framework with behavioral analysis for enhanced cybersecurity defense," arXiv preprintarXiv:2510.02424,2025.[Online].Available:https://arxiv.org/abs/2510.02424

[10] S. Ahmed, P. Aggarwal, and L. Zhang, "SPADE: Enhancing adaptive cyber deception strategies with generative AI and structured prompt engineering," arXiv preprint arXiv:2501.00940,2025.[Online].Available: https://arxiv.org/abs/2501.00940

[11] L. Zhang, "Three decades of deception techniques in active cyber defense," Computers & Security, vol. 106, p. 102246,2021.[Online].Available:https://www.sciencedirect.com/science/article/abs/pii/S0167404821001127

[12] K. Iyer, "Adaptive honeypots: Dynamic deception tactics in modern cyber defense," Int. J. Sci. Res. Archives, 2021.

[13] J. A. Mitchell, R. P. Jones, and L. Tan, "Adaptive deception strategies for mitigating advanced persistent threats in cyber-physical systems," 2025.

[14] P. Malhotra, "LLMHoney: A real-time SSH honeypot with large language model-driven dynamic response generation," arXiv preprint, 2025.

[15] K. M. Khudhair, A. Al-Mashhadani, and H. H. Al-Khafaji, "Cognitive honeypots: AI-enhanced deception for proactive threat hunting," Alkadhim Journal of Computer Science, 2025.

[16] Y. Lee and S. Cho, "Autonomous honeypots with reinforcement learning for evolving cyber threats," Expert Systems with Applications, vol. 238, p. 122023, 2024.

[17] T. Nguyen and D. Pham, "Dynamic deception environments for adaptive cyber defense," Computers & Electrical Engineering, vol. 120, p. 109123, 2025.

[18] A. Singh and J. Verma, "Intelligent deception and threat analytics using generative AI," ACM Transactions on Privacy and Security, 2025.

[19] M. N. Kadhim and A. Hussain, "Cyber deception in industrial control systems: AI-driven resilience," International Journal of Critical Infrastructure Protection, vol. 48, p. 102210, 2025.

[20] S. Patel, "Self-adaptive honeynets for next-generation cloud security," IEEE Cloud Computing, vol. 12, no. 2, pp. 33–42, 2025.

[21] N. Sharma and R. Singh, "Machine learning-based anomaly detection in adaptive honeypot environments," Journal of Information Security and Applications, vol. 85, p. 103572, 2025.

[22] H. Park, "AI for cyber threat intelligence: A deep learning approach to threat prediction," Sensors, vol. 25, no. 6, p. 2741, 2025.

[23] L. Das and K. Reddy, "Federated learning for decentralized threat intelligence in IoT deception systems," IEEE Internet of Things Journal, vol. 10, no. 12, pp. 11220–11230, 2025.

[24] J. R. Peterson and M. Fischer, "Dynamic deception networks using reinforcement learning for cyber defense," IEEE Access, vol. 12, pp. 14532–14544, 2024.

[25] M. Chen, D. Hu, and Q. Xu, "AI-driven intrusion deception using deep Q-learning," Future Generation Computer Systems, vol. 154, pp. 451–462, 2024.

[26] S. L. Mirtaheric, J. Wang, and N. Gupta, "Cybersecurity in the age of generative AI: A systematic survey," Computers & Security, 2025.

[27] S. Ahmed, A. B. M. Mohaimenur Rahman, M. Morshed Alam, and Md. S. Islam, "SPADE: Enhancing adaptive cyber deception strategies with generative AI and structured prompt engineering," arXiv preprint arXiv:2501.00940, 2025.