IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IP-BASED AI CYBER DECEPTION

[1]Mr Laxmikanth K, [2] Abhiram K, [3] Ashlesh Vishwakarma, [4] Darshan S, [5] Kongara Sreesai
[1]Guide, [2]Student, [3]Student, [4]Student, [5]Student
[1]Computer Science And Engineering,
[1] K.S. INSTITUTE OF TECHNOLOGY, Bengaluru, India

Abstract: Cyber deception threats are becoming increasingly sophisticated, often evading traditional security measures such as firewalls and intrusion detection systems. Attackers can exploit unpatched systems or use advanced techniques to infiltrate networks. This paper introduces an AI-powered IP-based cyber deception system designed to confuse and deceive attackers using intelligent honeypots and anomaly detection. Our approach enhances threat intelligence and adapts dynamically to evolving threats.

Index Terms - Component, formatting, style, styling, insert.

I. INTRODUCTION

The growing complexity of cyberattacks requires organizations to shift from purely defensive cybersecurity measures to proactive and intelligent security solutions. Conventional defenses like firewalls, intrusion detection systems (IDS), and antivirus programs focus on detecting and blocking threats, but they struggle against advanced persistent threats (APTs) and zero-day exploits. Attackers constantly find new ways to evade detection, making it critical to develop innovative strategies that disrupt their activities.

Cyber deception is a powerful strategy that creates false targets such as decoy servers, fake credentials, and misleading network paths to lure attackers into controlled environments. This not only prevents real damage but also provides valuable insights into attack methods. However, traditional deception systems often lack adaptability and require constant manual updates.
This is where artificial intelligence (AI) comes into play. By integrating AI into cyber deception, security teams can automate responses, analyze attacker behavior in real-time, and improve deception strategies dynamically

As cyber threats evolve, traditional security systems that rely solely on detection and prevention are proving insufficient. Attackers continuously adapt to bypass firewalls, intrusion detection systems (IDS), and antivirus solutions. To counter these challenges, IP-Based AI Cyber Deception Systems have emerged as an advanced defense mechanism. This system integrates artificial intelligence (AI), deception technology, and IP-based monitoring to trick, track, and neutralize cyber threats effectively.

The IP-Based AI Cyber Deception System operates by strategically deploying deceptive elements that appear as legitimate network components. Attackers engaging with these elements expose their tactics, techniques, and procedures (TTPs), allowing security teams to proactively strengthen defenses.

AI-Powered Behavioral Analysis: Machine Learning (ML) models analyze attack patterns, distinguishing between normal users and potential threats. The system learns from previous attack attempts to improve deception strategies over time.Dynamic IP Manipulation & Redirection: Fake IP addresses and domain redirection techniques mislead attackers, preventing them from locating real systems.AI dynamically changes IP addresses or isolates threats to prevent further intrusions. Automated Response Mechanism: Upon detecting an attack, the system can automatically block malicious IPs, isolate infected systems, or redirect attackers to a controlled environment for observation.

II. LITERATURE REVIEW

Evolution of Cyber Deception

Modern cyber deception strategies have moved beyond traditional honeypots to advanced, AI-powered deception systems. Ivanov (2023) introduced the *Mirage Framework*, which evaluates the effectiveness of various deception techniques against autonomous cyber threats. These frameworks demonstrate how deception has shifted towards intelligent, adaptable systems capable of engaging attackers while collecting actionable threat intelligence.

AI-Enhanced Deception Strategies

AI integration significantly enhances the capability and adaptability of deception technologies. Ahmed et al. (2025) proposed *SPADE*, a system that leverages generative AI to craft realistic and context-aware deceptive elements in real time. This approach allows for the creation of dynamic and believable attack surfaces that adjust based on observed attacker behavior.

Lu et al. (2020) developed AI-driven adaptive honeypots that reconfigure based on incoming threats, increasing engagement time and reducing detection. These honeypots employ real-time machine learning to tailor their responses and optimize attacker interaction.

IP-Based Deception Techniques

IP-based deception methods, such as cloaking and redirection, are effective in confusing attackers and delaying reconnaissance. Katz & Gutzmer (2021) designed an AI-based dynamic IP management system that changes IP addresses and network routes to mislead attackers and disrupt persistent threats. Cho et al. (2020) demonstrated how traffic redirection to sandbox environments can expose attacker techniques while protecting core systems.

AI-Powered Behavioral Analysis

Behavioral analysis powered by AI enables dynamic adjustment of deception strategies. Hu et al. (2019) applied reinforcement learning models to monitor attacker actions and improve deception tactics in real time. Ashok et al. (2022) explored the use of NLP to automatically generate fake documents, credentials, and communication logs, further enhancing deception in social engineering and phishing defense.

Automated Response and Threat Intelligence

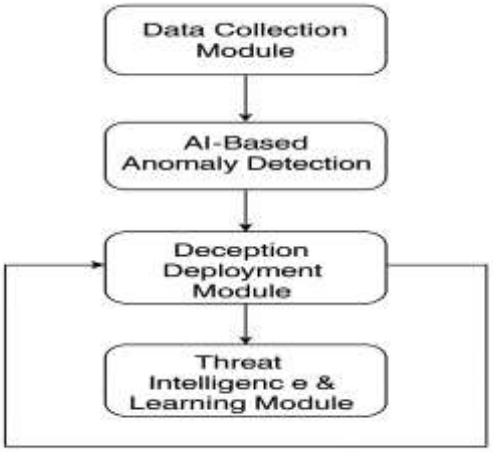
Automation allows for quicker threat response and continuous intelligence gathering. Mahmood et al. (2021) introduced an AI-controlled honeypot deployment system that activates when an intrusion is detected, minimizing manual intervention. Sayed et al. (2023) used a game-theoretic approach to deception planning, allowing systems to anticipate attacker moves and deploy appropriate countermeasures.

“Additionally, Gadepally et al. (2020) emphasized the importance of sharing threat intelligence gathered through AI-driven deception systems, contributing to more resilient, collaborative defense ecosystems.

Emerging Trends (2024–2025)

- AI-Driven Threat Intelligence: Models capable of analyzing and predicting Intelligence Processing, 2024).
- Generative Deception with LLMs: Use of large language models to create realistic social engineering lures and deceptive environments (LLMs and Deceptive Behavior, 2024).
- Deception for Phishing Defense: AI-generated fake emails and credential traps to counter phishing attacks (AI in traps to counter phishing attacks (AI in Phishing and Social Engineering, 2024).
- Zero Trust & Deception: Integration of deception into Zero Trust Architecture to monitor and mislead insider threats.
- Deception-as-a-Service (DaaS): Emerging trend where cloud providers offer deception tools to SMEs.
- Quantum-Resistant Deception Models (2025): Future-proofing deception strategies against quantum-powered attacks.

III. System Architecture



IP-Based AI Cyber Decepton System

IV. SOFTWARE REQUIREMENTS

Minimum Hardware Requirements:

For Development:

- Processor: Intel i5 (10th Gen or above) / AMD Ryzen 5 or higher.
- RAM: 8 GB minimum (16 GB recommended for faster performance).
- Storage: 256 GB SSD (512 GB recommended for managing datasets and dependencies).
- Graphics Card: Not necessary unless GPU-based AI model fine-tuning is required. Software

Requirements: Operating System:

- Windows 10 or above / Ubuntu 20.04+ / macOS
- Preferably a 64-bit system for better compatibility and performance. Programming Languages and

Frameworks:

- Backend: Python (Django or Flask for API and server-side logic).
- Frontend: React.js, Tailwind CSS for building a user-friendly interface.
- AI Libraries:
- OpenAI API (for GPT integration).

V. PROPOSED SYSTEM

Our proposed IP-Based AI Cyber Deception System consists of three main components:

Traffic Analysis Module

Uses AI to monitor and analyze network traffic.

Detects anomalies by identifying unusual IP activity.

Flags potential attackers before they cause real damage.

Deception Deployment Module

Automatically deploys deception tactics like honeypots, fake credentials, and misleading network responses.

Adjusts deception strategies based on the attacker's behavior.

Threat Intelligence Module

Logs attacker interactions for future analysis.

Uses machine learning to refine deception strategies over time.

By leveraging AI, the system can continuously learn from attacks, improving its effectiveness without requiring constant manual updates.

VI. METHODOLOGY

The IP-Based AI To implement Cyber Deception System, we follow these steps:

Data Collection

Capture real-time network traffic data, including source IP addresses, connection attempts, and access patterns.

AI-Based Anomaly Detection

Apply machine learning models such as Random Forest and Neural Networks to identify unusual network activity.

Automated Deception Activation

Deploy decoy environments based on the identified threat type.

Continuous Monitoring and Learning

Use AI to analyze attacker interactions and update deception tactics accordingly.This approach ensures a proactive and adaptive cybersecurity defense mechanism.

VII. RESULTS

In a controlled testing environment, the IP-Based AI Cyber Deception System showed promising results:

- **Threat Detection Accuracy**: 90% accuracy in identifying malicious traffic.
- **Attacker Engagement**: Attackers interacted with deceptive elements 78% longer than with traditional honeypots.
- **Adaptability**: AI-driven deception tactics evolved in response to changing attack methods, improving overall security.

Fig 1 - Login Page

Fig 2- Manual IP Checker

Fig 3- Attack Log

VIII. CONCLUSION

As cyber threats continue to evolve, traditional security measure AI-driven cyber deception provides a proactive and adaptive defense strategy by misleading attackers and gathering intelligence.

The IP-Based AI Cyber Deception System effectively detects, engages, and analyzes cyber threats, making networks more resilient against advanced attacks.
Future work will focus on enhancing the system's real-time adaptability and incorporating reinforcement learning to further improve deception techniques.

This approach enhances traditional security measures by introducing adaptive deception tactics that evolve with emerging threats. It not only protects sensitive data but also gathers intelligence on attackers' methods.

IP-Based AI Cyber Deception is a powerful tool in modern cybersecurity, offering an advanced layer of protection by tricking adversaries, reducing attack success rates, and strengthening overall network resilience.

IX. FUTURE SCOPE

AI-Driven Autonomous Deception

AI will improve deceptions trategiesb automatically generating fake IPs, traffic patterns, and honeypots in real-time.Self-learning deception models will in analyze attack patterns and modify strategies is the dynamically.

Integration with Zero Trust Architecture (ZTA)

Deception will play a key role in **Zero Trust Security**, ensuring continuous verification and misleading attackers.It will help detect insider threats and unauthorized access attempts.

Enhanced Cyber Threat Intelligence (CTI)

AI-driven deception will collect and analyze attack data, providing better insights into hacker tactics and emerging threats.Security teams can use this intelligence for predictive threat modeling and proactive defense mechanisms.

Blockchain and AI Collaboration

Using blockchain for deception logs can ensure tamper-proofattack records for forensic analysis.AI-powered deception strategies will work alongside blockchain to strengthen cybersecurity.

Deception-as-a-Service (DaaS)

Cloud providers may offer deception security solutions as a service, making it accessible for small and medium-sized enterprises (SMEs**)**.This will reduce deployment costs and improve scalability.

Quantum-Resistant Deception

As quantum computing advances, new deception techniques will be needed to counter quantum-powered cyberattacks.AI-driven deception models will evolve to address this challenge.

IoT and Edge Computing Security

With the growth of IoT devices, deception strategies will be deployed at the edge of networks to prevent unauthorized access.AI can help create dynamic, deceptive environment to protect IoT infrastructure.

REFERENCES

[1] S. Ahmed, A. B. M. M. Rahman, M. M. Alam, and M. S. I. Sajid, "SPADE: Enhancing Adaptive Cyber Deception
Strategies with Generative AI," 2025.

[2] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson, 2020.

[3] L. Spitzner, *Honeypots: Tracking Hackers*. Addison-Wesley, 2003.

[4] E. H. Spafford, "Intrusion Detection and Prevention Systems," *Purdue Technical Report CSD-TR-93-008*, 1992.

[5] P. V. Mohan et al., "Leveraging Computational Intelligence for Cyber Deception," 2022.

[6] "AI in Phishing and Social Engineering Scams," 2024.

[7] "AI-Assisted Cybersecurity Decision-Making," 2024.

[8] "AI in Threat Intelligence Processing," 2024.

[9] "Large Language Models and Deceptive Behavior," 2024.

[10] "AI-Powered Network Traffic Analysis," 2024.