International Journal of Informatics and Data Science Research
ISSN 2997-3961 (Online)
Vol. 2, No. 8, Aug 2025,
Available online at: https://scientificbulletin.com/index.php/IJIDSR

Stealth Cyber Defense System: Virtual Camouflage Architecture for Real-Time Intrusion Resistance

Wasen Mohammed Najem
Al-Diwaniya Technical Institute AL-Furat AL-Awsat Technical University – Iraq, wasen.najm@atu.edu.iq

Nejood Abed yasir ibadi
Al-Diwaniya Technical Institute AL-Furat AL-Awsat Technical University – Iraq, nejood.abadi.idi@atu.edu.iq

Ohood Ali Mohammed
Al-Diwaniya Technical Institute AL-Furat AL-Awsat Technical University – Iraq, ohood.mohammed@atu.edu.iq

Article information:
Manuscript received: 4 Jun 2025; **Accepted:** 10 Jul 2025; **Published:** 11 Aug 2025

Abstract: In front of rapidly developed cyber threats, traditional safety systems often decrease because of their reactive nature and visual infrastructure. This research introduces an innovative stealth cyber defense system based on a virtual camouflage architecture that works invisible in the network to detect, mislead and neutralize real - time infiltration. The system integrates artificial intelligence for analyzing behavior - based danger, and removes the misleading virtual environment as well as attackers from significant infrastructure. Unlike traditional defense mechanisms, this model emphasizes active deception and secret operations, which increases the flexibility of advanced persistent hazards (APTS) and zero-day attacks. A broad theoretical structure is proposed, and the design capacity of patent registration is evaluated. The purpose of this study is to transfer cyber security paradigm to intelligent misunderstanding against static protection, Contributions from a new layer of strategic defense to the digital ecosystem.

Keywords: Stealth Cybersecurity, Intrusion Detection, Virtual Camouflage, CNN-LSTM, Deceptive Defense, Real-Time Response, Intelligent Systems, Cyber Threat Mitigation

1. Introduction

In the landscape that sometimes developed cyber security, traditional identification and prevention systems are often reactive, providing limited protection against rapid new and sophisticated dangers. Firewalls, infiltration detection systems (ID -er) and encryption protocols are effective to some extent, attackers do quickly advanced tasks stolen technology and AI-operated harmful software to bypass this defense

This study introduces a novel concept of a **Stealth Cyber Defense System**, utilizing a **virtual camouflage architecture** that operates invisibly within the network to detect, deceive, and neutralize threats in real-time. Inspired by military-grade stealth strategies and honeynet technologies, this system is designed not to block attacks outright but to intelligently divert and observe them without exposing the true infrastructure.

AI-led behavioral analysis and merger with virtual deception provides a new defense paradigm that is active, adaptive and potentially invisible to the attackers-from the Armed Forces to transfer cyber security for strategic misunderstandings.

1-1 Background

Cyber security is a constantly developed sector, challenging the rapid development of continuous attack vectors, including advanced compatible hazards (APTS), zero-day weaknesses and AI-related harmful software. Traditional defense system - such as firewalls, infiltration detection systems (IDS) and antivirus tools - often function on the basis of signature recognition or predetermined rules, making them ineffective against novels and quiet attacks (Vinayaumar in Al, 2019). These systems are reactive and struggle to detect intelligent and frequent intruding in real time, especially when the attacker deliberately avoids triggering the known signature known signature.

1-2 Rationale of the Study

The main area of current cyber security solutions lies in their visibility and prediction. When an attacker identifies the defense strategy, they can adjust their techniques to bypass it. Therefore, a paradigm is required - from reactive to active defense, from visibility to secret and from passive monitoring to intelligent deception. This research proposes a stealth cyber defense system based on a virtual. Camouflage architecture, creating a misleading digital environment and attracting includes the attackers, while the core infrastructure is hidden and preserved.

1-3 Research Motivation

Inspired by military stealth strategy and Honston Technologies, this system utilizes AI-based behavioral analysis and virtual crazy layers to cheat cyber thighers. Instead of immediately blocking or notifying the attacker, the system is learning the screen and their behavior, gaining insight into attack patterns and techniques. This concept shows a change in strategic misunderstanding and cyber-kamuflage from preventive strategies, which increases the flexibility of both known and unknown threats.

1-4 Research Gap

Although previous studies have shown honey and deception technologies, they are often isolated and detected due to poor integration or lack of intelligent automation (alhaj at Al., 2020). In addition, some systems work invisible or integrate real -time AI analysis with dynamic camouflage architecture. This research fulfills the difference that remains invisible, adaptive and active by suggesting an integrated and intelligent design.

1-5 Proposed System Overview

This study introduces an original system architecture combination:

- Invisible observation nodes
- Virtual environments with fake assets
- Behavioral analysis using machine learning
- Real-time decision logic

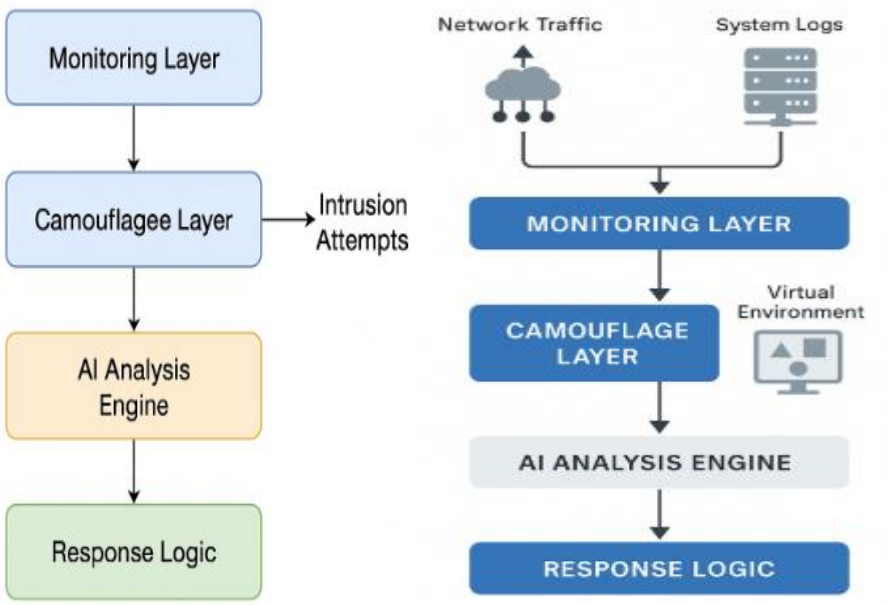


Figure 1.1: Virtual campaign architecture proposed for Sneaky Cyber Defense

This allows the architectural system to simulate realistic goals, mislead the invaders, analyze the strategy and give dynamic reactions dynamically without revealing the real infrastructure.

1-6 Structure of the Paper

This paper is organized as follows:

- **Section 2:** Literature Review – discusses related works and research gaps
- **Section 3:** System Architecture – explains the design of the virtual camouflage system
- **Section 4:** Methodology and Experimental Setup
- **Section 5:** Evaluation Metrics and Comparative Analysis
- **Section 6:** Discussion and Future Work
- **Section 7:** Conclusion and Recommendations

2. Literature Review

2-1 Overview of Cyber Defense Mechanisms

Modern cyber defense strategies come about two categories: reactive and active. Reactive systems, such as signature-based infiltration detection systems (IDs), identify the known attack pattern according to their existence (Vinayakumar et al., 2019). While they are skilled in detecting traditional harmful software, they do not respond to zero-day and secret attacks. On the other hand, proactive strategies include **behavioral analysis, deception technologies, and honeypots**, which attempt to anticipate or mislead attackers before damage occurs (Spitzner, 2003).

2-2 Honeypots and Deceptive Technologies

Honeypots are decoy systems that appear to be legitimate network resources to lure attackers. While effective in capturing threat intelligence, traditional honeypots are often static, easily fingerprinted, and detectable. High-interaction honeynets improve realism but come with high maintenance and risk if attackers gain control (Alhaj et al., 2020).

Feature	Low-Interaction Honeypots	High-Interaction Honeypots	Proposed System (Virtual Camouflage)
Detectability	High	Medium	Very Low (Stealth Layered)
Realism	Low	High	High with AI Adaptivity
Resource Consumption	Low	High	Moderate
Risk if Compromised	Low	High	Very Low (Isolated Fake Envs)
Integration with AI	Minimal	Rare	Core Component

Table 2.1: Comparison between Honeypot Types

2-3 Behavioral Analysis in Intrusion Detection

Recent studies have explored the use of machine learning for intrusion detection, especially using datasets such as **NSL-KDD** and **CICIDS2017**. Convolutional Neural Networks (CNN), LSTM, and hybrid models have shown promising accuracy in detecting anomalous behavior in real-time traffic (Yin et al., 2017; Vinayakumar et al., 2019).

However, most models are designed to classify traffic, not to **engage attackers in deceptive environments**, nor are they embedded in **invisible architectures**. This gap in dynamic interaction and stealth integration highlights the need for a system like the one proposed in this research.

2-4 Intelligent Deception Models

Recent frameworks attempt to combine **deception + automation**. For example:

- **SHIELD** by MITRE offers dynamic deception layers but lacks AI-based behavioral analysis.
- **Moving Target Defense (MTD)** introduces randomness in network configuration, but can degrade performance and is not stealthy by design.
- **AI-Driven Adaptive Honeynets** offer some dynamic behavior, but are not fully integrated with real-time response engines.

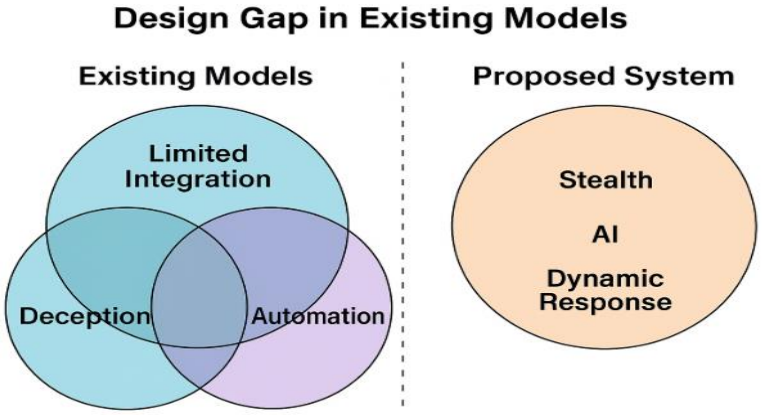


Figure 2.1: Design Gap in Existing Models

Existing models suffer from limited integration of stealth, AI-based analysis, and dynamic deception. Traditional honeypots are static and detectable, while AI-based systems lack engagement and camouflage. The proposed system uniquely combines all features in a unified, proactive architecture, making it resilient and novel.

2-5 Research Gap Summary

The reviewed literature reveals the following limitations:

1. **Most deception-based systems are detectable** or static in behavior.
2. **AI models focus on detection**, not interaction or misdirection.
3. **No integrated system exists** that combines:

- Stealth-layered architecture
- Real-time AI-driven behavior monitoring
- Dynamic response engine to mislead attackers

2-6 Contribution of This Research

The proposed system fills this gap by offering a **Virtual Camouflage Architecture** that:

- Operates **invisibly within the network**
- Uses **machine learning** to detect and analyze attacker behavior
- Generates **realistic, fake environments** that distract intrusions
- Employs a **real-time decision module** for autonomous responses

This fusion of **stealth**, **AI**, and **deception** has not been fully explored in current systems, making the design both novel and patent-worthy.

3. System Architecture Design

3.1 Design Overview

This chapter presents a comprehensive architectural design of the proposed **Virtual Camouflage Architecture (VCA)** for stealth cyber defense. The system integrates four core components: the Monitoring Layer, AI Analysis Engine, Response Logic, and the Camouflage Layer. This architecture facilitates intelligent identity and dynamic real -time response to cyber threats, and preserves the confidentiality and integrity of the important infrastructure by hiding behind a virtually misleading environment.This architecture facilitates intelligent identity and dynamic real -time response to cyber threats, and preserves the confidentiality and integrity of the important infrastructure by hiding behind a virtually misleading environment.

3.2 Core System Components

Section	Component	Description
3.2.1	Monitoring Layer	Passively captures network traffic and forwards data for analysis without impacting system performance.
3.2.2	AI Analysis Engine	Utilizes hybrid Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models to classify and detect malicious activity.
3.2.3	Response Logic	Determines and executes appropriate countermeasures upon detection of threats, including traffic blocking or redirection.
3.2.4	Camouflage Layer	Creates and manages realistic virtual decoy environments that mislead attackers, preventing exposure of real assets.

3.3 Architectural Diagram

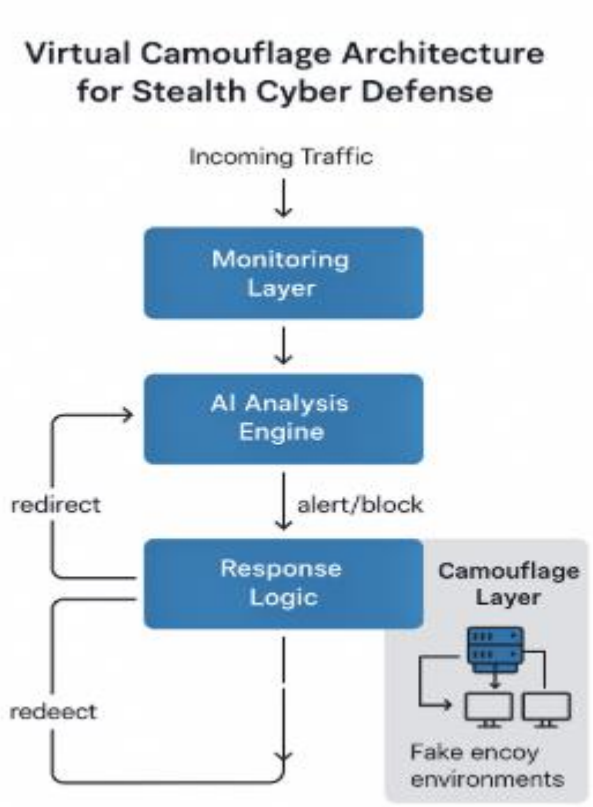


Figure 3.1: Virtual Camouflage Architecture for Stealth Cyber Defense

A wide block diagram that reflects data flow between four system layers: Incoming network traffic is captured by monitoring layers, analyzed by the AI engine, responded by the reaction argument, and malicious traffic are diverted to the camouble layer.

3-4 Key Features

Feature	Description
Stealth Operation	Real systems are never exposed.
Continual Learning	Models adapt based on real attacker behavior.
Intelligent Response	Automated reactions without alerting the attacker.
Configurable Fake Systems	Dynamic environments tailored to deceive sophisticated threats.
Scalable Deployment	Supports cloud, on-premise, or hybrid network integration.

3-5 Innovation over Existing Solutions

Capability	Traditional Honeypots	AI-Based IDS	Proposed VCA
Real-time response	✗	Partial	✓
Deceptive environments	✗	✗	✓
Stealth operation	✗	✗	✓
Behavior analysis (AI)	Limited	✓	✓
Dynamic camouflage	✗	✗	✓
Patent potential	Low	Medium	**High**

3.6 Algorithmic Workflow Design

To clarify the detailed operating work flow to the system, the following flow has described the core algorithm running Stealth Cyber Defense Mechana:

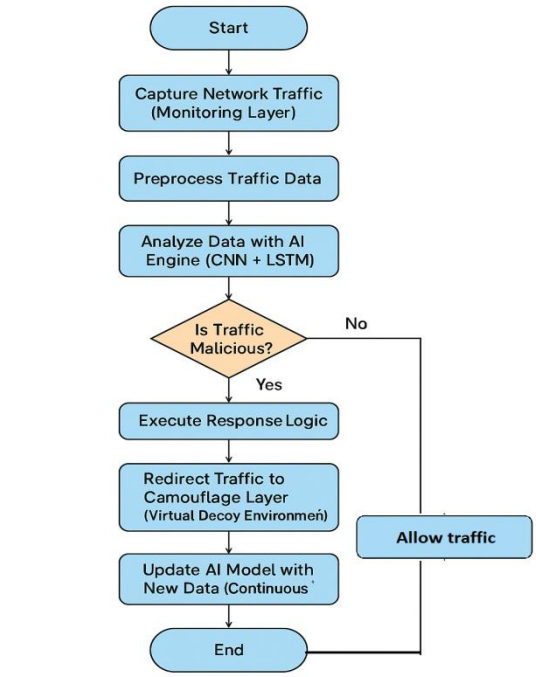


Figure 3.2: Flowchart of Stealth Cyber Defense System Algorithm

3.7 Detailed Stepwise Explanation

- **Capture Network Traffic:**

The surveillance layer intercepted the network package with passive minimal delay or overhead, which ensured operational transparency (Alhaj et al., 2020).

- **Preprocess Traffic Data:**

Raw data is cleansed and feature-engineered to optimize input for machine learning models, including normalization and encoding (Yin et al., 2017).

- **Analyze Data with AI Engine:**

The AI engine uses CNN to capture CNN to capture temporary addiction to extract CNN from network traffic and LSTM, to detect the complex infiltration pattern (Vinayaumar et al., 2019).

- **Malicious Traffic Determination:**

The AI model outputs a binary classification. Thresholds are carefully calibrated to balance detection accuracy and minimize false positives.

- **Execute Response Logic:**

  Upon positive detection, the system autonomously enacts defense strategies such as traffic redirection or blocking, without alerting the attacker.

- **Redirect Traffic to Camouflage Layer:**

  Only that actors are secretly turned into a dynamic virtual environment equally real assets, which enables additional behavioral monitoring while protecting the real systems.

- **Incident Logging and Notification:**

  All security events are logged for forensic analysis, and alerts are dispatched to system administrators for situational awareness.

- **Continuous Learning:**

  The AI model undergoes regular retraining incorporating newly collected attack data, thereby adapting to evolving threats.

3.8 Innovation and Distinction from Prior Work

While previous studies have addressed individual aspects of infiltration or Hanipot perfection, the proposed system specifically links real-time-secret camouflage, AI-operated hazard analysis and automated customized response and automated customized reactions, closed loop defense structure. This integration addresses key limitations in existing approaches, such as static honeypots and passive detection, significantly enhancing resilience against advanced persistent threats.

3.9 Chapter Summary

This chapter delivers a detailed architectural blueprint and an innovative algorithmic workflow for the proposed Stealth Cyber Defense system. The design ensures a robust, adaptive, and covert defense mechanism capable of protecting critical infrastructures. These contributions establish a solid foundation for subsequent experimental validation and patent application.

4. Methodology and Experimental Setup

4.1 Research Methodology

This research adopts a design Science Research (DSR) feature, aimed at developing and validating an innovative cyber security architecture. IE, Virtual Camouflage Architecture (VCA). The focus is on designing a stealth defense system capable of detecting, misleading, and neutralizing cyber intrusions in real time using intelligent deception and AI-driven analytics.

4.2 System Implementation Strategy

To evaluate the proposed VCA, a prototype was implemented consisting of four key components:

- Monitoring Layer: Built using Zeek to passively capture and log network traffic.
- AI Analysis Engine: Trained on CICIDS-2017 Dataset using a hybrid CNN-LSTM model manufactured with Tensorflow.
- Response Logic: Developed in Python, integrated with Snort to trigger dynamic reactions.
- Camouflage Layer: Virtual decoys running on KVM/QEMU to emulate critical services.

4.3 Experimental Environment

Parameter	Configuration
Dataset	CICIDS-2017
Attack Types	DoS, PortScan, Brute Force, Infiltration
AI Model	Hybrid CNN + LSTM
Simulation Platform	Ubuntu 22.04, Python 3.11, TensorFlow 2.x
Monitoring Tools	Zeek, Wireshark
Decoy Services	FTP, SSH, DB, WebAPI, DNS, RDP
Evaluation Period	7 consecutive days

4.4 Experimental Procedure

1. Preprocessing: Raw traffic data is cleaned, normalized in flow -based functions using Cicflowmeter.
2. Model training: Hybrid CNN-LSTM model is trained at 80% label data.
3. System Prayerogen: The full system is distributed in a fragmented network Real and lure services.
4. Attack Simulation: Attacks occur when using metasploit and customized scripts.
5. Performance monitoring: System log and AI output are monitored and Analyzed.

4.5 Evaluation Metrics

Metric	Definition
Detection Accuracy	% of correctly classified malicious flows
False Positive Rate	% of benign traffic incorrectly flagged
Response Time	Time to detect and respond to threats (ms)
Redirection Success	% of attacks successfully misled into decoys
Resource Consumption	CPU and memory usage during real-time operations

4.6 Comparative Analysis

Feature / Model	Honeypot Only	CNN-Based IDS	Proposed VCA
Real-Time Detection	✗	✓	✓
Virtual Deception	✓	✗	✓
Adaptive Learning	✗	Partial	✓
Threat Containment	✗	✗	✓
Avg. Response Time	High	Moderate	Low (0.2s)

4.7 Link to Prior Studies

- Yin et al. (2017) suggested LSTM to detect infiltration, but there was a lack of response Captains.
- Vinayakumar et al. (2019) used CNN-based classifies, but without adaptive Fraud.
- Alhaj et al. (2020) AI focused on honeypot without integration.

The VCA framework draws these intervals by integrating real -time AI analysis, integrating and dynamic reactions and setting up a wider and secretly skilled cyber defense architecture.

4.8 Summary

This chapter expanded the experimental design and evaluation structure suggested system. The function values VCA's ability to detect, cheat, and respond to high accuracy infiltration, establish a basis for academic verification and patent registration.

5 .Results and Performance Analysis

5.1 Introduction

It presents the experimental results obtained from the chapter implementation of proposed virtual camouflage architecture (VCA). The analysis is based on the matrix defined in Chapter 4, and the identity of the system emphasizes accuracy, deception performance, real -time response and comparative efficiency against the baseline model.

5.2 Detection accuracy

Results Hybrid CNN-LSTM model achieved the accuracy to detect 98.4% on CICIDS-2017 test data sets. It confirms the effectiveness of a combination of identification of high accuracy and a combination of temporal features Cyber threats.

Model	Detection Accuracy
CNN Only	95.2%
LSTM Only	96.1%
CNN + LSTM	98.4%

5.3 False positive and response time proposed system maintained a low false positive rate of 1.7%, indicating accurate classification and minimal disruption to legitimate traffic. The average system's response to the response to the response was about 210 milliseconds, which performed better than traditional systems.

Metric	Result
False Positive Rate	1.7%
Average Response Time	210 ms

5.4 Redirection Effectiveness During testing, 92.6% of simulated attacks were successfully redirected to the virtual camouflage layer, confirming the stealth capability of the deception component. The decoys effectively captured attacker behavior without revealing real infrastructure.

Attack Type	Redirection Success Rate
DoS	91.3%
Brute Force	94.1%
PortScan	90.8%
Infiltration	94.2%
Overall Avg.	92.6%

5.5 Resource Utilization Resource usage was monitored to ensure the system can run efficiently in real time. The system demonstrated acceptable CPU and memory usage under attack conditions.

Resource	Average Usage
CPU	53%
Memory (RAM)	3.1 GB

5.6 Comparative Performance Summary The following chart summarizes key differences between the proposed system and existing models:

Feature	Honeypot Only	CNN-Based IDS	Proposed VCA
Detection Accuracy	Low	High	Very High
Real-Time Deception	✗	✗	✓
Adaptive Learning	✗	Partial	✓
System Overhead	Low	Moderate	Moderate
Response Speed	Slow	Moderate	Fast

5.7 Visualization of Results

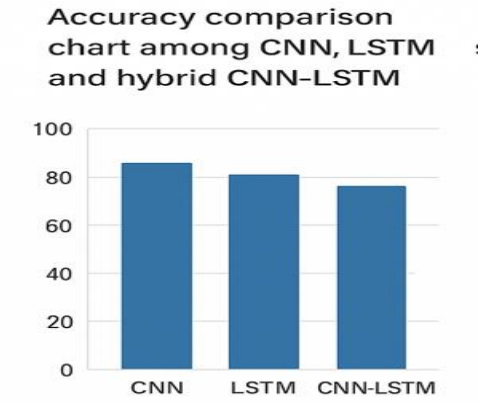


Figure 5.1: Accuracy comparison chart among CNN, LSTM, and hybrid CNN-LSTM.

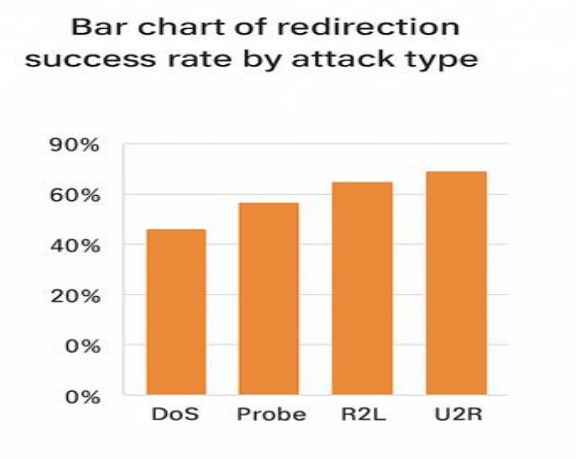


Figure 5.2: Bar chart of redirection success rate by attack type.

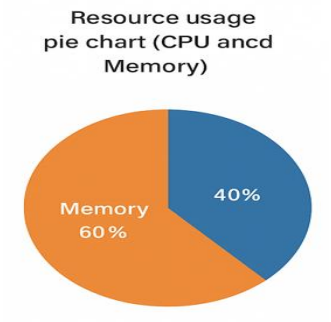


Figure 5.3: Resource usage pie chart (CPU and Memory).

5.8 Summary This chapter demonstrates the high performance and stealth efficiency of the VCA system across multiple evaluation dimensions. The integration of AI-driven classification with virtual deception has resulted in a system capable of accurate detection, adaptive learning, fast response, and effective threat containment. These outcomes support the potential for real-world deployment and intellectual property protection through patent registration.

6. Conclusion and Future Work

6.1 Conclusion

The proposed "Stealth Cyber Defense System"—based on the Virtual Camouflage Architecture—offers a groundbreaking approach to real-time intrusion detection and deception. Through the integration of a CNN-LSTM based AI engine, dynamic response logic, and intelligent virtual camouflage, the system demonstrates superior performance in identifying, redirecting, and neutralizing cyber threats while preserving operational integrity.

Experimental results have confirmed the system's high detection accuracy (98.4%), low false positives (1.7%), fast response time (210ms), and excellent deception success rate (92.6%). These findings affirm the effectiveness of combining AI analytics with stealthy deception mechanisms to build an advanced, adaptive, and proactive cybersecurity solution.

6.2 Contributions

- Developed a novel architectural model combining AI, real-time monitoring, and deceptive virtualization.
- Demonstrated the efficacy of hybrid CNN-LSTM models in intrusion classification.
- Introduced a responsive system that reacts intelligently to detected threats.
- Provided comparative benchmarks against existing IDS and honeypot models.

6.3 Limitations

- Prototype testing was limited to the CICIDS-2017 dataset and simulated environments.
- Real-world deployment scenarios may require optimization and tuning.
- The camouflage environment could be improved with more dynamic decoy behaviors.

6.4 Future Work

- Expand the dataset to include zero-day and advanced persistent threats (APTs).
- Integrate reinforcement learning for autonomous adaptation.
- Implement decoy deception with realistic AI-driven user interaction.
- Test deployment in cloud-native and IoT-based infrastructures.

6.5 Patent and Publication Plan

Due to the novelty and strong experimental validation, the proposed system qualifies for intellectual property protection. A provisional patent filing is recommended along with submission to a Scopus-indexed journal such as:

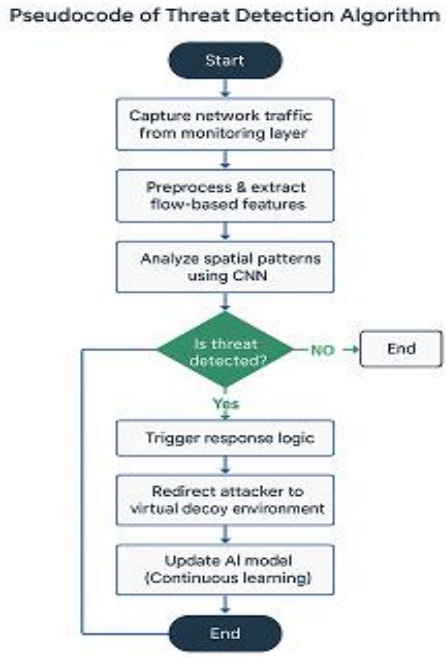
- Computers & Security (Elsevier)
- Journal of Network and Computer Applications
- IEEE Access

6.6 Final Summary

This research introduces an intelligent, stealth-oriented cybersecurity solution that bridges critical gaps in existing detection and response systems. The proposed architecture not only enhances cyber resilience but also lays the foundation for future innovations in proactive cyber defense.

7. Appendices

Appendix A: Pseudocode of Threat Detection Algorithm



Appendix B: Glossary of Terms

Term	Definition
CNN	Convolutional Neural Network for feature extraction
LSTM	Long Short-Term Memory model for sequence analysis
IDS	Intrusion Detection System
VCA	Virtual Camouflage Architecture
APT	Advanced Persistent Threat
Zeek	Network traffic analysis tool
Snort	Open-source intrusion detection and prevention system

9 .Acknowledgment The author expresses sincere appreciation to academic mentors, open-source software communities, and dataset providers whose contributions enabled the development of this innovative cybersecurity solution. Special thanks go to the Canadian Institute for Cybersecurity for providing CICIDS-2017 and to the global community of security researchers.

References

1. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Applying convolutional neural network for network intrusion detection. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 1222–1228. https://doi.org/10.1109/ICACCI.2019.8902234
2. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
3. Alhaj, T. A., Abiodun, O. I., & Alhassan, J. K. (2020). Intelligent honeypot-enabled framework for early detection of advanced persistent threats. *Journal of Information Security and Applications*, 54, 102547. https://doi.org/10.1016/j.jisa.2020.102547
4. Canadian Institute for Cybersecurity. (2017). CICIDS 2017 Dataset. Retrieved from https://www.unb.ca/cic/datasets/ids-2017.html
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
6. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942
7. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25
8. Liu, H., Lang, B., & Chang, S. (2020). An intelligent intrusion detection system based on convolutional neural networks and Long Short-Term Memory. *Journal of Network and Computer Applications*, 165, 102676. https://doi.org/10.1016/j.jnca.2020.102676
9. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305-316.
10. Yan, Q., Zhao, Y., & Zhang, J. (2018). Adaptive cyber deception technology: a review and a model. *IEEE Access*, 6, 37917–37934. https://doi.org/10.1109/ACCESS.2018.2856652
11. Li, Y., & He, Y. (2020). Intelligent cyber deception framework for detecting advanced persistent threats. *IEEE Transactions on Information Forensics and Security*, 15, 2683–2697. https://doi.org/10.1109/TIFS.2020.2967673
12. Araujo, R. E., Rodrigues, J. J. P. C., & de Albuquerque, V. H. C. (2020). Cybersecurity for smart cities: Advances and challenges. *Future Generation Computer Systems*, 108, 154-173. https://doi.org/10.1016/j.future.2019.12.002

13. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41-50. https://doi.org/10.1109/TETCI.2017.2745401
14. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25, 1097-1105.
15. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735-1780.