JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Deception-as-a-Service (CDaaS): A Multi-Layered Approach for Early Threat Detection and Adaptive Defence.

Mr. Meeth Mali [1], Mr. Sufiyan Patel [2]
MSc. CS Cybersecurity Student, Assistant Professor

Nagindas Khandwala College
University of Mumbai, Maharashtra, India

Abstract: The rise of cyber threats has exposed significant limitations in traditional defence mechanisms such as firewalls, antivirus software, and signature-based intrusion detection systems. Due to reactive nature these conventional tools often fail to detect various attacks like insider attacks, and zero-day exploit. Cyber deception has emerged as a proactive defence strategy that aims to mislead attackers by deploying fake assets including honeypots, honeytokens, decoy databases, and simulated services to detect and study the attacker's behaviors in real-time. In this paper, we propose Cyber Deception-as-a-Service (CDaaS): a unified and modular framework designed to integrate multiple deception layers into a single deployable system. CDaaS provides realistic decoys such as honeyfiles, multi-level honeypots, honey-nets, DNS sinkholes, deceptive databases etc. and also an intuitive alert dashboard. The framework is designed for lightweight deployment on individual machines (for small organizations) and is scalable to enterprise-level networks. The system continuously monitors and logs attacker interactions with decoys, generating actionable alerts to Security Operation Centers. It includes adaptive decoy generation techniques that analyses attacker behaviors patterns and automatically deploy new deceptive artifacts to maintain engagement. The design emphasizes ease of use, minimal maintenance, and effective threat detection without impacting the organization's operational environment.

Key challenges addressed include balancing decoy realism with performance overhead, ensuring seamless integration into existing network infrastructures, and providing an intuitive interface for security analysts. The framework avoids over-reliance on external APIs, instead using internal databases SQLite and Python-based automation for core functionality.

This research contributes to the cybersecurity field by presenting a practical, extensible, and enterprise-ready solution for proactive threat detection. It also highlights gaps in current research around holistic deception frameworks, motivating further innovation in adaptive and scalable security architectures.

***Index Terms*:** Cyber Deception-as-a-Service (CDaaS), Honeypots, Honeyfiles, Honeytokens, DNS Sinkhole, Multi-layered security frameworks, Deceptive Database, Threat detection, Intrusion Detection, Artificial Intelligence, Machine Learning.

INTRODUCTION

Over the last few years, cyberattacks have grown at an unprecedented rate. Incidents such as the SolarWinds supply chain attack in 2020, the Colonial Pipeline ransomware attack in 2021, and the Ransomware attack on the All-India Institute of Medical Sciences (AIIMS) in 2022 have revealed that even the most advanced organizations and infrastructures are vulnerable. Traditional defence mechanisms, such as firewalls, intrusion detection systems, and antivirus software, are primarily reactive in nature. They detect and respond to threats only after malicious activity has begun, often leaving defenders with very little time to act.

Advanced attackers use zero-day exploits, insider threats, and lateral movement techniques that easily bypass standard security measures. These gaps highlight the need for proactive defenses strategies that do not just react but proactively engage and misdirect malicious actors.

Cyber deception has emerged as an effective strategy in this context. By creating fake assets-such as honeypots, honeytokens, and decoy files-organizations can mislead attackers, waste their resources, and detect intrusions at an early stage. Unlike traditional tools, deception offers a low false-positive rate because only attackers interact with the decoys, not legitimate users.

Despite the availability of numerous cyber deception solutions, the market is extremely fragmented. Few solutions provide a complete, scalable, all-in-one platform; the majority are specialized, concentrating on a specific function, such as honeypots or honeynets. Due to the substantial barrier to entry created by this lack of integration, it is difficult for individual users and smaller companies to successfully apply deception tactics. We suggest Cyber Deception-as-a-Service, a multi-layered deception platform, to close this gap. Honeyfiles, honey-nets, DNS sinkholes, deceptive databases, advanced imitating, and alerting dashboards are just a few of the tools that CDaaS combines into a unified architecture. In contrast to conventional corporate-only deception systems, CDaaS is made to be both scalable for enterprise deployments and portable enough to run on a laptop.

LITERATURE REVIEW

Overview of Related Work

1. A comprehensive survey on cyber deception techniques to improve honeypot performance. (2024) [1]

This paper presents a detailed survey of cyber deception techniques aimed at improving the stealth and effectiveness of honeypots and honeynets. It categorizes deception assets by interaction level, deployment method, and security purpose. Additionally, it proposes a mathematical model for evaluating honeynet configurations and simulating attacker engagement.

Relevance: It directly supports our CDaaS framework, which integrates multi-layered deception assets like honeypots, honeyfiles, DNS sinkholes, and deceptive databases into one system.

2. Deception for Cyber Defence: Challenges and Opportunities. (2022) [2]

This study explores the development of scalable, realistic cyber deception services designed to proactively detect and disrupt attackers. The paper proposes using ML to dynamically generate deceptive artifacts such as fake documents, websites, email threads, and databases that mimic real organizational assets. These deception services are intended to lure attackers, trigger alerts, and collect intelligence on adversary behaviour.

Relevance: This work introduces automation and realism into deception services, showing how AI can be used to create adaptive decoys. It directly influences our CDaaS proposal by emphasizing the need for scalable, machine-learning-driven deception that reduces attacker dwell time and enhances actionable threat intelligence.

3. Cyber Deception for Computer and Network Security: Survey and Challenges (2020) [3]

This paper provides a structured overview of cyber deception techniques used to enhance security across computer systems and networks. It categorizes deception strategies such as honeypots, honeytokens, fake services, and decoy environments and explains how they are employed to mislead attackers, gather intelligence, and delay or prevent breaches. The survey also highlights the evolution of deception from static traps to dynamic, adaptive systems, and discusses key challenges like realism, scalability, attacker profiling, and integration with existing security infrastructure.

Relevance: This paper is essential for cybersecurity professionals, researchers, and system architects aiming to implement deception as a proactive defence layer. It not only consolidates current practices but also identifies gaps and future directions, making it a valuable guide for designing resilient, adaptive security systems that go beyond traditional detection.

4. Creating Personally Identifiable Honeytokens (2008) [4]

This paper introduces a method for generating realistic fake personal data, such as names, addresses, phone numbers, and social security numbers, to serve as digital honeytokens. These synthetic records are designed to appear valuable and authentic to attackers, helping organizations detect unauthorized access or data misuse. A key use case is embedding these honeytokens in sensitive databases like hospital records to trigger alerts when accessed, thereby identifying potential breaches.

Relevance: This approach is highly beneficial for CDaaS. By embedding believable decoy data into systems, organizations gain an early warning mechanism against insider threats, data leaks, and identity theft without compromising real user information.

5. Honeypots and Honeytokens in Active Defence (2024) [5]

The paper explores how deceptive technologies like honeypots and honeytokens can be strategically deployed to strengthen active cyber defence. It categorizes active defence tactics into detection, deterrence, and attribution, showing how honeypots lure attackers into controlled environments for behavior analysis.

Relevance: This paper offers practical insights into how diverse deception assets can be orchestrated to enhance real-time threat detection and attacker profiling.

6. A Mathematical Model for Analysing Honeynets and Their Cyber Deception Techniques (2024) [6]

This presents a comprehensive framework for evaluating the effectiveness of honeynet configurations using formal modelling and simulation. It introduces a general honeynet model that incorporates network parameters, attacker strategies, costs, and benefits, allowing researchers to compare various deception techniques such as optimizing the number of honeypots, diversifying honeypot types, strategic placement, dynamic behaviour, and network topology shaping.

7. Leveraging Computational Intelligence Techniques for Defensive Deception (2022) [7]

This paper reviews how computational intelligence especially machine learning, fuzzy logic, and evolutionary algorithms can be applied to enhance cyber deception strategies. It explores recent advances in automating the generation of deceptive artifacts like honey files, fake credentials, and decoy systems, making them more adaptive and context aware. They also identify open problems such as realism, adversarial learning, and scalability, and propose future directions like integrating deception with autonomous cyber defence and cognitive modelling.

8. SPADE: Enhancing Adaptive Cyber Deception Strategies with Generative AI and Structured Prompt Engineering (2025) [8]

The paper introduces a framework that uses generative AI models like GPT-2 and GPT-3 combined with structured prompt engineering to automate and personalize cyber deception techniques. SPADE dynamically generates realistic honeyfiles, fake credentials, and decoy communications tailored to specific threat scenarios, making deception more adaptive and scalable. The framework is designed to allow integration with existing security systems and enabling real-time deployment of deception assets.

9. Deception Techniques in Computer Security: A Research Perspective (2018) [9]

The paper provides a conceptual and strategic overview of how deception can be used as a proactive defence mechanism in cybersecurity. It outlines various deception methods such as honeypots, honeytokens, fake services, and misleading system responses and examines their roles in detecting, delaying, and diverting attackers. The authors emphasize the psychological and behavioural dimensions of deception, arguing that effective deployment requires understanding attacker decision-making and tailoring deceptive.

10. A multi-layered security architecture for modelling complex systems (2008) [10]

This paper introduces a simplified multilayer security model semantic, logical, and physical that enables holistic analysis of complex systems by capturing human, organizational, and technical interactions. Unlike traditional models, it supports reasoning about system-wide dependencies and vulnerabilities, making it suitable for critical infrastructure like electricity grids.

Relevance: This architecture provides a foundational framework to structure multilayer deception assets across layers. By aligning deceptive elements with semantic (user behaviour), logical (network activity), and physical (device-level traps) layers, your CDaaS can deliver deeper, context-aware protection and adaptive threat response.

11. Hybrid cyber defense strategies using Honey-X: A survey (2023) [11]

The survey on hybrid cyber defense strategies using Honey-X explores how deception technologies like honeypots, honeytokens, and honeyfiles can be integrated with traditional security systems and AI-based tools to create more adaptive and proactive defenses. By luring attackers into fake environments, these strategies help detect threats early, gather intelligence, and reduce false positives.

Relevance: This approach is especially relevant today as cyber threats grow more sophisticated, making layered and intelligent defense mechanisms essential for protecting sensitive systems and data.

12. Cyber Deception: State of the art, Trends, and Open challenges (2024) [12]

This survey presents a comprehensive review of Cyber Deception (CYDEC)—a proactive defense strategy that uses decoys, traps, and fake assets to mislead attackers and gather intelligence. The paper analyzes core components of deception systems, proposes a unified taxonomy, and compares existing solutions with and without AI integration. It also highlights current trends like AI-enhanced deception, adaptive decoy systems, and deception-as-a-service, while identifying open challenges such as scalability, realism, attacker-aware evasion, and ethical concerns.

Relevance: This paper directly relevant to your CDaaS system as it outlines the limitations of current deception tools—such as fragmentation, lack of realism, and poor scalability which your framework addresses through a unified, multi-layered approach. CDaaS integrates diverse deception assets like honeypots, honeyfiles, and DNS sinkholes, while also incorporating AI/ML for adaptive decoy generation and attacker profiling, aligning perfectly with the paper's call for intelligent, scalable, and proactive cyber defense solutions.

RELATED WORK AND PROBLEM STATEMENT

Analysis of Existing Deception Systems

Current cyber deception strategies can be grouped into standalone honeypots, honeytokens, and honeynets, each with distinct limitations. Standalone honeypots like Honeyd, Dionaea, and Kippo are effective for basic threat capture but rely on static configurations and are easily fingerprinted by skilled adversaries.[5] Honeytokens and canary-tokens act as passive tripwires for data access but lack network-level coverage against lateral movement or advanced reconnaissance.[4] Honeynets and honey walls simulate entire networks for in-depth adversary study, yet they demand complex deployment, heavy resources, and expert management, restricting them to specialized labs.[6]

Commercial deception platforms (e.g., Illusive Networks, TrapX, Attivo Networks) offer enterprise-grade dashboards, analytics, and adaptive decoys but are cost-prohibitive, proprietary, and opaque to academic or SME users.[2] Research prototypes covering adaptive honeypots, deceptive databases, and DNS sinkholes provide strong theoretical foundations but remain limited to small-scale testbeds without practical, scalable integration.[7]

Research Gaps and Problem Statement

Despite numerous tools and studies, critical gaps persist:

- Fragmentation: Most solutions focus on a single technique (e.g., honeypots or honeytokens) without a unified, multi-layered framework.[1]
- Static and Unrealistic Decoys: Deception assets often remain static, allowing attackers to detect, fingerprint, and bypass them with ease.[9]
- Lack of Lightweight Deployment: Existing frameworks target large-scale enterprise environments, leaving researchers and SMEs with no accessible, low-resource options.[5]
- Limited Adaptive Capabilities: Few systems dynamically generate or adapt decoy assets in response to attacker behaviour using AI/ML.[8]
- Lack of Centralized Visibility: Security teams must juggle multiple disparate tools, lacking a single dashboard to monitor alerts, analyses behaviour, and coordinate deception cohesively.[2]
- Evaluation Challenges: Standardized metrics and comprehensive simulation frameworks for comparing deception assets (e.g., honeypots vs. DNS sinkholes) are missing.[6]

Research Objective

There is a clear need for a unified, multi-layered, and adaptive deception framework Cyber Deception-as-a-Service that integrates diverse deception assets, supports lightweight deployment, provides centralized monitoring, and evolves with emerging threats.

Theoretical Background

This research builds on core concepts from cyber deception and security architecture:

- Defence-in-Depth: Layered security controls to ensure overlapping protection even if one layer is breached.[11]
- Deception Taxonomy: Categorizing assets by interaction level (low to high), deployment method, and security purpose to guide multi-layered design. [9]

PROPOSED SYSTEM

1. Host-Level Deception Layer

This layer deploys decoys directly onto endpoints and servers to detect illicit access and internal reconnaissance. It comprises four primary assets:

- Honeypots: These are decoy systems and services designed to lure attackers by mimicking real applications (e.g., SSH, HTTP). The framework supports varying levels of interaction:
  - Low-interaction: honeypots emulate simple service banners to detect mass scans and brute-force attempts.
  - Medium-interaction: honeypots simulate partial functionality (like an SSH terminal) to log commands.
  - High-interaction: honeypots deploy full operating systems within controlled VMs or containers to safely study detailed attacker behaviour.

These are deployed as lightweight containers by the CDaaS agent, which automatically rotates them to avoid fingerprinting.

- Honeytokens and Honeyfiles: These components function as digital tripwires.

- Honeytokens are fake but realistic data, such as credentials, API keys, or database entries, planted in configuration files, databases, or Active Directory.
- Honeyfiles are decoy documents (e.g., "SalaryDetails2025.xlsx," PDFs) embedded with tracking mechanisms like canary tokens or beaconing URLs.

- Deceptive Databases: The framework can deploy containerized decoy databases mimicking MySQL populated with synthetic yet believable records. These decoys divert attackers from production databases, allowing the system to safely log all queries and analyses the attacker's objectives.

2. Network-Level Deception Layer

This layer creates a deceptive network topology to mislead attackers attempting lateral movement and to prevent external command-and-control (C2) communication.

- Honey-nets: The system generates a Honey-net, an interconnected network of the previously mentioned honeypots that simulates a real IT environment.
- DNS Sinkholes and DMZ Simulation: To neutralize malware, the agent deploys DNS Sinkholes. These are fake DNS servers that capture and redirect malicious queries, preventing malware from contacting its C2 server while logging the attempted communication.

3. Advanced Mimicking (AI/ML-Enhanced Realism)

To maintain believability and evade detection by sophisticated attackers, the framework integrates AI and ML for adaptive deception. This layer uses Generative AI, as defined by the SPADE framework [8], to produce realistic decoy credentials, log files, and communication artifacts. It employs Computational Intelligence, such as fuzzy logic [7], to automatically adjust decoy behaviors based on attacker interactions.

4. Alerting, Monitoring, and Threat Profiling

All attacker interactions across the deception landscape are captured in a centralized logging system (utilizing SQLite/Firebase). When any deception asset is accessed, the system generates real-time alerts delivered to defenders via email, Slack, or the central dashboard.

5. Defender's Dashboard (Management Console)

All components are managed via a centralized Defender's Dashboard. Developed using a React.js framework, the console provides clear visualization modules showing active decoy statuses, a timeline of attacker interaction, and network heatmaps illustrating attacker activity. The dashboard provides secure role-based access for SOC analysts, administrators, and threat researchers.

6. Scalability and Deployment Mechanism

The CDaaS architecture ensures scalability through a lightweight, agent-based deployment model. A single agent running on an endpoint or server manages the local provisioning of honeypots, honeyfiles, and honeytokens

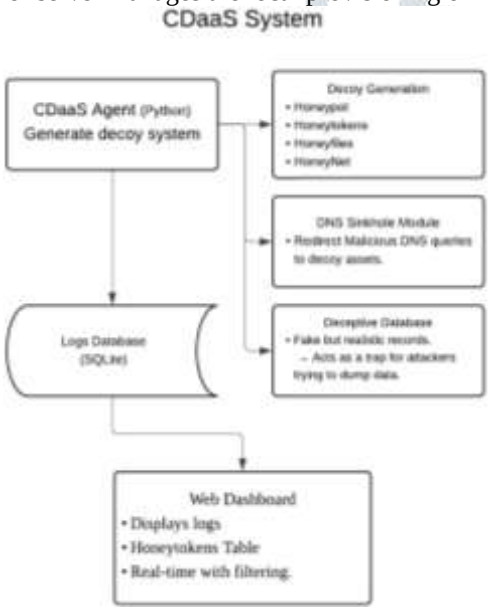

Fig. 1 CDaaS System

METHODOLOGY

Research Design

This research follows a prototyping-based experimental design. The goal is to develop a working system CDaaS in two phases:

1. Phase 1 (Mini Project): Develop a lightweight CDaaS prototype with core features (honeyfiles, honeytokens, basic honeypot, and a dashboard) as shown in *Fig. 1 CDaaS System*.
2. Phase 2 (Major Project): Expand the prototype into a full multi-layered adaptive framework integrating advanced honeynets, DNS sinkholes, deceptive databases, AI/ML modules, and centralized event monitoring.

The approach is iterative and incremental, enabling continuous testing and improvement.

Data Collection Methods

1. Synthetic Data Generation: Create fake decoy assets (honeyfiles, honeytokens, honeypots). Deploy decoy databases with synthetic records.

2. Simulated Attacker Interactions: Use tools like Nmap, and Kali Linux to simulate scanning, exploitation, and lateral movement. Open honeyfiles manually or via automated scripts.
3. Event Logging: The agent logs every interaction (e.g., file access, login attempts, DNS queries) into SQLite/Firebase. Metadata (timestamp, IP address, decoy type) is recorded.

Analysis Techniques

1. Real-Time Monitoring: Logs collected by the dashboard are visualized in a structured format (timeline, IP mapping, TTP correlation).
2. Forensic Analysis: Analyses attacker behaviour patterns from log data to identify techniques used.
3. Performance Testing: Measure CPU/RAM usage, number of decoys deployed, and response time of the system. Test scalability by deploying multiple agents reporting to one dashboard.

Justification for the Chosen Approach

1. Unified Multi-Layer Design: Unlike existing fragmented solutions, this approach integrates honeypots, honeyfiles, honeytokens, DNS sinkholes, and deceptive databases into one lightweight, scalable system.
2. Lightweight & Scalable: Designed to work on both single laptops and enterprise networks, making it accessible for SMEs, individuals, and large organizations.
3. AI/ML Integration: Future-ready approach to adapt decoys based on attacker behavior, providing more realistic and dynamic deception compared to static traps.
4. Centralized Visibility: A single dashboard reduces complexity for security teams by providing a unified view of all deception activity and actionable alerts.

RESULTS AND DISCUSSION

The proposed Cyber Deception-as-a-Service (CDaaS) framework is expected to deliver the following results:

1. Early Detection of Attacks: Decoys such as honeyfiles, honeytokens, and honeypots will detect attacker interactions in the earliest phase of an attack, providing early warnings before actual systems are compromised.
2. Low False Positives: Unlike traditional IDS/IPS systems, decoys are only triggered by malicious behavior, drastically reducing false positive alerts.
3. Real-Time Alerts and Visualization: Attack interactions will be instantly logged and displayed in a web-based dashboard with attacker metadata (IP address, geolocation, timestamp, type of asset triggered).
4. Detailed Attacker Behavior Profiling: The system will log detailed attacker interaction data (e.g., commands used in honeypots, accessed honeyfiles), enabling forensic analysis of attacker techniques and intent.
5. Scalability and Lightweight Performance: The system will run smoothly on a single laptop (for prototype) and scale to multiple agents reporting to a central dashboard for enterprise setups, demonstrating minimal resource usage (CPU, RAM).
6. Adaptive Decoy Update (Future Work): Future AI/ML modules are expected to dynamically generate new decoys and adapt existing ones based on observed attacker behavior, improving long-term resilience and engagement.
7. Comprehensive Coverage of Attack Vectors: The multi-layered architecture ensures wide coverage of attack vectors (file-based attacks, network-based scanning, DNS manipulation, database probing), improving the overall defence posture.
8. Proof of Concept Validation: Through controlled attacker simulations (manual attacks, automated tools like Nmap or Metasploit), the prototype will validate that decoys effectively engage attackers and trigger alerts as intended.

FUTURE DIRECTIONS

Suggestions for Further Research

1. AI-Driven Adaptive Deception: Research can focus on advanced machine learning techniques to dynamically generate and update deception artifacts (e.g., honeyfiles, honeytokens, honeypots) based on attacker behaviour patterns. This allows the system to automatically evolve over time, making decoys harder to detect.[8]
2. Deceptive Database Generation: Future work can investigate automated methods for generating realistic, fake database records that are context-aware, interlinked, and harder to differentiate from real data, increasing the likelihood of attacker interaction.[12]
3. Advanced Ransomware Detection via Deception: Research can develop modules that simulate vulnerable file systems to detect ransomware behaviour by monitoring suspicious file encryption patterns in honeyfiles or decoy directories.

Emerging Trends in the Field

1. Integration with Threat Intelligence Platforms: Deception systems will increasingly integrate with TIPs to automatically ingest and respond to real-time threat data, improving decoy relevance and reducing attacker dwell time.
2. Behavioral Analytics & Attacker Profiling: Next-generation systems are moving toward behaviour-based analysis to profile attackers dynamically, mapping their tools and tactics to frameworks like MITRE ATT&CK, enabling better response strategies.
3. IoT and Cloud-Native Deception: Deceptive techniques are expanding into IoT environments and cloud infrastructures, where fake sensors, decoy containers, and cloud-specific APIs will play a critical role in defending increasingly distributed systems.[11]

CONCLUSION

In today's evolving cybersecurity landscape, traditional defence mechanisms such as firewalls and antivirus systems are no longer sufficient to counter advanced and persistent cyber threats. Attackers continuously bypass perimeter defences using sophisticated tactics like zero-day exploits, insider threats, and lateral movement techniques. This research presents Cyber Deception-as-a-Service (CDaaS), a multi-layered and unified deception framework designed to proactively mislead attackers, collect actionable intelligence, and reduce attacker dwell time. Unlike existing fragmented solutions, CDaaS integrates diverse deception assets, including

honeypots, honeytokens, honeyfiles, deceptive databases, DNS sinkholes, and advanced mimicking powered by AI/ML techniques. The system is designed for lightweight deployment, scalable from individual laptops to enterprise networks, making it accessible for both SMEs and large organizations. The centralized dashboard provides defenders with real-time visibility of attacker activity, enabling rapid response and deep forensic analysis.

Furthermore, the future direction of CDaaS focuses on integrating adaptive AI models to automate decoy generation and attacker profiling, ensuring the system evolves in line with emerging threats. In conclusion, CDaaS contributes to the field of proactive cyber defence by filling the gap between fragmented deception tools and enterprise-level complexity, providing a comprehensive, scalable, and intelligent solution for modern cybersecurity challenges.

BIBLIOGRAPHY

1. Amir J., Forough J., Tarik T., Mohammad S., Chafika B. (2024*). A comprehensive survey on cyber deception techniques to improve honeypot performance*. *ScienceDirect*.
2. David L, Surya N, Kristen M, Cody J... (2022). *Deception for Cyber Defence: Challenges and Opportunities* ResearchGate.
3. Zhuo Lu, Cliff Wang, Shangqing (2020). *Cyber Deception for Computer and Network Security: Survey and Challenges.* arXiv.
4. Jonathan White (2024) *Creating Personally Identifiable Honeytokens. ResearchGate.*
5. *Amir J,* Forough J., Tarik T., Mohammad S., Chafika B. *(2024). A Mathematical Model for Analyzing Honeynets and Their Cyber Deception Techniques. IEEE.*
6. *Pilla V, Shriniket D, Amogh G, Utkarsh C, Kathiravan S, Jung T (2022). Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open. Problems and Future Directions. Semanticscholar.*
7. Shihab A, A B M, Md Morshed, Md Sajidul (2025). *SPADE: Enhancing Adaptive Cyber Deception Strategies with Generative AI and Structured Prompt Engineering*. *arXiv*.
8. Xiao Han, Nizar Kheir, Davide B (2018*). Deception Techniques in Computer Security: A Research Perspective.* ACM
9. Blackwell, C. (2008). *A multi-layered security architecture for modelling complex systems.* ACM Digital Library.
10. Baghirov, E. (2024). *A comprehensive investigation into robust malware detection with explainable AI.* Science Direct.
11. Xingsheng Qin, Frank Jiang, Mingcan Cen, Robin Doss (2023). *Hybrid cyber defense strategies using Honey-X: A survey.* ScienceDirect
12. Pedro Beltr´ an L´ opez, Manuel Gil P´ erez, Pantaleone Nespoli Cyber *(2024). Deception: State of the art, Trends, and Open challenges. arXiv*.

Project: https://www.github.com/Masontysom/CDaaS