



Self-Adapting Enterprise Threat Intelligence tool with Automated Deception and Real-Time Cyber Defense

Deepkumar Wagh,

M.Tech Artificial Intelligence-Data Science, National Forensic sciences university, Goa

Dr. Panem Charanarur,

Assistant Professor, National Forensic Sciences university, Goa

Abstract

Cyber threats have increased in sophistication and complexity, and traditional perimeter security defenses are failing to stop advanced persistent threats, zero-day attacks, and targeted intrusion attacks. The project aims to design, implement, and test an AI-powered Cyber Deception System. It is a proactive cybersecurity system that includes honeypot emulation, threat classification with machine learning, unsupervised anomaly detection and reinforcement learning based deception strategy adaptation in a single deployment that requires limited resources. The system will deploy 4 honeypot services: SSH, HTTP, FTP, Telnet. These services monitor the attacker's actions without revealing any production resources. Each source IP is given a behavioural fingerprint and passed on to a Random Forest classifier which classifies attack traffic into five categories: brute-force, reconnaissance, exploitation, lateral movement, and data exfiltration. It is accompanied by another anomaly detector called Isolation Forest for the detection of unknown attack patterns (zero-day and out-of-distribution) that are not present in the training data of the classifier. A composite threat score will add the confidence levels of the classifiers, the magnitude of the anomaly, how often it occurs in the behaviour and the recurrence signals for each attacker IP and can help prioritise responses according to the risk. A Q-Learning reinforcement learning agent selects a strategy from a catalogue of seven deception strategies. The agent learns the strategies that most help the attacker to spend more time during simulated engagement episodes. It shows consistent improvement in rewards as training continues.

Keywords: Cyber Deception, Honeypot, Machine Learning, Random Forest, Isolation Forest, Reinforcement Learning, Q-Learning.

1. INTRODUCTION

1.1 Overview

Widespread networked systems and infrastructure, such as those connected to the Internet, have made cybersecurity one of the most critical issues of our time. Legacy security measures, such as firewalls, IDS, and signature-based antivirus solutions, apply the principle of exclusion: they intimidate the competitors. However, sophisticated attackers have effectively gotten clever and managed to outsmart perimeter defenses time and time again. defenses do not work against APTs and zero-day attacks. attacks. In this project we present an AI-Powered Cyber Deception System that is designed to Empower the defender to change their stance from reactive to proactive with a cyber security framework. Exclude in active misdirection. It is based on an intelligent honeypot network, which consists of fake services. In the past, they were used to make the machine attract and entrap attackers, now it is used to machine learning (ML) and reinforcement learning (RL). Qualify threat, attacker behaviour, and self-adapt attack techniques.

1.2 Motivation

Traditional IDSs are based on known attack signatures. Such systems fail often. They produce tons of annoying non-sense, which makes analysts' lives miserable. They don't only make noise, they are also oblivious to new dangers. These unnoticed signals permeate hardened targets vulnerable. Cyber deception addresses these gaps by creating dummy infrastructure for attackers to breach. Certainly, it is a controlled environment that safely watches techniques through the entire process of testing executed within a sandbox segregated from the production data, eliminating all risk. In fact, all the interactions you see logged here begin with a threat actor. There are literally 0 false positive when it comes to honeypots, because a bot can only touch a honeypot and no legitimate person would ever touch a honeypot. All behavioral telemetry collected during these engagements helps to construct robust training data for adaptive machine learning models. The use of reinforcement learning introduces an adaptive self-improving aspect. Your system learns which strategies work best to confuse or fingerprint certain intruders, to slow their movement toward your most valuable assets. It works. The motivation for building this is the abysmal lack of lightweight open-source platforms that implement not only a honey pot orchestration layer but also an ML threat classification and RL agent adapt strategy implementation. Currently, everything I can find seems either bloated or not yet ready for production use at the typical level. This project addresses this gap with an edge-ready solution that is made for small-to-medium enterprises and academic researchers. If

teams are going to do high-fidelity security, they should be able to deploy a single package without the normal administrative overhead. Every single deployment then continues to aim for efficiency.

1.3 Objectives

- To develop and implement a distributed honeypot network emulating the SSH, HTTP, FTP, and Telnet services, recording high-fidelity attacker interactions.
- Create a 19-feature behavioral fingerprint from the in-the-wild traffic that you have observed, and use it with Random Forest to classify types of attack (brute-force, reconnaissance, exploitation, lateral movement, data exfiltration).
- To implement an Isolation Forest anomaly detector recognizing zero-day and new attack patterns going beyond the supervised classification boundary.
- To develop a Q-Learning reinforcement learning agent that is capable of maximizing the time spent by attackers in the honeypot environment while searching for optimal deception strategies per attacker type.
- You will have a chance to implement a composite threat scoring pipeline creating one 0–1 whisker in human-readable risk metric from classifier confidence, anomaly scores, behavioral signals and recurrence factors.

Here, we want to create one platform for cyber deception that is enhanced with AI. These systems are required to demonstrate the effectiveness of honeypot threat capture, supervised behavioural classification, A combination of unsupervised anomaly detection and reinforcement learning based deception adaptation. in a single efficient architecture. When dealt with, responses fragment, resulting in isolated segments of performance being created on each pipeline. In fact, to overcome these systemic failures, our study makes three main contributions. Let us introduce Developed a Q learning deceptive optimizer to solve the strategy selection problem as a Markov Decision Process A (MDP) that acquires the policy by interacting with the feedback received during real attacks. It just works. MoSo's Predictive Signature with Multi-Dimensional Behavioural Fingerprints. The roots of MoSo follows the trend of being predictive signature and stateful behaviour model based. The model is an extension of the dimensional behavioural fingerprinting that captures temporal, voluminal and protocol-diversity and captures the diversity of behavioural typologies. entropy of multiple signals of traffic flows from a traffic source IP entity fused together into a single feature. layer.

Finally, a composite threat scoring approach that fuses a classifier confidence and anomaly value and behaviour recurrence into a unified actionable risk score. These components Give a repeatable defence structure to be used in an adaptive manner in a resource limited set of deployed environments.

RESULTS AND DISCUSSIONS

Attack Simulation and Classification Performance The attack simulation and classification performance has been enhanced. Attack simulation and classification performance improved. The classifier was tested on 4 of the main attack vectors: SSH brute-force, HTTP reconnaissance, FTP credential sprays, and Telnet injections. The system proved to be robust in identifying per class, especially for aggressive brute-force patterns.

Table 1 Classification Performance and Strategy Specialization

Attack Category	Precision	Recall	F1-Score	Learned Strategy Optimization
SSH Brute-Force	0.94	0.91	0.92	Slow Response (Strategy 1)
HTTP Reconnaissance	0.89	0.93	0.91	Redirect Maze (Strategy 5)
FTP Credential Spray	0.96	0.92	0.94	Credential Replay (Strategy 3)
Telnet Injection	0.87	0.90	0.88	Fake Data Injection (Strategy 2)

The Random Forest classifier performed with a good precision (0.88) in the case of FTP credential spraying, furthermore, it was able to identify random noise and structured attacks. the Isolation Forest had a recall of 0.85 for zero-day anomalies to guarantee that novel tactics were isolated. even if there are no labels, high-risk is identified.

Reinforcement Learning Convergence

The Q-Learning agent was trained for more than 1000 simulated episodes to maximize the

dwell time of the attacker. At least twice the original baseline. This improvement verifies that the agent was successful in achieving this improvement. transitions between random selection of strategy and a "threat-aware" policy, favouring stalling Tactics to fight automated bots and high fidelity deception to fend off reconnaissance

CONCLUSION

In this project, we have designed end-to-end AI-Powered Cyber Deception System and then implemented and validated the prototype system. It combines four complementary key technologies-multi-protocol honeypot emulation, supervised behavioural classification, unsupervised anomaly detection and reinforcement learning-driven deception strategy optimization. They all get wrapped into a single Python application (which is memory-efficient). This it is a good fit for resource constrained environments such as low-power business networks, university laboratories, and entry level IoT gateway defenders. The automated test suite tests all key modules and passes transitions between the modules are secure and failproof entirely confirming the accuracy of the program and guaranteeing that along the way across the various modules there are safe and secure transitions with no scope for errors. integration is intact. Not only is it useful, this paper provides three insights into lightweight Optimizing strategy selection through the online deceptive way of honeypot literature - Q-Learning. attacker type, a multi-dimensional behavioural fingerprint based on a compact unified Representation of temporal, volumetric, protocol-diversity and entropy patterns and finally Detects, and social index measures, is employed to calculate the composite threat score. A composite threat scoring mechanism is used that combines the outputs from a supervised classifier confidence, anomaly detection, and social indexes. To give a risk score in an actionable unit, size and behaviour avg recurrent interval are provided. These set of contributions, in total, define a repeatable playbook for responsive and agile cyber defence.

References

- [1]. AI Deception: Risks, Dynamics, and Controls. (2025). arXiv:2511.22619.
- [2]. Jain, A., Aiyappa, L., MJ, M., & A, U. A. (2025). Real Time Honeypot with Behavioral Fingerprinting of Attackers Using an ML Model. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 12(11).
- [3]. Next-Generation Smart Grid Cybersecurity: A Systematic Review of OT Cyber Threats, AI-Driven Defense, and Cyber Deception Techniques. (2025). IEEE Access.
- [4]. Sharma, et al. (2021). The Role of Reinforcement Learning in Adaptive Cyber Defense Mechanisms. *All Multidisciplinary Journal*.
- [5]. AI-powered cyber incident response system for cloud platforms. (2025). IEEE/arXiv.
- [6]. Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. (2025). PMC11990953.
- [7]. Pujari, M., Pakina, A. K., & Sharma, A. (2025). View of AI governance via explainable reinforcement learning (XRL) for adaptive cyber deception in zero-trust networks. *Journal of Information Systems Engineering & Management*, 10, Article 8308.
- [8]. Alhajahmad, B. (2026). Learning from the Normal: Anomaly-Based Intrusion Detection Using Isolation Forest, LOF, and One-Class SVM. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 30(1), 29-42.
- [9]. FireRL: Adaptive Firewall Strategy Generation and Optimization Based on Reinforcement Learning. (2025). *Informatica*, 49.
- [10]. Web Traffic Anomaly Detection Using Isolation Forest. (2024). MDPI Digital.
- [11]. Honeypsy: A Honeypot Design to Understand Hacker Expertise and Personality. (2025).
- [12]. ResearchGate.
- [13]. AlQahtan, N., AlOlayan, A., AlAjaji, A., & Almaslukh, A. (2025). HoneyLite: A Lightweight Honeypot Security Solution for SMEs. *Sensors*, 25(16), 5207.
- [14]. A Review of Honeypots: Fingerprinting Techniques, Detection, and Evasion Mechanisms. (2026). *Future Internet*.
- [15]. Kyriakou, S. (2025). Exploring the fingerprintability of honeypot systems and prevent detection. B.Sc. Thesis, Cyprus University of Technology.
- [16]. TrafficPrint: A Pattern Extraction Framework to Enable Adaptable Analysis of Diverse Honeypot Payloads. (2025). PMC12788154.
- [17]. Lawal, S., & Garba, M. (2026). Data-Driven Threat Scoring System for Dynamic Cyber Risk Management. ResearchGate.
- [18]. Adaptive Firewall Strategy Generation and Optimization Based on Reinforcement Learning. (2025). *Informatica*, 49.
- [19]. LLM-powered honeypots: Taxonomy and Roadmap. (2025). arXiv:2510.25939.

- [20]. Adaptive Honeypot Systems via RAG: Enhancing Threat Intelligence with Generative AI. (2025). International Journal of Innovative Engineering Applications, 9(2), 175-183.
- [21]. Holoscope: A Lightweight, Cloud-Native Platform for Distributed Sensors. (2025). arXiv:2512.19842.
- [22]. Data-Driven Threat Scoring System for Dynamic Cyber Risk Management. (2026).
- [23]. Robust IoT security using isolation forest and one class SVM algorithms. (2025).