NetSentinel: A Multi-Tier, AI-Driven DNS Filtering System with Explainable Threat Reporting

1st Ameen Siddiqui
NetSentinels - CyberGuardians Track
Abu Dhabi University
Abu Dhabi, UAE
siddiqui.ameen@outlook.com

2nd Mohamed Idres
NetSentinels - CyberGuardians Track
Abu Dhabi University
Abu Dhabi, UAE
mohamedidres7@outlook.com

3rd Ahmed Mohammed Hussein
NetSentinels - CyberGuardians Track
Abu Dhabi University
Abu Dhabi, UAE
ahmed1202002@gmail.com

***Abstract*—In an age of constant digital threats, NetSentinel is a groundbreaking new defense system created for the 'Cyber Guardians' challenge. Old security tools that use simple blocklists are failing to stop modern cyber-attacks. Our project, NetSentinel, solves this problem with a smart, multi-level protection system. It instantly stops known dangers and sends any new, unknown website requests to a powerful AI brain for a deep check. This AI uses advanced analysis to score the risk of the new site. If it seems suspicious, the system does an even deeper investigation using global threat data. The best part is our 'Ask Why' feature, which explains in simple English why a threat was blocked. This makes advanced AI security easy for anyone to understand and trust.**

***Index Terms*—cybersecurity, DNS security, network defense, explainable AI (XAI), machine learning, innovative technology, smart cities**

I. Introduction

Think of the internet's Domain Name System (DNS) as its phonebook. Every time you visit a website, your computer uses DNS to look up the right address. But what if criminals poison the phonebook, sending you to a dangerous place? This is a huge problem today. Hackers use malicious websites for everything from phishing to malware, and they create thousands of new ones every day.

Old security systems rely on a simple list of bad websites. This is like having a phonebook of known criminals, but it's useless when a new criminal comes to town. Our challenge for the 'Cyber Guardians' track was to build a smarter guard—one that can spot a new threat *before* it has a chance to do any damage.

NetSentinel is that smart guard. We built it from scratch in just 30 hours to be a proactive, intelligent defender for any network. Our main goals were:

- To build a multi-level system that is both lightning-fast for safe traffic and incredibly thorough for new, unknown websites.
- To create a team of specialized AI "detectives" that work together at the same time to analyze different clues.
- To train our own custom AI model that can spot a bad website just by looking at the structure of its name.
- To create a feature that explains every single decision the AI makes in plain, simple English, building trust and making security easy for everyone.

II. Our Solution: The NetSentinel Method

NetSentinel acts as a smart checkpoint for all internet traffic. It checks every website request and makes a split-second decision: is it safe or is it dangerous? Its power comes from a multi-level analysis process, as shown in the professional flowchart in Fig. 1.

The NetSentinel Multi-Tier Decision Flowchart. This diagram shows how every query is processed for maximum speed and security.

A. Level 1 Analysis: The Quick Scan

Every website request first goes through a quick, high-speed scan.

1) Checking the Lists: First, the system checks its memory of "good lists" and "bad lists." If the website is already known to be safe or dangerous, a decision is made instantly. This makes the system extremely fast for 99

2) The AI Detective Team: If a website is new (not on any list), the request is sent to our team of three AI "detectives" that all work at the same time.

- **The Name Detective:** This AI looks for clues in the website's name. Strange patterns, lots of numbers, or unusual characters can be signs of a malicious site.
- **The History Detective:** This AI checks the website's background. Was it created just a few hours ago? Is the owner hiding their identity? These are red flags.
- **The Behavior Detective (Prototype):** This part of the system is designed to look for strange patterns, like one computer suddenly trying to contact hundreds of new websites at once.

These detectives vote, and if the risk score is high, the system escalates the case.

B. Level 2 Analysis: The Deep Investigation

A high-risk website from Level 1 is immediately sent for a deeper investigation. This saves time by not deeply checking obviously safe sites.

Project submission for the Innovation Hackathon UAE 2025, held at Zayed University, Dubai Campus, from 18-20th October 2025.

- **Global Threat Reports Check:** The system checks with VirusTotal, a global database of threats, to see if security experts around the world have already flagged this site.
- **Website Content Analysis:** The system does a quick check of the website itself to look for suspicious elements.

This two-level process gives a final, very accurate verdict: ”MALICIOUS,” ”SUSPICIOUS,” or ”LEGIT.”

C. A System That Learns and Improves

Every decision NetSentinel makes is recorded. When it confirms a new site is bad, it automatically adds it to the ”bad list” for the future. This means NetSentinel is constantly learning and gets smarter and faster over time.

III. How We Built It: Tools and Technologies

The NetSentinel prototype was fully built in just 30 hours during the hackathon. We chose simple, powerful, and fast tools to get the job done.

- **Core System and AI Brains:** We used **Python**, a popular and powerful language, with the **Flask** framework to build our main engine and all the AI detective modules.
- **Artificial Intelligence:** The ”Name Detective” uses a `RandomForestClassifier` model from the **Scikit-learn** library, a standard for machine learning. We trained this model ourselves on a dataset of good and bad domains.
- **Checking Website History:** We used the `python-whois` library to automatically look up the registration details for any website.
- **Memory and Logging:** We used **SQLite** as our system’s memory. It’s a simple, file-based database that is perfect for logging every event without needing a big, complex server.
- **The Dashboard:** The control panel was built with standard **HTML, CSS, and JavaScript**. It feels like a modern web app and updates in real-time, but it’s built on simple, reliable technology.

IV. What We Achieved: Results and Impact

Our final prototype is a complete, working security solution. It’s a polished and powerful platform that is ready to protect a network.

A. An Easy-to-Use Command Center

The main dashboard is the heart of the system. It gives a simple, clear view of the network’s security at a glance. It shows real-time stats like how many threats have been blocked, and it allows anyone, even non-technical staff, to easily manage the system’s lists.

B. The ’Ask Why’ Feature: A Breakthrough in Trust

Our most important innovation is the ”Ask Why” feature. In most AI systems, decisions are a mystery—a ”black box.” We solved this problem. With NetSentinel, an operator can simply type in a website or a query ID and get an instant report in plain English explaining *exactly* why it was blocked. For example: ”This website was blocked because the Name Detective found its name was suspicious, and the History Detective saw it was created only 5 hours ago.” This builds trust and makes powerful AI accessible to everyone.

V. Conclusion and The Vision for the Future

In just 30 hours, we turned an idea into a fully working prototype of a next-generation security system. NetSentinel proves that it’s possible to build a defense that is both extremely fast and deeply intelligent. It’s exactly the kind of smart security needed to protect the UAE’s fast-growing digital world.

Our ’Ask Why’ feature is a major step forward, making complex AI simple and trustworthy.

This project is just the beginning. For the future, we plan to:

- **Activate the Behavior Detective:** Fully build out the module that can spot suspicious patterns and behaviors over time.
- **Add More Global Intel:** Connect NetSentinel to more global threat report databases to make its decisions even smarter.
- **Make it Ready for the Cloud:** Package the system using Docker, a technology that makes it easy to deploy and scale anywhere, from a small office to a huge corporation.

NetSentinel is more than just a project; it’s a new way of thinking about security. It provides a strong, practical, and innovative foundation that perfectly matches the hackathon’s goal of creating real-world solutions to protect our nation’s digital future.