Network Security (CS3403)
Project Report

Secure TCP-based IoT Honeypot for Attacker Behaviour Monitoring

Submitted by

Jeevan EG

1RVU22CSE069

School of Computer Science

RV University

Submitted to

Dr Chandramouleeswaran Sankaran

Professor

School of Computer Science

RV University

Submission date : 15-04-2025

Network Security (CS3403)
Project Report

1. Abstract

This project implements a TCP-based IoT honeypot system designed to detect and log malicious activities targeting edge and IoT devices. The system simulates vulnerable services and captures attacker payloads using encryption, fake banners, and logging mechanisms. An interactive Streamlit dashboard visualizes real-time attacker data. The goal is to understand attacker behavior in a safe, controlled environment.

2. Introduction

Project Background and Relevance:

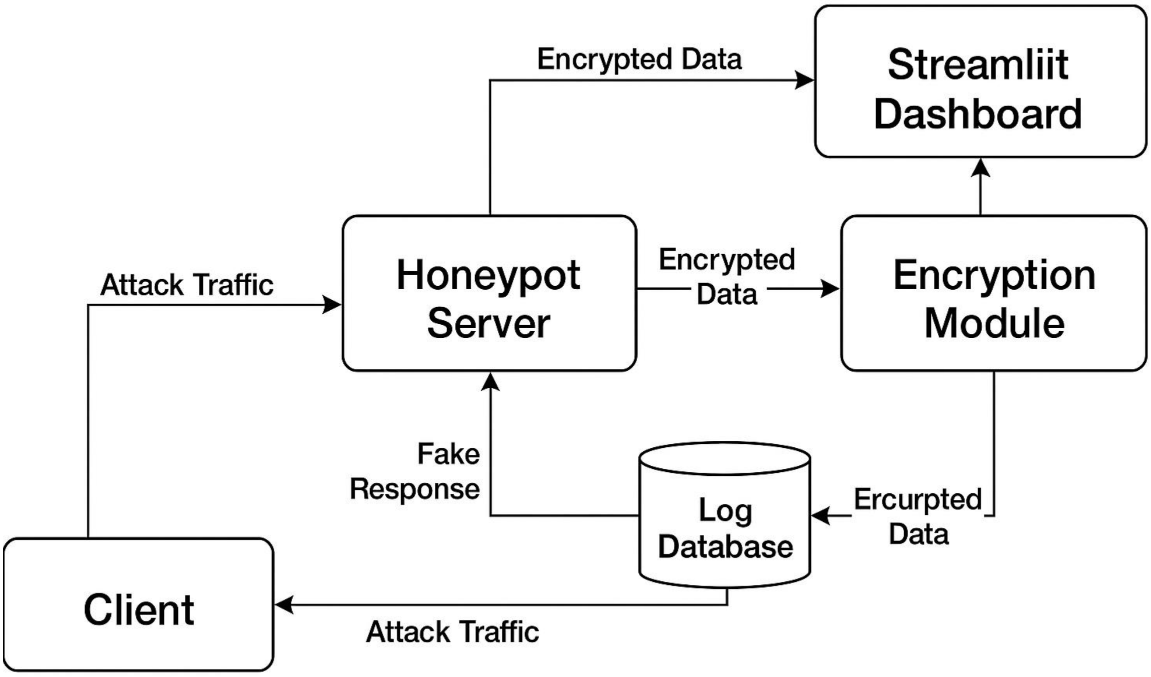
As IoT and edge devices proliferate, they become prime targets for attackers due to their limited computing resources and often weak security. Honeypots provide a passive defense mechanism to detect and analyze these threats without compromising real systems.

Objectives:

- Simulate a fake vulnerable IoT device service.
- Securely capture attacker payloads and IPs.
- Visualize and analyze malicious behavior.
- Learn attacker tactics in real-time through a dashboard.

3. System Overview

System Architecture:



4. Design:

Core Components:

- **Server (server.py)**: Accepts incoming connections, decrypts data, logs it, and responds with fake system banners.
- **Client (client.py)**: Simulates attacker commands and sends data to the server after encrypting with a shared secret key.

- **Encryption (encryption.py)**: AES-based symmetric encryption using cryptography.fernet.
- **Logger (logger.py)**: Logs attacker data into both CSV and SQLite3.
- **Payload Handler (honeypot_core.py)**: Responds with fake OS-like replies to attacker commands.
- **Dashboard (dashboard.py)**: Built using Streamlit to monitor logs, frequency, and timeline of attacks.

5. Security Features:

- **Encrypted communication** using Fernet symmetric key encryption.
- **Fake IP injection** to simulate attacker geography.
- **Secure logging** of IPs, timestamps, and payloads.
- **Data visualization** for better forensic analysis.
- **Multi-client support** to simulate concurrent attacks.
- **No real system is compromised** — all payloads are sandboxed.

6. System Requirements

- **Operating System:** Windows 10/11 + WSL2 (Ubuntu)
- **Languages Used:** Python 3.11+
- **Network Ports Used:** TCP port 9090
- **Required Libraries:** cryptography, streamlit, pandas, sqlite3, requests

7. Open-source libraries and tools

- **cryptography (v41.0+)**

Used for symmetric key encryption and decryption using Fernet (AES-128 under the hood). Ensures secure communication between client and server.

- **streamlit (v1.30+)**

Used to build the interactive dashboard for real-time monitoring of attacker activity. Enables filtering, graphs, and CSV download.

- **pandas (v2.2+)**

Used for data manipulation and reading/writing logs in CSV format. It powers log filtering and analytics in the dashboard.

- **sqlite3 (built-in)**

A lightweight SQL database used for persistent attacker log storage. Helpful for scalable data logging and retrieval.

- **requests (v2.31+)**

Used to interact with `ip-api.com` to get geolocation info based on the attacker's (fake) IP address.

8. Implementation and Testing

- **Multi-client testing** with different fake IPs (e.g., `8.8.8.8`, `51.140.123.1`).

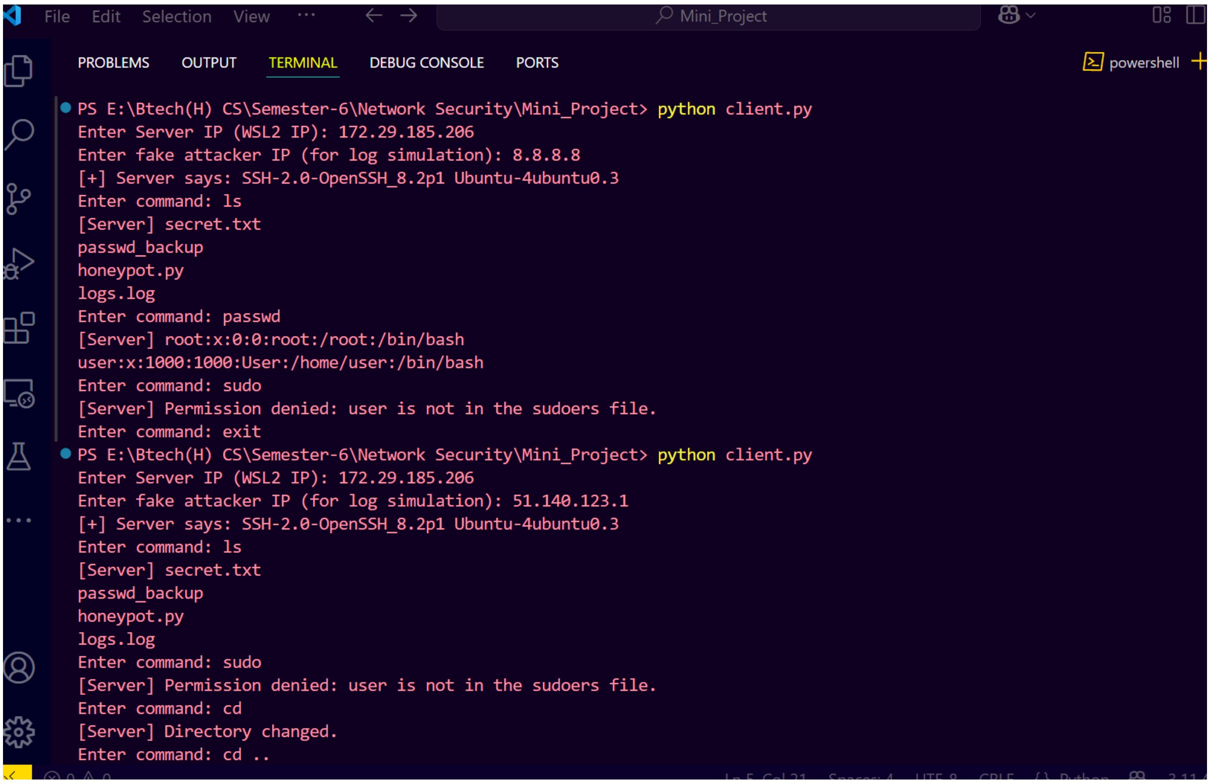
- **Live communication** between client & server validated with encrypted responses.

- **Attack simulation** through multiple terminals with different payloads (`ls`, `whoami`, etc.)

- **Visualization validated** with Streamlit dashboard using SQLite3 data.

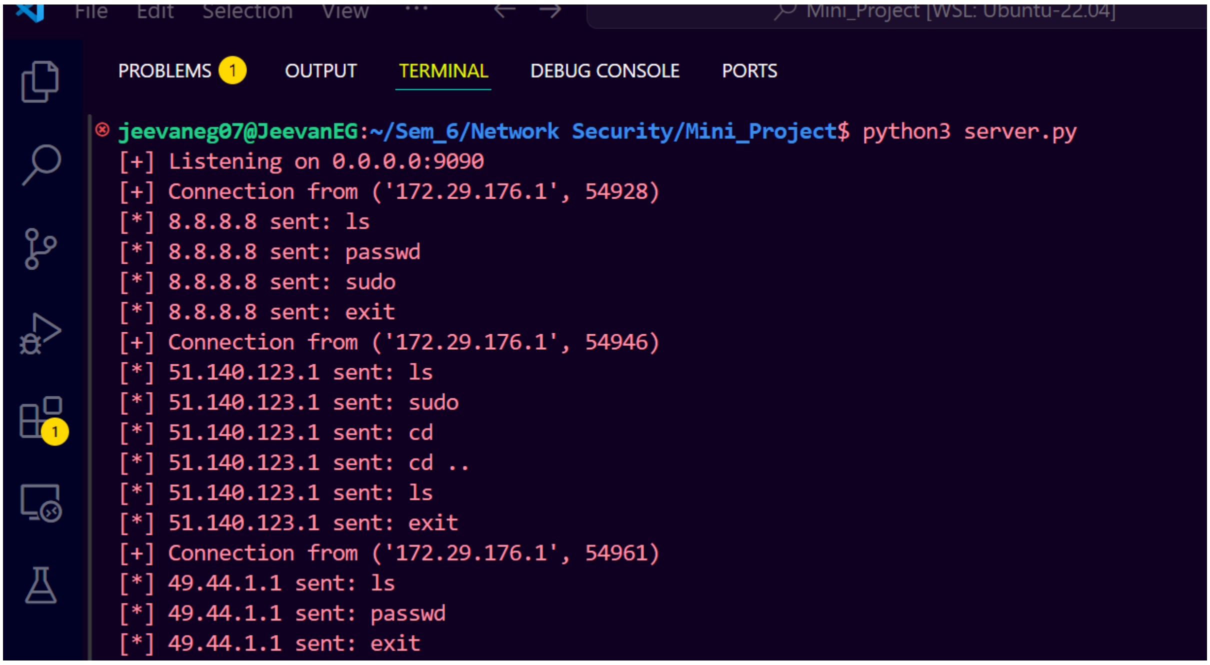
9. Results

- **Running Client with IP Address of different countries.**



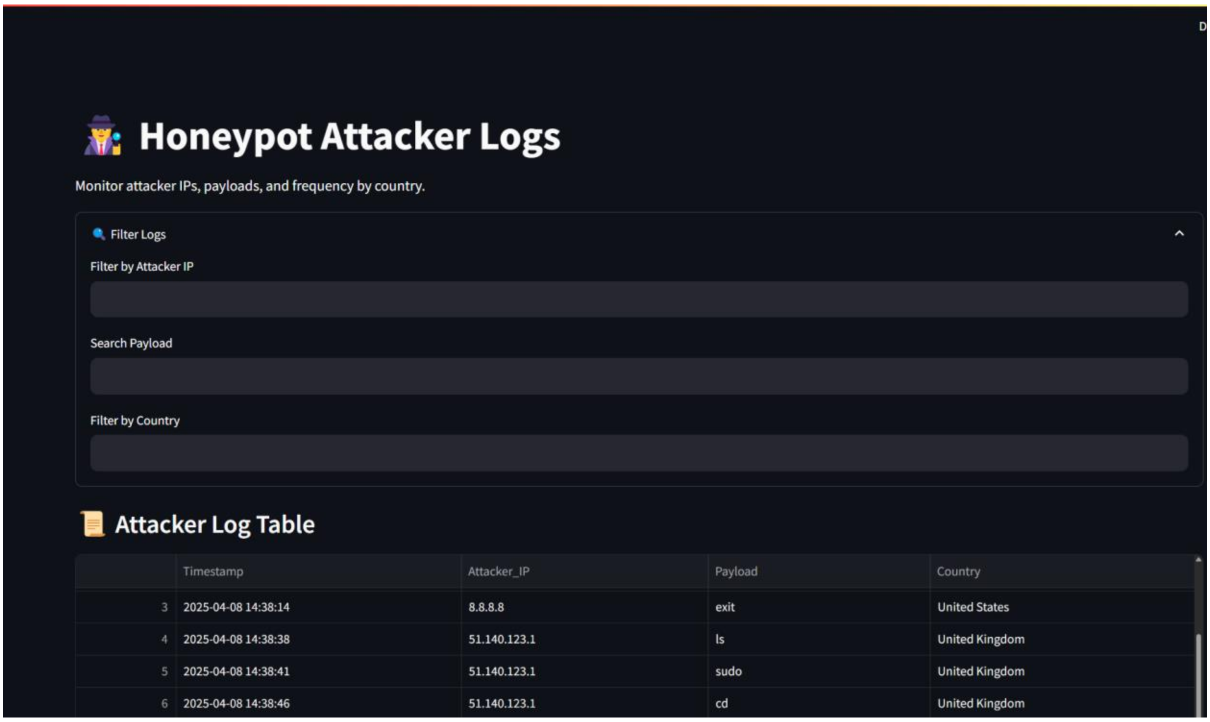
```
PS E:\Btech(H) CS\Semester-6\Network Security\Mini_Project> python client.py
Enter Server IP (WSL2 IP): 172.29.185.206
Enter fake attacker IP (for log simulation): 8.8.8.8
[+] Server says: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
Enter command: ls
[Server] secret.txt
passwd_backup
honeypot.py
logs.log
Enter command: passwd
[Server] root:x:0:0:root:/root:/bin/bash
user:x:1000:1000:User:/home/user:/bin/bash
Enter command: sudo
[Server] Permission denied: user is not in the sudoers file.
Enter command: exit
PS E:\Btech(H) CS\Semester-6\Network Security\Mini_Project> python client.py
Enter Server IP (WSL2 IP): 172.29.185.206
Enter fake attacker IP (for log simulation): 51.140.123.1
[+] Server says: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
Enter command: ls
[Server] secret.txt
passwd_backup
honeypot.py
logs.log
Enter command: sudo
[Server] Permission denied: user is not in the sudoers file.
Enter command: cd
[Server] Directory changed.
Enter command: cd ..
```

- **Fake Server Logging all the Info of the Attacker**



```
jeevaneg07@JeevanEG:~/Sem_6/Network Security/Mini_Project$ python3 server.py
[+] Listening on 0.0.0.0:9090
[+] Connection from ('172.29.176.1', 54928)
[*] 8.8.8.8 sent: ls
[*] 8.8.8.8 sent: passwd
[*] 8.8.8.8 sent: sudo
[*] 8.8.8.8 sent: exit
[+] Connection from ('172.29.176.1', 54946)
[*] 51.140.123.1 sent: ls
[*] 51.140.123.1 sent: sudo
[*] 51.140.123.1 sent: cd
[*] 51.140.123.1 sent: cd ..
[*] 51.140.123.1 sent: ls
[*] 51.140.123.1 sent: exit
[+] Connection from ('172.29.176.1', 54961)
[*] 49.44.1.1 sent: ls
[*] 49.44.1.1 sent: passwd
[*] 49.44.1.1 sent: exit
```

- **GUI Interface that logs all the info like timestamp , Attacker IP, Payload, country**



🕵️ Honeypot Attacker Logs

Monitor attacker IPs, payloads, and frequency by country.

🔍 Filter Logs

Filter by Attacker IP

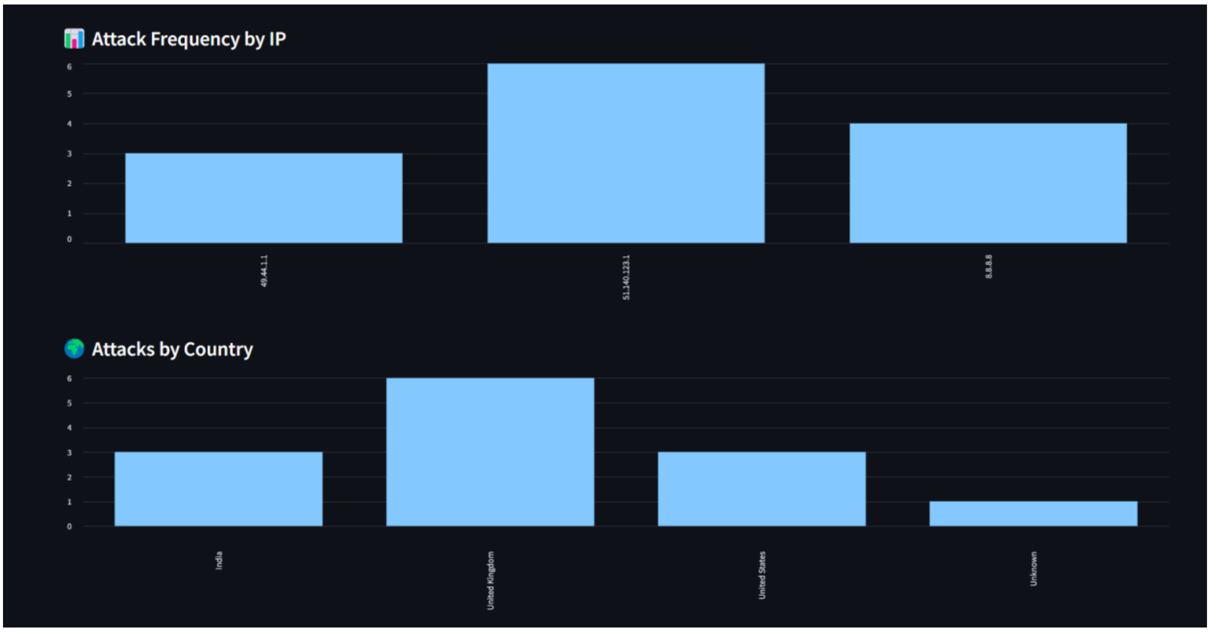
Search Payload

Filter by Country

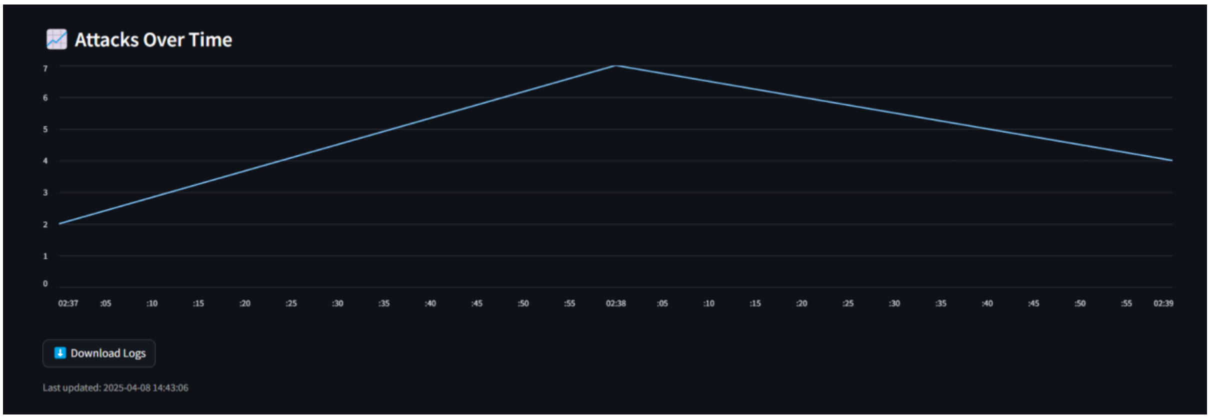
📜 Attacker Log Table

	Timestamp	Attacker_IP	Payload	Country
3	2025-04-08 14:38:14	8.8.8.8	exit	United States
4	2025-04-08 14:38:38	51.140.123.1	ls	United Kingdom
5	2025-04-08 14:38:41	51.140.123.1	sudo	United Kingdom
6	2025-04-08 14:38:46	51.140.123.1	cd	United Kingdom

- **Attack Frequency by IP && Attacks by Country**



- **Attacks Over Time**



Last updated: 2025-04-08 14:43:06

10.Conclusion

This project provided hands-on experience in network security, encryption, attacker simulation, and real-time data visualization. We learned how attackers probe systems and how honeypots can serve as an effective tool for early detection and forensic logging in IoT environments.

****