Project Concept Sheet

Title: Bio-Adaptive Honeynet for IoT Threat Intelligence

1. Background / Problem Statement

The Internet of Things (IoT) connects billions of devices — cameras, smart locks, sensors, medical tools — all with minimal security and weak patching. Attackers exploit these devices to form botnets, steal data, or launch DDoS attacks. Traditional honeypots can capture attacks but are static: once identified, attackers simply avoid or disable them. We need a honeypot system that evolves and adapts — like a biological immune system — to stay unpredictable and resilient.

2. Project Aim

To design and implement an adaptive honeypot framework for IoT networks that: - Attracts and studies real-time cyberattacks, - Shares intelligence across honeypots (like cells sharing immune signals), - Evolves its own signatures and behavior based on captured data, - And visualizes attack patterns as living “infection maps.”

3. Specific Objectives

1. Deploy a cluster of IoT-emulating honeypots using lightweight virtualization. 2. Implement morphing logic — periodic self-reconfiguration of device fingerprints. 3. Integrate a quorum-based alert system to validate alerts collaboratively. 4. Develop a learning module that evolves detection signatures using AI. 5. Create a real-time visualization dashboard showing attacker origins and propagation paths.

4. Methodology / System Design

Layer	Component	Biological Inspiration	Function
1	IoT Honeypots	Cells	Emulate IoT devices to attract threats
2	Morphing Engine	Polymorphism	Mutate visible attributes periodically
3	Quorum Service	Quorum Sensing	Cross-node alert validation
4	Learning Engine	Immune Memory	Update and distribute detection rules
5	Visualization	Epidemiology Maps	Display live attack flows

5. Tools & Technologies

Python, Docker, Flask, Conpot/Cowrie/Honeyd, Redis or MQTT, Grafana/Kibana, Scikit-learn

6. Expected Outcomes

- A working prototype that changes its identity automatically. - Distributed honeypots that collaborate for validation. - Self-learning detection system improving over time. - Live dashboard showing attack attempts and propagation. - Dataset and analytics report summarizing attack trends.

7. Novelty / Contribution

- Combines biological adaptation principles with IoT security. - Introduces quorum sensing for collaborative detection. - Adds self-learning immune mechanisms. - Visualizes IoT threats using biological metaphors.

8. Deliverables

1. Technical report and documentation. 2. Working prototype (Dockerized honeypot cluster). 3. Visualization dashboard. 4. Final presentation and demo video.

9. Supervisors / Collaborators

Supervisor: Dr. Dorcus Arshley
Team Members: Chelsea Abida, Michael Muriithi, Davies Kabii, Festus Pokodu

10. Project Timeline (suggested 4-phase)

Phase	Duration	Output
1. Research & Design	Weeks 1–3	Architecture and setup scripts
2. Implementation	Weeks 4–7	Honeypot cluster + morphing engine
3. Integration & Learning	Weeks 8–10	Quorum and learning module
4. Testing & Visualization	Weeks 11–12	Dashboard + final evaluation