Dynamic Honeypots for Zero-Day IoT Exploits Using Self-Adaptive Behavioral Traps

- **Problem Statement**: Current honeypots for IoT devices often fail to adapt to new exploits, especially zero-day attacks. Research a **self-adaptive honeypot** system that evolves in real-time by learning attacker patterns and simulating vulnerabilities dynamically.
- **Why Unique**: Existing honeypots are often static and ineffective against new IoT attack vectors. No standard system addresses **zero-day exploits dynamically** in IoT ecosystems.
- **Approach**:
    - Design a system that analyzes incoming attack payloads using ML.
    - Use generative techniques to evolve honeypot behavior, mimicking exploitable vulnerabilities on the fly.
    - Deploy on small IoT devices like smart cameras or thermostats to monitor real-world efficacy.
- **Impact**: Disrupts attacker reconnaissance on IoT networks and gathers intelligence on emerging attack methods.

Quantum Cryptographic Algorithms in Blockchain Consensus Mechanisms

- **Problem Statement**: While quantum-safe encryption is a hot topic, its application in blockchain consensus mechanisms like **Proof-of-Stake (PoS)** is still underexplored. Investigate how quantum cryptographic algorithms could secure blockchain voting systems.
- **Why Unique**: Blockchain's reliance on classical encryption makes it vulnerable to future quantum attacks, but integrating quantum algorithms into consensus mechanisms is a nascent field.
- **Approach**:
    - Replace standard cryptographic primitives (e.g., RSA) in PoS blockchains with quantum-safe algorithms (e.g., lattice-based cryptography).
    - Simulate performance trade-offs in transaction speed and scalability.
- **Impact**: Future-proofs blockchain technology against quantum threats while maintaining decentralization.

Advanced Phishing Kits Using ChatGPT-like Models for Personalized Attacks

Problem Statement: Investigate the growing use of large language models (LLMs) to generate highly personalized phishing emails and propose countermeasures to detect AI-generated phishing attempts.
Why Unique: Targets the specific abuse of **LLMs in social engineering** attacks.
Research Focus:

- Analyze the linguistic patterns of LLM-generated phishing emails compared to human-written ones.
- Develop a detection system that combines linguistic forensics with metadata analysis.
- Evaluate the system on real-world datasets of phishing emails.

Analysis and Mitigation of QR Code Phishing on Digital Kiosks

Problem Statement: Study how attackers embed malicious QR codes on public digital kiosks to steal user credentials or direct users to phishing websites. Develop tools to detect malicious QR codes using pattern recognition and website analysis.
Why Unique: Very niche focus on **public kiosk systems and QR code-based phishing attacks**, a growing but under-researched threat.
Research Focus:

- Collect a dataset of real and malicious QR codes.
- Design a scanner that integrates QR code decoding with real-time domain verification (e.g., using VirusTotal).
- Test the solution on real-world digital kiosks (e.g., in malls, airports).

Exploitation of Zero-Day Vulnerabilities in Kubernetes Clusters via Container Escape Attacks

Problem Statement: Study how container escape vulnerabilities (e.g., CVEs in Docker runtime) can be exploited in Kubernetes clusters and propose runtime monitoring solutions specific to escaping processes.
Why Unique: Focuses on **container security within Kubernetes**, targeting niche zero-day vulnerabilities in runtime isolation.
Research Focus:

- Reproduce real-world container escape exploits in a controlled Kubernetes environment.
- Develop tools to identify malicious process patterns at the kernel level.
- Benchmark solutions against open-source intrusion detection tools like Falco.