Abstract

AI-Powered APT Detection System with Blockchain and Network Simulation

Advanced Persistent Threats (APTs) are sophisticated cyber-attacks designed to evade traditional security defenses while infiltrating networks for prolonged periods. This project proposes an **AI-powered APT detection system** integrated with **blockchain and network simulation** to enhance cybersecurity defenses. The system utilizes **Graph Neural Networks (GNNs), anomaly detection models, and temporal analysis** to identify stealthy attack patterns. **Blockchain technology ensures tamper-proof security logs, decentralized threat intelligence sharing, and automated incident response via smart contracts.**

The project also incorporates **network simulation tools (e.g., GNS3, NS3, or Mininet)** to model real-world attack scenarios, enabling security teams to test and refine their defense mechanisms. The system is designed to work in real-time, continuously learning from new attack patterns and providing security analysts with **graph-based visualizations of attack paths**.

Tech Stack:

- **Machine Learning & AI:** Python, TensorFlow/PyTorch, Scikit-learn, Graph Neural Networks (GNNs)
- **Blockchain:** Ethereum, Hyperledger Fabric, IPFS, Smart Contracts (Solidity)
- **Network Simulation & Security Tools:** Kali Linux, Wireshark, Snort, Suricata, GNS3, NS3, Mininet
- **Databases & Storage:** Neo4j (Graph DB), MongoDB, Apache Kafka (Streaming Data)
- **Visualization & Dashboarding:** D3.js, Grafana, Kibana

By combining **AI, blockchain, and network simulation**, this project aims to build an advanced, **scalable, and explainable cybersecurity solution** capable of detecting and mitigating APTs effectively. The outcome will be a robust **intrusion detection system (IDS) that enhances threat intelligence, strengthens digital forensics, and automates security responses**