**AI-Powered Self-Healing Security Framework**

**Overview**

Cyber threats require proactive defences. This project introduces an AI-powered self-healing security system integrating automated threat response, adaptive security policies, and self-repair mechanisms to enhance resilience.

**Technical Approach**

* **Automated Incident Response:** AI-driven threat classification using Random Forest, Neural Networks, and Reinforcement Learning for dynamic mitigation.
* **Adaptive Security Policies:** Bayesian Optimization, Genetic Algorithms, and deep learning-based behavioural analysis to refine configurations.
* **Self-Healing Mechanism:** Blockchain-based integrity verification, containerized recovery (Docker/Kubernetes), and fault-tolerant architectures.
* **Scenario-Based Testing:** Attack simulations (ransomware, IoT botnet) with metrics on resilience, response time, and false positives.

**Tech Stack**

* **AI & ML:** TensorFlow, PyTorch, Scikit-learn
* **Security Tools:** Snort, Suricata, Zeek, OpenAI GPT
* **Automation:** Ansible, Terraform, Kubernetes
* **Cloud:** AWS, Azure, Google Cloud
* **Blockchain & Cryptography:** Hyperledger Fabric, SHA-256
* **Languages:** Python, Java, Go

**Key Findings**

* AI anomaly detection improves threat classification accuracy (>90%).
* Adaptive security policies optimize defences and reduce false positives.
* Self-healing reduces system downtime by 75%.
* Continuous learning enhances cybersecurity resilience.

**Conclusion**

This scalable AI-powered security framework strengthens enterprise IT, cloud, and IoT cybersecurity. Future enhancements include refining AI models, expanding real-world testing, and integrating advanced threat intelligence.