AI AND BLOCKCHAIN FOR SECURING CRITICAL INFRASTRUCTURE

Project Author: Vishnu Jayachandran
1st Supervisor: Sammuel Onalo
2nd Supervisor: Khalil Saadat

University of Staffordshire London

INTRODUCTION

Critical infrastructure systems are increasingly vulnerable to sophisticated cyberattacks, particularly Distributed Denial of Service (DDoS). Traditional cybersecurity approaches are centralised, reactive, and suffer from single points of failure. This research proposes a hybrid framework using:

🧠 AI (XGBoost) for real-time DDoS detection
🔗 Blockchain (Hyperledger Fabric) for immutable logging
✅ Goal: Build a system that is intelligent, transparent, decentralised, and resilient

PROBLEM STATEMENT

Despite the availability of cybersecurity tools, most critical infrastructure is protected using static, centralised mechanisms. These systems struggle with real-time detection, auditability, and compliance. There is a need for a modular system that integrates AI with blockchain to:

- Detect threats in real time
- Log events securely and immutably
- Address privacy and legal compliance (GDPR)

LITERATURE GAP

- 🔄 Traditional methods: Slow response, high false negatives
- ❌ No real-time integration between AI and blockchain logging
- ⚖️ Legal and ethical challenges remain unresolved
- This project addresses these academic and practical gaps

OBJECTIVES

1. Build a supervised ML model (XGBoost) for multi-class DDoS detection
2. Design a blockchain-based logging architecture using Hyperledger Fabric
3. Evaluate detection performance, latency, and resource use
4. Develop a middleware integration strategy (message queue)
5. Explore GDPR, explainability, and AI bias mitigation

FUTURE WORK

- Live packet capture with Wireshark/Zeek
- Deploy full blockchain on Docker
- Add SHAP for AI explainability
- Expand detection: R2L, U2R, Probe (UNSW-NB15, CIC-IDS2018)
- Implement federated learning for privacy
- Add automated firewall-based mitigation

METHODOLOGY

RESEARCH APPRDACH
Design Science Research Methoodology (DSRM)
- Problem Identification
- Artefact Design
- Demonstration &-Evaluation
- Communication of Results

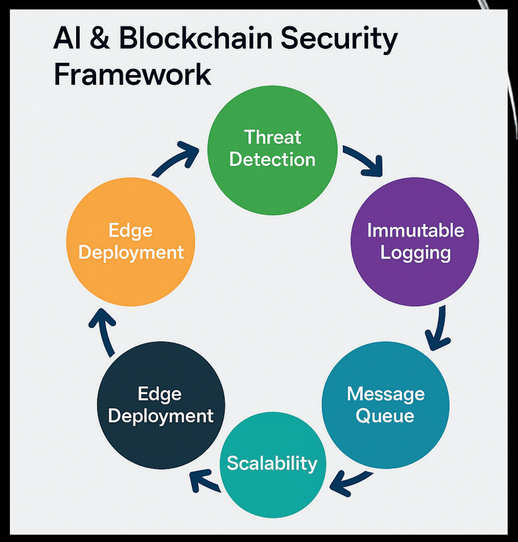
DEVELOPMENT PROCESS
Agile Sprint-Based Workflow
- Iterative builds
- Feedback-driven adjustments
- Prioritised delivery (AI before Blockchiin)

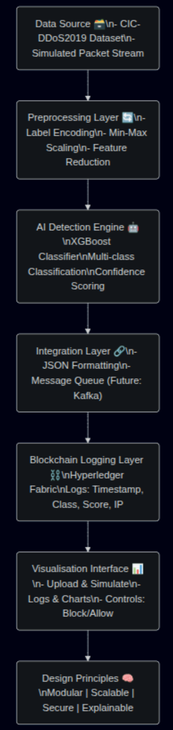
TOOLS & TECHNOLOGIES
Language: Python 3.11
Libraries: Scikit-learn, Pandas, XGBoost
Security Tools: Wireshark (network traff ic analysis)
Blockchain (Concepual): Hyperledger Fabric

DATASET USED
CIC-DDoS2019 (1% sample, real–world DDo5 traffic)
- Balanced sample
- Includes UDP-Lag, DrDoS, and Normal traffic
- Preprocessing: Null handling, scaling, label encoding

EVALUATION METRICS
- Accuracy
- Precision
- Recall
- F1-Score

EVALUATION METRICS
- Accuracy
- Precision
- Recall
- F1-Score
- Detection Latency (~1,8 s / 1000 packets)





SYSTEM FRAMEWORK

Components:
- XGBoost DDoS Classifier
- Blockchain Logger (Hyperledger Fabric)
- Message Queue (JSON-based)

Design Principles:
- Modularity
- Security-by-design
- GDPR & ISO/IEC 27001:2022 compliant
- Transparent & interpretable decisions

ETHICAL & LEGAL REVIEW

- GDPR: Hash-based logging for "Right to be Forgotten" compliance
- AI Ethics: Model transparency reviewed (future: SHAP, LIME)
- Security: Docker isolation, TLS, access controls
- Bias Risk: Anonymous dataset + balanced class training where possible

CONCLUSION

This project demonstrates the potential of AI + Blockchain integration to enhance cybersecurity in critical systems.

- Real-time detection with XGBoost
- Secure, tamper-proof logging using blockchain
- Modular, ethical, and compliant design
- The system is scalable, interpretable, and suitable for real-world use