ENHANCING CYBERSECURITY MEASURES IN HYBRID CLOUD ENVIRONMENTS THROUGH AI AND BLOCKCHAIN INTEGRATION

University of Staffordshire London

Author: Okikiade Adeyemi

1st Supervisor: Dr Samuel Onalo

2nd Supervisor: Dr Mohammad Heydari

Introduction

Hybrid cloud environments offer agility and scalability but introduce critical security challenges. This research aims to strengthen cybersecurity by integrating machine learning (ML) for threat detection and blockchain for tamper-proof and immutable logging.

OBJECTIVES

To design and implement an improved cybersecurity framework using:

- AI-based anomaly detection.
- Blockchain-based immutable logging.
- Modular architecture for hybrid cloud systems.

Research Gap

Most hybrid cloud security frameworks handle threat detection and data integrity in isolation. Traditional models often rely on outdated detection techniques or centralised logging, which are prone to tampering.

There is an apparent lack of integrated, real-time solutions that combine:

- Machine Learning for Dynamic Anomaly Detection
- Blockchain for tamper-proof event logging

This project bridges the gap by developing a modular framework, TrustGate, CyberShield, and BlockSecure, that delivers real-time visibility and immutable security logs in hybrid cloud environments.

System Framework

- TrustGate: MFA, RBAC, Identity Validation.
- CyberShield: AI anomaly detection.
- BlockSecure: Blockchain-based secure logging.

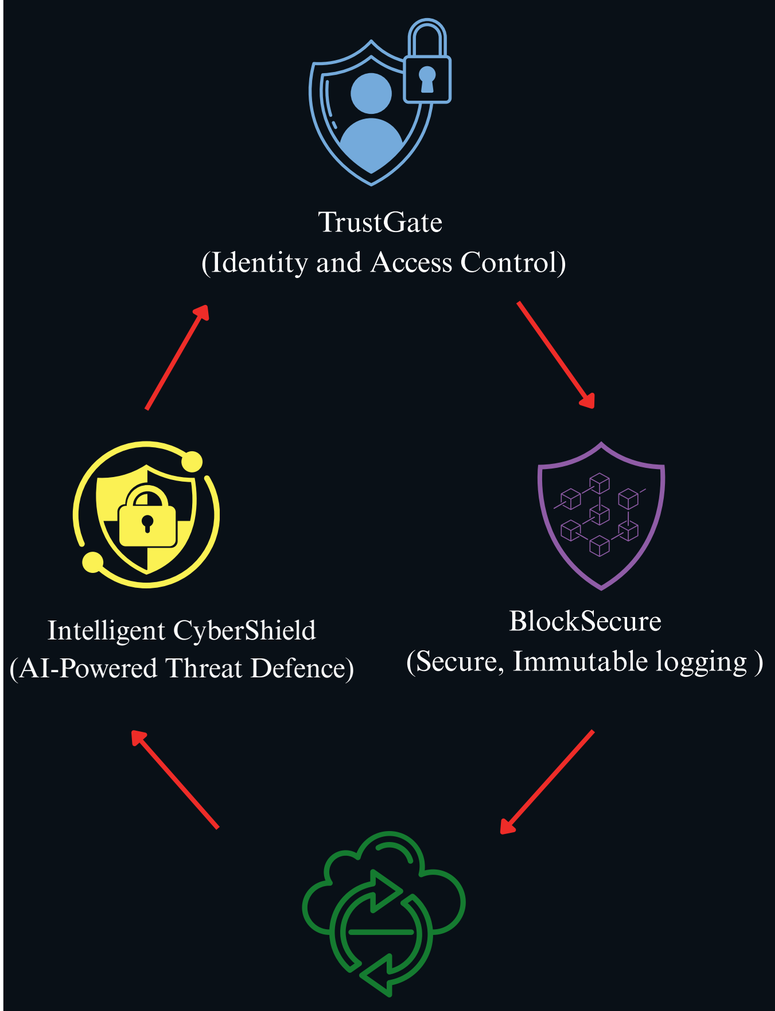

Fig 1. Framework Cyclic Diagram

Methodology

- Research Approach : Design Science Research Methodology (DSRM).
- Implementation Tools: Python (Jupyter Notebook), Scikit-learn (Isolation Forest), Web3.py & Ganache (Blockchain logging), and Remix IDE (Smart contract development).

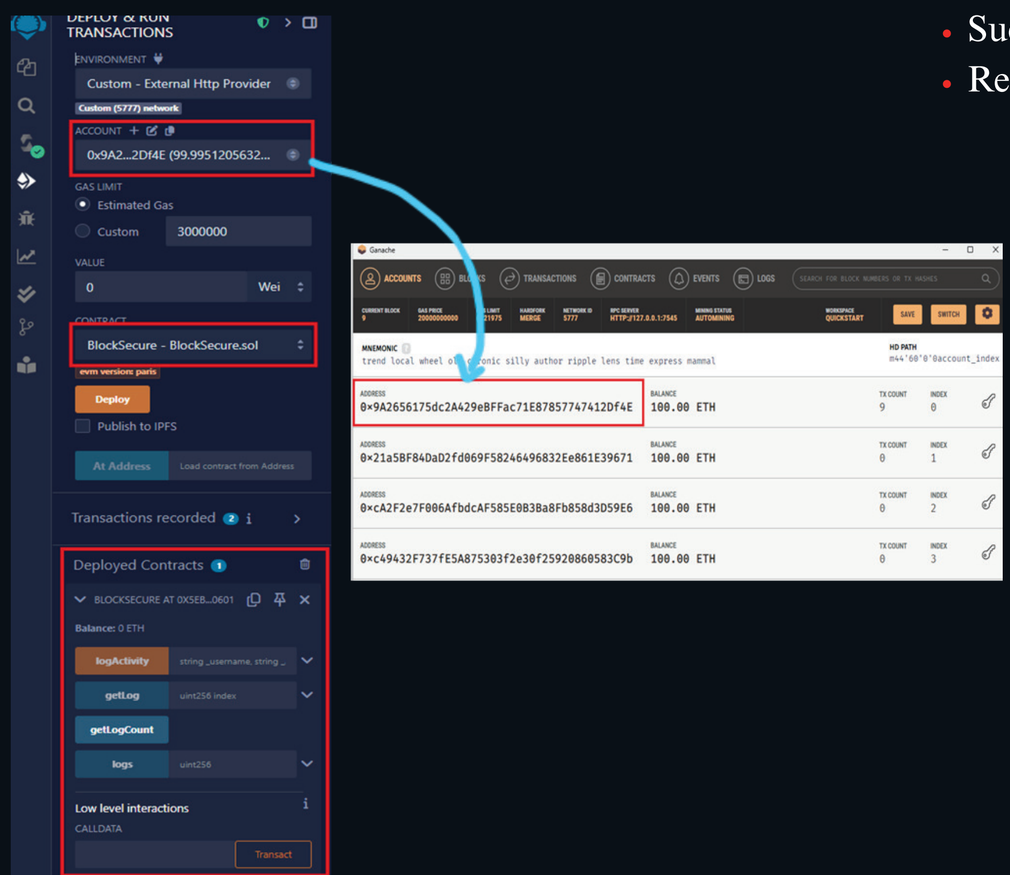

Fig 2. Deployment Confirmation & Blockchain Wallet Integration

RESULTS

CyberShield:

- Achieved a detection accuracy of 65%. (This is due to the limited dataset provided, a larger dataset would yield more precise results.)
- Confusion Matrix & Classification Report show practical viability.

BlockSecure:

- Successfully deployed smart contract on Ganache.
- Real-time event logging using transaction hashes.

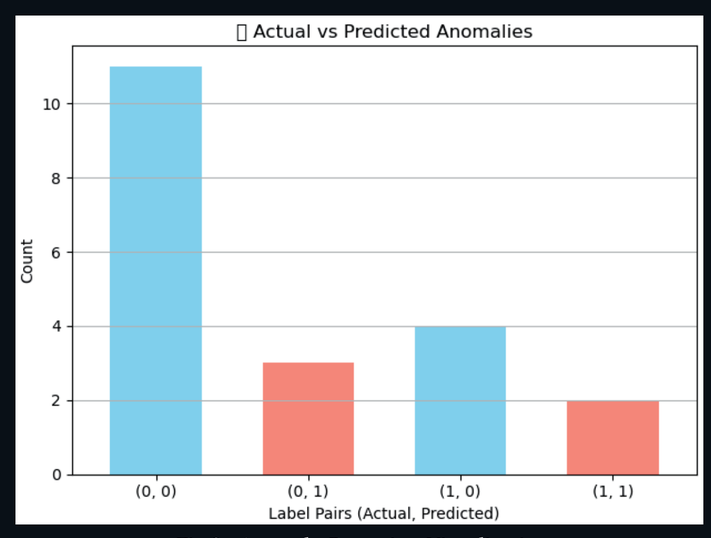

Fig 3. Anomaly Detection Visualisation

Analysis

- Isolation Forest detected anomalies based on login success, location, and access behaviour.
- Blockchain logs enhance traceability and auditability.
- Practical use case for Zero Trust enforcement in cloud systems.

Conclusion

The framework proves AI and blockchain integration can enhance security posture in hybrid cloud infrastructures, offering scalable and tamper-proof solutions.

Future Recommendations

- Deploy in actual enterprise testbeds.
- Incorporate deep learning models like LSTM and support cross-chain smart contracts.

Acknowledgements

I want to thank my supervisor, Dr. Samuel Onalo, for their invaluable guidance and support throughout this project, and the University of Staffordshire for providing essential resources and knowledge during the research process.