AltFlex: Technical Specification and Implementation Guide

A Flexible AI-Powered Forensic Framework for Exploit Detection in Cross-Chain Bridges and DeFi Protocols

Document Type: Technical Specification & Implementation Guide

Version: 1.0.0

Date: January 29, 2026

Authors: Jay Arre P. Talosig, Rinoah Venedict Dela Rama,
Alexander Castilo, Nicko Nehcterg D

Institution: National University Manila

Course: CCSFEN2L - Software Engineering 2

Instructor: Professor Armida Salazar

Executive Summary

AltFlex represents a novel integration of artificial intelligence and digital forensics methodologies specifically engineered to address the escalating security vulnerabilities in decentralized finance (DeFi) protocols and cross-chain bridge infrastructure. This technical specification delineates the architectural design, algorithmic foundations, and implementation strategies employed in constructing a production-grade exploit detection framework capable of real-time threat identification and forensic analysis.

The framework synthesizes machine learning-based anomaly detection with rule-based pattern matching to achieve comprehensive coverage of known and emerging exploit vectors. Through rigorous empirical validation against historical exploit datasets totaling $406.35M in documented losses, AltFlex demonstrates the viability of proactive security monitoring in the Web3 ecosystem.

Key Technical Contributions:

• Hybrid Detection Architecture: Integration of XGBoost-based anomaly detection with deterministic rule engines

• Multi-Layer Address Verification: 5-stage validation pipeline incorporating EIP-55 checksum verification, on-chain intelligence, and behavioral analysis

• Forensic Integrity Mechanisms: Cryptographic audit logging and tamper-evident transaction recording

• Production-Ready Implementation: 146 automated test cases, API security hardening, and enterprise-grade frontend interface

Document Structure

This PDF contains the title page and executive summary of the AltFlex Technical Specification. The complete document includes the following sections:

1. Literature Review Synthesis and Research Gap Analysis

2. System Architecture (with Mermaid diagrams)

3. Blockchain Data Layer ↔ AI Detection Module Interaction

4. Component Specifications (Data Collectors, Feature Engineering, ML Models)

5. Forensic Analysis Module: Technical Specification

6. Forensic Integrity and Tamper-Proofing Mechanisms

7. Known Exploits: Empirical Analysis

8. API Security and Production Hardening

9. Frontend Architecture and User Interface

10. Testing and Validation Strategy

11. Deployment and Operational Considerations

12. Conclusions and Future Work

13. References and Appendices

Note: For the complete technical specification with all diagrams, code examples, and detailed analysis, please refer to the markdown version: *docs/TECHNICAL_SPECIFICATION.md* or the HTML version: *docs/RRL/TECHNICAL_SPECIFICATION.html*