AltFlex: AI-Powered Forensic Framework

Exploit Detection in Cross-Chain Bridges

Working Title

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

Group Members

Name	Role	Specialization
Jay Arre Talosig - COM231	Lead Developer & AI Architect	Blockchain, AI/ML, Smart Contract
Rinoah Venedict Dela Rama - COM232	Forensic Analyst & Python Developer	Digital Forensics, Python, Data Engineering
Mark Jhosua Taberna - COM231	Full Stack Developer & UI Specialist	Digital Forensics,Full-Stack, Web Development
Nicko Nehcterg Dalida - COM232	Quality Assurance & Security Tester	Digital Forensics, QA, Pentesting
Alexander Castilo - COM231	Penetration Tester & Threat Researcher	Digital Forensics, Ethical Hacking, Threat Intelligence

Project Overview

AltFlex is an integrated AI and digital forensics framework designed to proactively detect and analyze security exploits in cross-chain bridges and DeFi protocols. By combining maching learning anomaly detection with blockchain forensic analysis, the system provides a comprehensive security solution for the rapidly evolving Web3 ecosystem.

Problem Statement

DeFi protocols and cross-chain bridges are increasingly vulnerable to exploits, resulting in significant financial losses. Current security measures often lack the agility and intelligence to detect sophisticated attack vectors. AltFlex addresses this critical need by providing a proactive and adaptive solution for identifying and mitigating potential exploits using advanced AI/ML techniques.

Objectives

Primary Objective:

- Develop a functional AI-powered forensic framework (AltFlex) for automated exploit detection in DeFi and cross-chain environments.

Secondary Objectives:

- Implement machine learning models for anomaly detection and pattern recognition in transaction data.
- Create a user-friendly interface for visualizing forensic analysis results.
- Establish a comprehensive database of known exploit signatures and attack patterns.
- Evaluate the framework's effectiveness through rigorous testing and validation against real-world exploit scenarios.

Scope and Limitations

Initial Scope:

- Focus on exploit detection in Ethereum-based DeFi protocols and cross-chain bridges.
- Development of core AI/ML models for anomaly detection and signature matching.
- Implementation of a basic user interface for data visualization.

Future Enhancements:

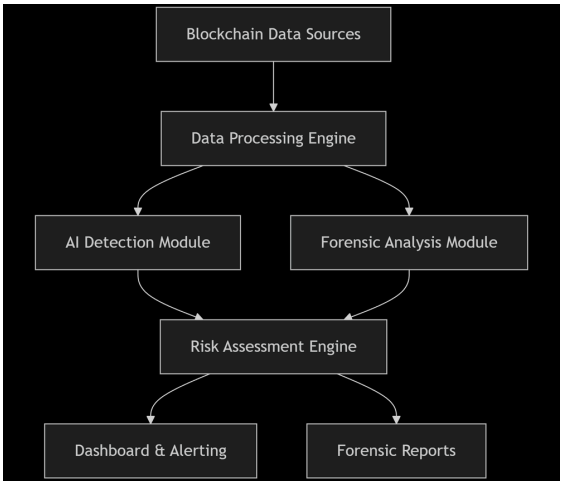
- Expansion to support other blockchain platforms (e.g., Binance Smart Chain, Polygon).
- Integration of advanced forensic analysis techniques (e.g., smart contract decompilation, symbolic execution).
- Development of automated incident response capabilities.

Methodology

The project will be executed in the following phases:

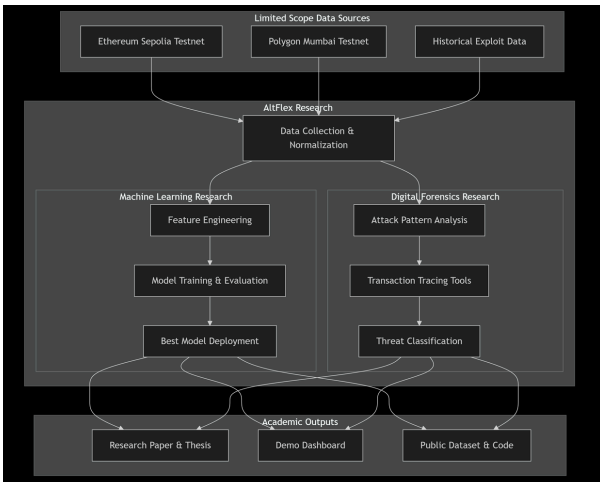
1. **Data Collection:** Gather historical transaction data, smart contract code, and exploit reports from various DeFi protocols and cross-chain bridges.
2. **Data Preprocessing:** Clean, transform, and normalize the collected data for use in machine learning models.
3. **Model Development:** Develop and train AI/ML models for anomaly detection, pattern recognition, and exploit signature matching.
4. **Framework Implementation:** Integrate the developed models into the AltFlex framework, including the user interface and data visualization components.
5. **Testing and Validation:** Evaluate the framework's performance against simulated and real-world exploit scenarios.
6. **Integration and Testing:** Deploy and test the implemented solution in sandboxed blockchain environments.

Technical Architecture



AltFlex will employ a modular architecture, comprising of data ingestion, preprocessing, AI/ML model training, exploit detection, alert generation, and visualization components. A central database will store transaction data, smart contract code, and exploit signatures. APIs will be used to facilitate communication between the different modules.

Realistic System Architecture



Expected Outcomes

Software Deliverables:

- A functional AI-powered forensic framework (AltFlex) for exploit detection.
- Machine learning models for anomaly detection and pattern recognition.
- A user-friendly interface for visualizing forensic analysis results.
- A comprehensive database of known exploit signatures and attack patterns.

Documentation Deliverables:

- Project report detailing the design, implementation, and evaluation of AltFlex.
- User manual for the AltFlex framework.
- Technical documentation for the developed AI/ML models.

Timeline (3-Month Sprint)

Week	Task	Deliverable
1-3	Data Collection & Preprocessing	Functional data collectors, labeled dataset v1
4-6	Model Development & Training	Trained models, basic forensic analysis scripts
7-9	Framework Integration & Testing	Working prototype, integrated system
10-12	Testing, optimization, documentation	Final deliverable, documentation package

Resource Requirements

Technical Resources:

- High-performance computing infrastructure for model training.
- Access to blockchain data APIs and forensic analysis tools.
- Cloud storage for data and model artifacts.
- Version control (Git/ GitHub)

Development Stack:

- Backend: Python, Web3.py, Solidity
- Frontend: Streamlit/Flask, React or Next.js (optional)
- Machine Learning Frameworks: TensorFlow, PyTorch
- Blockchain Platforms: Ethereum
- Data: PostgreSQL/MongoDB for transaction storage
- Infrastructure: Docker, AWS/Google Cloud or any alternative best choice

Significance and Innovation

Technical Contributions:

- Development of an AI-powered framework for automated exploit detection in DeFi and cross-chain environments.
- Advancement of machine learning techniques for anomaly detection and pattern recognition in blockchain data.
- Creation of a comprehensive database of known exploit signatures and attack patterns.

Academic Contributions:

- Publication of research papers in peer-reviewed conferences and journals.
- Presentation of project findings at academic workshops and seminars.
- Contribution to the growing body of knowledge on DeFi security and forensic analysis.

Risk Assessment

Risk	Probability	Impact	Mitigation Strategy
Data scarcity	Medium	Medium	Utilize data augmentation techniques and public datasets
Model overfitting	Medium	High	Implement regularization and cross-validation
Evolving attack vectors	High	High	Continuously update models and exploit database
Timeline delays	High	Medium	Agile development, prioritized MVP scope
Technical complexity	Medium	High	Prototype-first approach, expert consultation

Conclusion

AltFlex addresses a critical gap in Web3 security through an innovative combination of artificial intelligence and digital forensics. The proposed framework provides a foundation for proactive security monitoring and comprehensive incident analysis, with significant potential for academic contribution and real-world impact in securing decentralized ecosystems.

This proposal represents our planned approach based on current understanding. We anticipate that certain aspects may require refinement as we progress through development phases and encounter real-world implementation challenges.