SYNOPSIS

ON

“BitSecure: Hybrid Detection Model BitCoin Fraud”

Submitted in

Partial Fulfillment of requirements for the Award of Degree

of

Bachelor of Technology

In

Computer Science and Engineering

By

(Project Id: 26_CS_4C_04)

Divyansh Saxena (2201640100140)
Deepali Sachan (2201640100126)
Aseem Pradhan (2201640100091)
Aryan Katiyar (2201640100087)
Asmita Chaurasia (2201640100099)

Under the supervision of
Dr. Rohit Saxena
(Associate Professor)

Pranveer Singh Institute of Technology.
Kanpur - Agra - Delhi National Highway - 19
Bhauti -Kanpur - 209305.
(Affiliated to Dr. A.P.J. Abdul Kalam Technical University)

1. Introduction

The rapid growth of cryptocurrencies, particularly Bitcoin, has transformed global financial systems by enabling decentralized, borderless, and transparent digital transactions. However, with this rise, the frequency and sophistication of fraudulent activities have also increased significantly. Modern cybercriminals exploit blockchain anonymity to perform illegal transfers, money laundering, ransomware payments, scamming, and illicit marketplace interactions. These fraudulent transactions pose serious challenges to users, regulators, exchanges, and financial authorities.

Traditional fraud detection mechanisms rely on heuristic rules, signature-based matching, or manual inspection, which are insufficient for handling the scale, complexity, and evolving nature of blockchain fraud. The decentralized and pseudonymous structure of Bitcoin transactions makes fraud detection even more challenging, as transaction patterns often differ from conventional banking systems.

To address these challenges, **BitSecure** aims to build an advanced, data-driven, hybrid detection model that leverages the combined power of supervised machine learning and unsupervised anomaly detection techniques. The hybrid approach enhances detection capability by learning from labeled fraudulent transaction patterns while simultaneously identifying new and unknown anomalies through unsupervised modeling. By incorporating blockchain-specific metadata, graph-based features, transaction flow analysis, and ensemble prediction, the system provides improved accuracy, reduced false positives, and adaptive learning to tackle emerging fraud patterns.

The final solution will serve as an intelligent fraud detection system that can be deployed as a real-time API for cryptocurrency exchanges, financial institutions, and cybersecurity organizations. It aims to contribute to safer blockchain ecosystems and enhance trust among users and enterprises engaging in digital asset transactions.

2. Project Objective

The primary objectives of the project are:

1. To design a hybrid ensemble-based fraud detection model that integrates supervised learning algorithms with unsupervised anomaly detection techniques.
2. To analyze and extract key blockchain-specific features such as transaction amount, timestamps, address behavior, graph connectivity, and transaction propagation patterns.
3. To develop a scalable and accurate Bitcoin fraud detection system capable of identifying malicious, suspicious, and high-risk transactions.
4. To reduce false positives and improve detection precision using ensemble learning and adaptive model updates.
5. To implement real-time monitoring and create a deployable REST API for integration with financial services and crypto exchanges.
6. To contribute academically through a research paper highlighting the hybrid model, dataset preparation, methodology, and evaluation metrics.

3. Feasibility Study:

1. Technical Feasibility

The project is technically feasible as it utilizes widely-available machine learning libraries such as Python, Scikit-learn, TensorFlow/PyTorch, and blockchain datasets like the Elliptic Bitcoin Dataset. Cloud platforms like Google Colab and local systems provide adequate computational support.

2. Operational Feasibility

The model is designed to be user-friendly and easily deployable as an API. Financial institutions and exchanges can integrate it with minimal dependencies. The team has the required skillsets in ML, Python, and backend development.

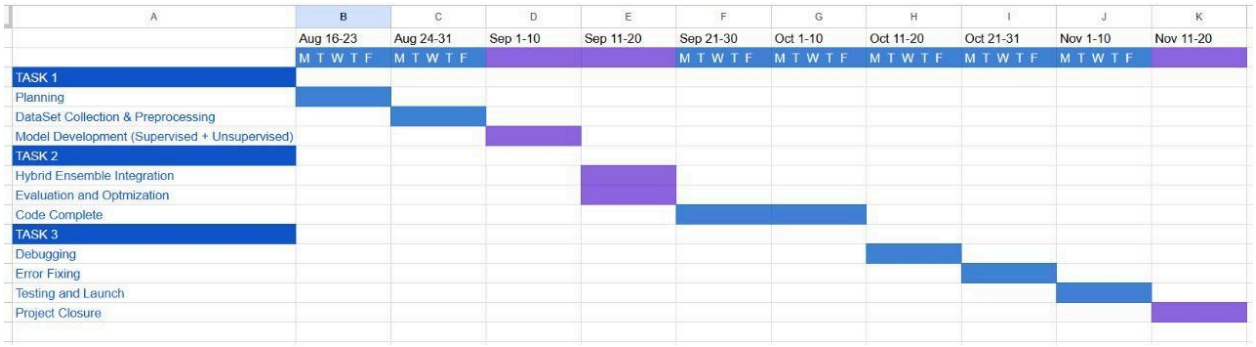
3. Economic Feasibility

   The project primarily uses open-source tools and cloud-based free GPU/CPU runtimes. No heavy financial investment is needed, making it cost-effective.

4. Legal Feasibility

   The project complies with open-source datasets and does not involve unauthorized blockchain node operations. It maintains data ethics and privacy standards.

Start Date: 16-Aug-2025 **End Date: 20-Nov-2025.**



4. Methodology/ Planning of work

The methodology consists of the following major stages:

1. Data Collection

- Collect Bitcoin transaction datasets (Elliptic Dataset, Kaggle sources, blockchain metadata).
- Extract relevant blockchain features such as transaction IDs, addresses, amount flow, timestamps, and graph-connected components.

2. Data Preprocessing

- Cleaning, normalization, removing missing values
- Feature engineering (behavioral + statistical + graph-based features)

- Label mapping for supervised learning

3. Model Development

- **Supervised Models**: Random Forest, XGBoost, Logistic Regression
- **Unsupervised Models**: Isolation Forest, LOF, Autoencoder
- Combine predictions using a weighted hybrid ensemble for improved reliability.

4. System Architecture

User/API → Transaction Processor → Feature Extractor → Hybrid ML Model → Risk Score/Prediction → Dashboard/Alerts

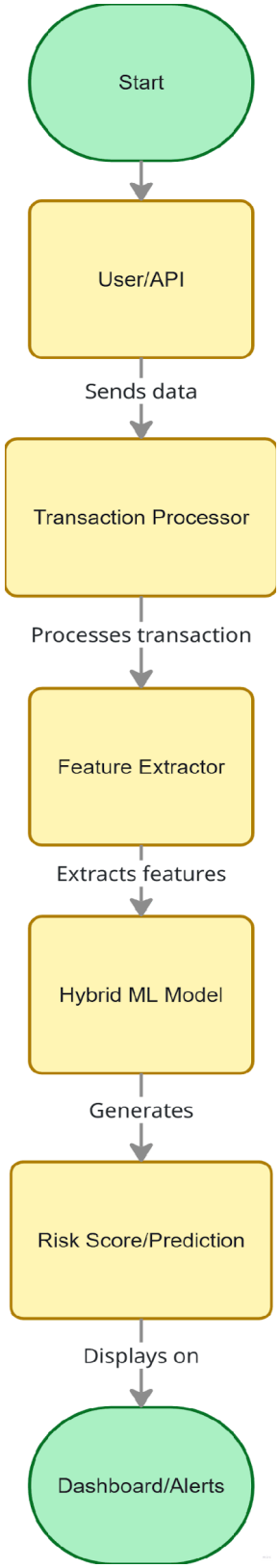
5. Model Evaluation

- Metrics: Accuracy, Recall, ROC-AUC, F1-Score, Precision, Confusion Matrix
- Compare single models with hybrid ensemble performance

6. Deployment

- Build REST API using Flask/FastAPI
- Real-time scoring: The system returns “Legit / Suspicious / Fraudulent” with confidence score

FlowChart


Start
User/API
Sends data
Transaction Processor
Processes transaction
Feature Extractor
Extracts features
Hybrid ML Model
Generates
Risk Score/Prediction
Displays on
Dashboard/Alerts

5. Tools/Technology Used:

5.1 Minimum Hardware Requirements

- **CPU:** Intel Core i3/i5 or AMD Ryzen 3/5
- **RAM:** Minimum 4 GB (8 GB recommended)
- **GPU:** Optional, but recommended for deep learning
- **Storage:** 256 GB SSD (512 GB preferred)
- **Others:** Stable internet connection for cloud training

5.2 Minimum Software Requirements

- **OS:** Windows 10/11 or Ubuntu 20.04+
- **Programming Language:** Python 3.10+
- **Libraries/Tools:**
    - TensorFlow / PyTorch
    - Scikit-learn
    - Pandas, NumPy
    - Matplotlib, Seaborn
    - FastAPI / Flask
    - Jupyter Notebook, VS Code, Google Colab
- **Database:** PostgreSQL/MySQL, MongoDB (if needed)
- **Deployment Tools:** Docker (optional), REST APIs

6. References: [IEEE format]:

- M. Weber et al., “Anti-Money Laundering in Bitcoin: Analyzing the Elliptic Dataset,” *IEEE International Conference on Data Mining*, 2019.
- Elliptic.co, “Elliptic Bitcoin Transaction Dataset,” 2020.
- S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
- X. Li and C. Wang, “The Technology and Economic Determinants of Cryptocurrency Exchange Rates,” *Decision Support Systems*, 2017.
- H. Moore, “Anomaly Detection Techniques in Financial Transactions,” *IEEE Transactions on Knowledge and Data Engineering*, 2021.