MACHINE LEARNING IN MONEY LAUNDERING DETECTION OVER BLOCKCHAIN TECHNOLOGY

Saddi Gopagari Varsha, T Radhika
M.Tech Student, Assistant Professor
Department of Computer Science and Engineering
Brilliant Institute of Engineering & Technology, Abdullapur (V), Abdullapurmet (M), Rangareddy (D), Hyderabad - 501 513
radhika.vyshu@gmail.com

Abstract Layering through cryptocurrency transactions represents a sophisticated mechanism for laundering money within cybercrime circles. This process methodically merges illegal funds into the legitimate financial system. Blockchain technology plays a crucial role in this integration by facilitating the quick and automated dispersal of assets across various digital wallets and exchanges. Machine learning emerges as a powerful tool for analyzing and identifying illicit transactions within Blockchain networks; however, a significant challenge remains in the form of a gap in advanced pattern recognition algorithms. This paper introduces a novel machine learning-based approach called Value-driven-Transactional tracking Analytics for Crypto compliance (VTAC) for the detection of illegal crypto transactions via Blockchain. The approach combines machine learning algorithms with a pre-training process, normalization, model training, and a de-anonymization process to analyze and identify illicit transactions effectively. Experimental evaluations show VTAC's capability to detect illegal transactions with a 97.5% accuracy using the XG Boost model, outperforming existing methods with an accuracy of up to 95.9%.Key performance metrics, including precision, recall, and F1-score, consistently exceeded 95%, highlighting VTAC's enhanced precision and reliability. The proposed solution will serve as an advisory framework to help financial crime investigators enhance the detection and reporting of suspicious cryptocurrency transactions in cyberspace.

INTRODUCTION

Cryptocurrency has become a popular medium for financial transactions due to its decentralization and anonymity. However, these features are exploited by cybercriminals for money laundering activities. Transaction layering is a sophisticated laundering technique used to obscure illegal fund flows. Traditional monitoring systems struggle to detect such patterns. Machine learning offers promising solutions for blockchain analytics. This project introduces VTAC, a machine learning-based framework for crypto compliance. The framework integrates preprocessing, normalization, model training, and de-anonymization. Blockchain transaction data is analyzed to identify illicit activities. XGBoost is used for its high predictive capability. Experimental results demonstrate superior detection accuracy. VTAC achieves 97.5 percent accuracy, outperforming existing methods. Precision, recall, and F1-score exceed 95 percent. The system effectively distinguishes illegal transactions. The framework supports financial crime investigations. It provides advisory insights for reporting suspicious activities. The methodology is systematic and reproducible. The project addresses gaps in advanced pattern recognition. It improves blockchain transparency. The approach enhances

regulatory compliance. The framework is scalable and adaptable. It integrates machine learning with blockchain forensics. The study contributes to crypto crime detection research. The system reduces investigation effort. It improves detection reliability. The framework aids decision-making. Overall, the project presents a robust solution for detecting illegal crypto transactions.

The primary objective of this project is to design an advanced machine learning-based framework for detecting illegal cryptocurrency transactions within blockchain networks. The project aims to address the problem of money laundering through transaction layering. It focuses on identifying illicit fund flows that are hidden within legitimate cryptocurrency transactions. The VTAC framework is proposed to enhance crypto compliance and forensic analysis.

Machine learning models are used to recognize complex transaction patterns. Pre-training and normalization techniques are applied to improve learning accuracy. The project aims to achieve high detection precision and reliability. XGBoost is used to optimize classification performance. Reducing false positives and false negatives is a key objective. The system supports financial crime investigators. It assists in regulatory compliance. The framework aims to improve transparency in blockchain transactions. Automation of detection processes is emphasized. The approach enhances cybercrime investigation capabilities. Overall, the project seeks to strengthen cryptocurrency fraud detection mechanisms.

PROJECT SCOPE

This project focuses on detecting illegal cryptocurrency transactions using blockchain analytics and machine learning. It analyzes transaction layering techniques used in money laundering. The scope includes collecting blockchain transaction data. Data preprocessing, normalization, and feature extraction are performed. The VTAC framework integrates machine learning with de-anonymization processes. The project implements models such as XGBoost for classification. Performance is evaluated using accuracy, precision, recall, and F1-score. The system operates in an offline analytical environment. Real-time blockchain monitoring is not included. The framework focuses on supervised learning. The scope includes comparative analysis with existing methods. Scalability for large transaction graphs is considered. Privacy and ethical handling of data are assumed.

The framework supports crypto compliance efforts. The project contributes to blockchain forensics research. Visualization is not a primary focus. The scope includes model training and evaluation. Deployment aspects are not covered. The framework is adaptable to different cryptocurrencies. The project focuses on transaction-level analysis. Network-level extensions are excluded. The system supports investigators and analysts. The project emphasizes detection accuracy. The framework aids regulatory reporting. The study enhances financial crime analytics. The project includes documentation and result interpretation. The scope is research-oriented. The framework supports advisory decision-making. The system improves cybercrime detection efficiency.

EXISTING SYSTEM

Existing systems rely on heuristic rules and basic analytics. Limited machine learning models are used. Detection accuracy is moderate. De-anonymization is insufficient. Systems are often reactive.

Disadvantages

1. Limited ability to detect complex layering patterns.
2. Lower detection accuracy.
3. High false negative rates.
4. Lack of advanced analytics.

PROPOSED SYSTEM

The proposed system introduces the VTAC framework. Machine learning models analyze blockchain transactions. Preprocessing and normalization improve learning. De-anonymization enhances traceability. XGBoost improves detection accuracy.

Advantages

1. High detection accuracy.
2. Improved precision and recall.
3. Effective detection of layered transactions.
4. Supports financial crime investigation.

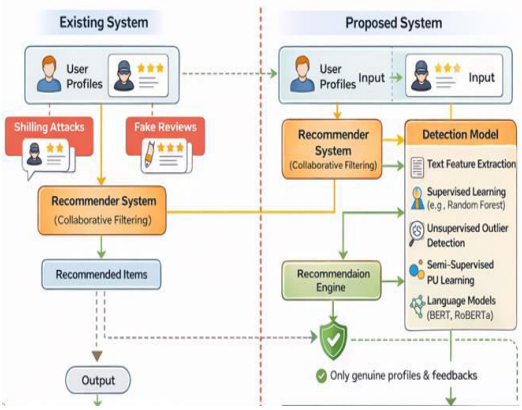
HARDWARE REQUIREMENTS

Processor	:	i3 or higher
Speed	:	2.9 GHz
RAM	:	4 GB (min)
Hard Disk	:	160 GB

4. SOFTWARE REQUIREMENTS

- **Operating system :** Windows 7 Ultimate
- **Coding Language :** Python
- **Back-End :** Django-ORM
- **Designing :** Html, css, javascript
- **Data Base :** MySQL (WAMP Server)

SYSTEM ARCHITECTURE



System Architecture

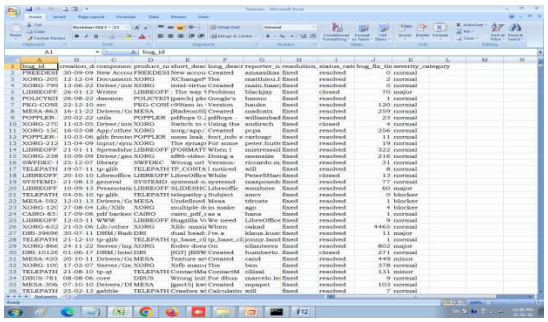
Algorithm used

The system follows blockchain data collection, preprocessing, normalization, feature extraction, machine learning model training, de-anonymization, and evaluation steps.

Algorithm techniques

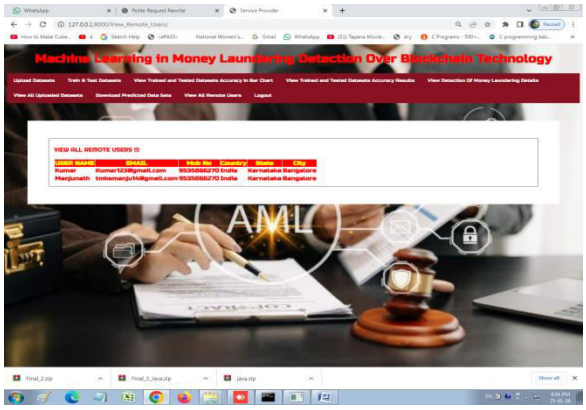
The project employs supervised machine learning techniques. XGBoost is used for classification. Data normalization improves convergence. Pre-training enhances learning efficiency. De-anonymization strengthens investigative insights.

RESULTS AND ANALYSIS

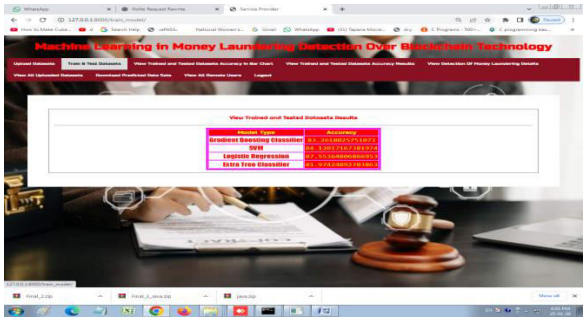


Data Sets

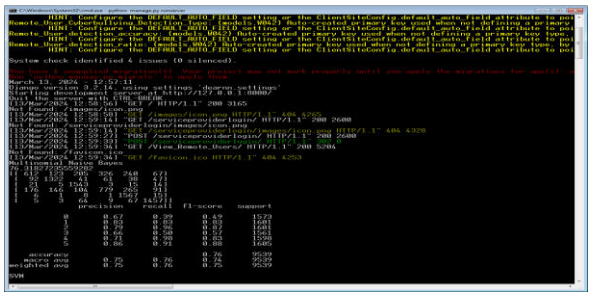
Home Page



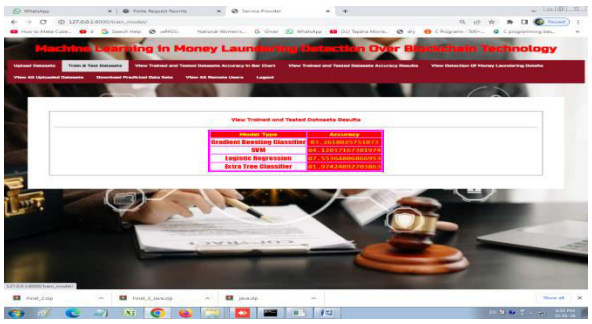
Login Page



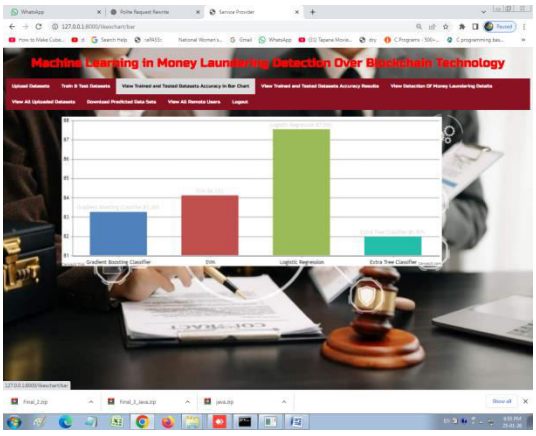
Admin Menu Operations



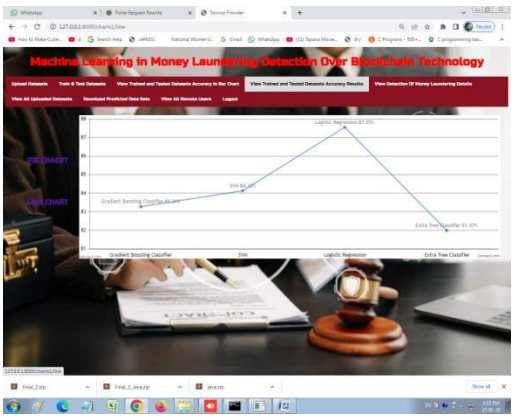
Ml Accuracy Charts



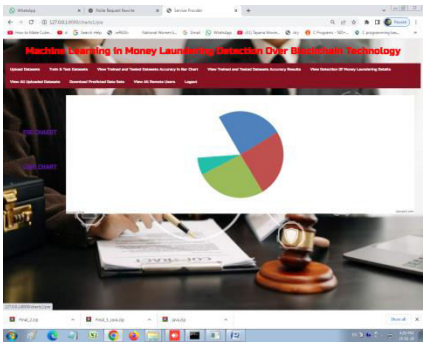
ML Accuracy



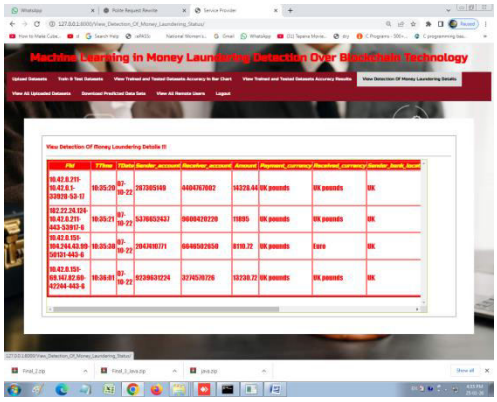
Graph Showing Ml Accuracy



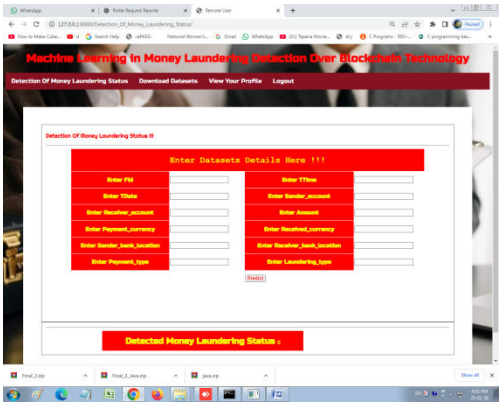
Line Graph Showing Ml Accuracy



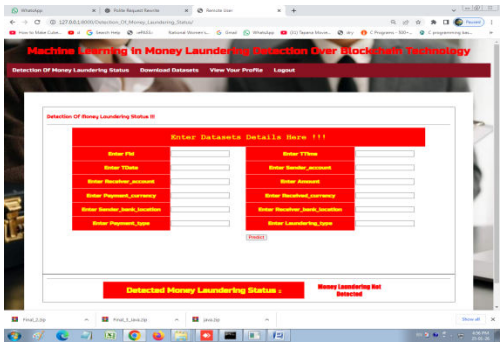
Pie Graph Showing Ml Accuracy



List of Fares with Status



Prediction of Claims



Prediction Results

CONCLUSION

This project presents VTAC, a novel framework for detecting illegal cryptocurrency transactions. By combining machine learning with blockchain analytics, the system effectively identifies illicit activities. XGBoost delivers superior accuracy of 97.5 percent. Precision, recall, and F1-score exceed 95 percent. The framework outperforms existing methods. VTAC addresses complex transaction layering patterns. De-anonymization enhances investigation capabilities. The system supports financial crime analysts. It improves regulatory compliance. The methodology is scalable and robust. Automation reduces manual effort. The framework enhances transparency. The study contributes to blockchain security research. It strengthens cybercrime detection. The approach is adaptable. The framework supports advisory decision-making. The results validate effectiveness. The project improves crypto compliance strategies. Overall, VTAC offers a reliable solution for detecting illegal crypto transactions.

REFERENCES

[1] M. A. Jamil, M. Arif, N. S. A. Abubakar, and A. Ahmad, ‘‘Software testing techniques: A literature review,’’ in Proc. 6th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M), Nov. 2016, pp. 177–182.

[2] W. Y. Ramay, Q. Umer, X. C. Yin, C. Zhu, and I. Illahi, ‘‘Deep neural network-based severity prediction of bug reports,’’ IEEE Access, vol. 7, pp. 46846–46857, 2019.

[3] W. Wen, ‘‘Using natural language processing and machine learning techniques to characterize configuration bug reports: A

study,'' M.S. thesis, College Eng., Univ. Kentucky, Lexington, KY, USA, 2017.
[4] J. Polpinij, ''A method of non-bug report identification from bug report repository,'' Artif. Life Robot., vol. 26, no. 3, pp. 318–328, Aug. 2021.
[5] S. Adhikarla, ''Automated bug classification.: Bug report routing,'' M.S. thesis, Fac. Arts Sci., Dept. Comput. Inf. Sci., Linköping Univ., Linköping, Sweden, 2020.
[6] K. C. Youm, J. Ahn, and E. Lee, ''Improved bug localization based on code change histories and bug reports,'' Inf. Softw. Technol., vol. 82, pp. 177–192, Feb. 2017.
[7] N. Safdari, H. Alrubaye, W. Aljedaani, B. B. Baez, A. DiStasi, andM. W. Mkaouer, ''Learning to rank faulty source files for dependent bug reports,'' in Proc. SPIE, vol. 10989, 2019, Art. no. 109890B.
[8] A. Kukkar, R. Mohana, A. Nayyar, J. Kim, B.-G. Kang, and N. Chilamkurti, ''A novel deep-learning-based bug severity classificationtechnique using convolutional neural networks and random forest with boosting,'' Sensors, vol. 19, no. 13, p. 2964, Jul. 2019.
[9] A. Aggarwal. (May 2020). Types of Bugs in Software Testing: 3 Classifications With Examples. [Online]. Available: https://www.scnsoft.com/software-testing/types-of-bugs
[10] A. Kukkar and R. Mohana, ''A supervised bug report classification with incorporate and textual field knowledge,'' Proc. Comput. Sci., vol. 132, pp. 352–361, Jan. 2018.