



AN ANALYSIS OF FINANCIAL RISK MANAGEMENT OF CRYPTO CURRENCY MARKET USING HRP MACHINE LEARNING ALGORITHM

¹Damarasingu Bindu Sai Sri, ²Dr K Srinivas,

, ³Mrs.D Lakshmi Prasanna, ⁴Mr.B Srinivas.

¹PG Scholar, ²Professor, ³Assistant Professor, ⁴Associate Professor

^{1,2,3,4}Computer Science and Engineering,

^{1,2,3,4}Bonam Venkata Chalamayya Institute of Technology and Science(A), Amalapuram, India

Abstract : Crypto currency is one of the famous financial state in all over the world which cause several type of risks that effect on the intrinsic assessment of risk auditors. From the beginning the growth of crypto currency gives the financial business with the wide risk in term of presentation of money laundering. In the institution of financial supports such as anti-money laundering, banks and secrecy of banks proceed as a specialist of risk, manager of bank and officer of compliance which has a provocation for the related transaction through crypto currency and the users who hide the illegal funds In this study, the Hierarchical Risk Parity and unsupervised machine learning applied on the crypto currency framework. The process of professional accounting in term of inherent risk connected with crypto currency regarding the occurrence likelihood and statement of financial impact. Determining crypto currency risks comprehended to have a high rate of occurrence likelihood and the access of private key which is unauthorized. The professional crypto currency experience in transaction cause the lower risk comparing the less experienced one. The Hierarchical Risk Parity gives the better output in term of returning the adjusted risk tail to get the better risk management result. The result section shows the proposed model is robust to various intervals which are re-balanced and the co-variance window estimation.

IndexTerms: Crypto currency, money laundering, provocation, private key, Hierarchical Risk Parity. E-Pilot, Hard Landing Prediction, Soft Landing, Flight Safety, Logistic Regression, Data Preprocessing, TensorFlow.

I. Introduction

Crypto currency has become an integral part of the global financial system, offering a decentralized alternative to traditional banking. However, its rapid growth has introduced significant risks, particularly in areas such as money laundering, unauthorized access, and transaction anonymity. Financial institutions, including banks and anti-money laundering agencies, face increasing challenges in monitoring and regulating cryptocurrency transactions due to the lack of centralized control. Users who engage in illegal activities can exploit the decentralized nature of cryptocurrency, making it difficult for auditors and compliance officers to track illicit funds. This project focuses on addressing these concerns by applying Hierarchical Risk Parity (HRP) and unsupervised machine learning techniques to analyze and manage the risks associated with crypto currency transactions.

The financial market is inherently complex, and crypto currency further adds to this complexity with its decentralized and volatile nature. Traditional financial models struggle to account for the risks associated with digital assets, making it necessary to develop new frameworks for risk management. HRP offers a solution by optimizing portfolio allocation while reducing the impact of extreme risk fluctuations. This paper examines the effectiveness of HRP in crypto currency risk assessment and explores how machine learning techniques can help identify high-risk transactions, unauthorized access, and potential security breaches. By leveraging these methodologies, the study aims to provide a structured approach to managing the uncertainties associated with crypto currency investments.

By implementing HRP and machine learning techniques, this project aims to enhance the security and reliability of crypto currency transactions. The findings will contribute to better risk management strategies, improved financial oversight, and a more structured approach to auditing digital assets. The results of the study will help financial professionals and institutions develop more effective policies to mitigate risks and ensure compliance with regulatory standards in the evolving crypto currency landscape.

II. Background and Literature Review

1. November 2017-ResearchGate's Introduction of ML-Based Risk Prediction Models

In November 2017, Research Gate introduced an early machine learning-based risk management system for analyzing financial risks in the crypto currency market. This system utilized Support Vector Machines (SVM) to classify market conditions as high-risk or low-risk based on historical trading data, volatility levels, and investor sentiment. The primary advantage of this system was its ability to detect potential market crashes by identifying unusual trading patterns and sudden price fluctuations. By leveraging SVM's ability to find optimal decision boundaries, the system provided a structured and data-driven approach to financial risk management.

2. February 2022 - Nile Journal's Introduction of Naïve Bayes for Crypto currency Risk Prediction.

In February 2022, the Nile Journal of Communication and Computer Science introduced a Naïve Bayes-based financial risk analysis system that utilized probability-based classification to detect high-risk investment periods. By considering historical returns, market sentiment, and volatility indices, Naïve Bayes calculated the likelihood of a market downturn or price spike.

A key benefit of this approach was its ability to handle real-time risk assessments with minimal computational overhead, making it a practical solution for high-frequency trading. However, a major limitation of Naïve Bayes was its strong independence assumption, which rarely holds in financial markets where price movements are influenced by multiple interdependent factors such as market news, investor sentiment, and economic policies. To improve model accuracy, researchers proposed Bayesian Network enhancements or hybrid models combining Naïve Bayes with Deep Learning to better capture complex dependencies.

3. March 2023 - IRJMETS' Introduction of Hybrid ML-Based Risk Analysis for Crypto currencies.

In March 2023, the International Research Journal of Modernization in Engineering, Technology, and Science (IRJMETS) introduced an automated crypto currency risk management system that combined multiple machine learning algorithms, including Decision Trees, Logistic Regression, and SVM. This system provided comprehensive risk assessments by analysing past market fluctuations and identifying potential financial threats using a hybrid model approach.

However, despite its effectiveness, the system had a key drawback—its sensitivity to large datasets and non-linear relationships. Since SVM works best with a clear margin between classes, highly volatile crypto currency price movements often led to misclassification. Additionally, computational inefficiencies made it challenging to apply SVM to real-time crypto currency trading environments. To address these issues, researchers recommended enhancements such as kernel-based SVM for non-linear decision-making and integration with real-time market feeds to improve the predictive accuracy of risk classification.

III. Proposed Methodology

The proposed system aims to provide a comprehensive approach to analysing cryptocurrency related risks, particularly in the context of professional accounting and financial statements.

By Evaluating the associated risks of cryptocurrency investments, the system helps financial analysts and investors understand the potential impact on financial reporting. Unlike existing models that struggle with accuracy and reliability, this system employs advanced methodologies to identify and quantify risks, ensuring a more precise risk assessment. By integrating financial accounting principles, the system enables users to make informed decisions based on a deeper understanding of the intrinsic risks tied to cryptocurrency markets.

One of the key features of the proposed system is its ability to detect intrinsic risks that exhibit negative correlations with cryptocurrency trends. This means the system can identify hidden factors that contribute to market volatility and help investors mitigate potential losses. Additionally, it categorizes security risks associated with cryptocurrency exchanges based on the likelihood of their occurrence. By ranking exchanges according to their risk levels, investors can make safer choices and avoid platforms prone to hacking, fraud, or operational failures. This feature enhances transparency and improves security within the cryptocurrency trading ecosystem.

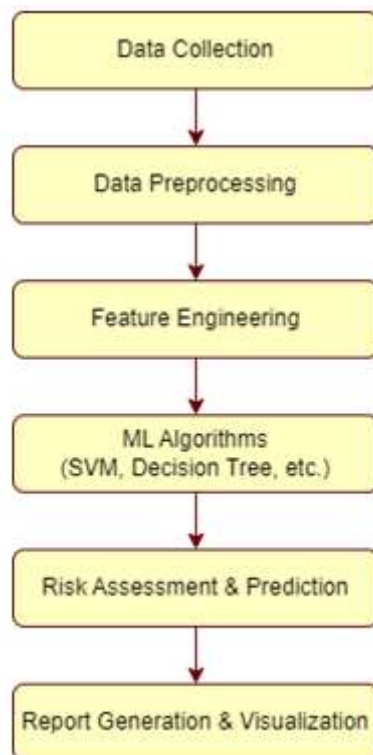


figure1: System Architecture of ML based Cryptocurrency Risk Management

The system architecture for Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management follows a structured workflow. It starts with Data Collection, where historical and real-time cryptocurrency data is gathered from exchanges, news sources, and market trends. Next, Data Preprocessing cleans and organizes the data by handling missing values, normalizing values, and removing inconsistencies. Then, Feature Engineering selects key market indicators like price trends, trading volume, and sentiment scores to improve model accuracy. The ML Algorithms (such as SVM, Decision Tree, and Logistic Regression) analyze this data to detect patterns and predict market risks. In the Risk Assessment and Prediction phase, the system categorizes risk levels (low, medium, high) and forecasts potential market fluctuations. Finally, Report Generation and Visualization presents these insights through charts, dashboards, and automated reports, helping investors make informed decisions.

IV Modules:

A module is a self-contained unit of a system that performs a specific function. In software development, a module is an independent component that can be developed, tested, and maintained separately while interacting with other modules. Modules help in organizing code, improving reusability, and simplifying debugging. They can include different functionalities such as user authentication, database management, or report generation. By dividing a system into modules, it becomes easier to manage and scale, making the overall system more efficient and maintainable. Different Modules in Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management.

The system is designed with various modules that work together to analyze financial risks in the cryptocurrency market using machine learning techniques. The primary modules in the system are:

1. Admin Module
2. User Dashboard Module

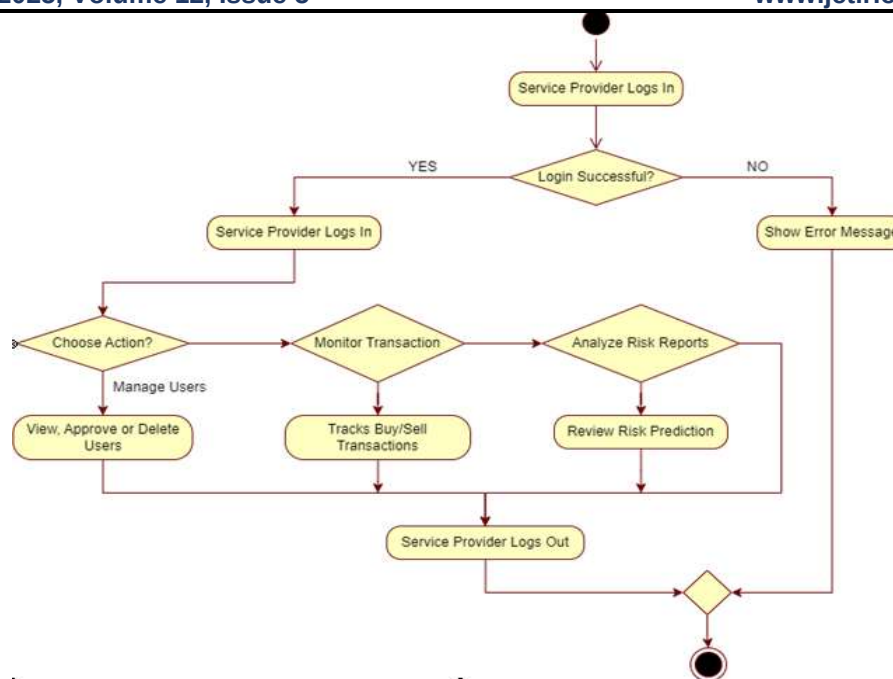


figure2: Admin module

V. Risk Prediction

Enter your crypto currency data and click on “Predict”. It will find if there is any risk or not. If it finds a risk, it will show “NO RISK FOUND”. Here service provider can monitor all user data and prediction and observe the accuracy by using given algorithms.



figure3: Accuracy Bar Chart



figure4: Accuracy Pie Chart

VI Conclusion

The Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management provides an efficient and data-driven approach to assessing financial risks in the volatile cryptocurrency market. By leveraging machine learning algorithms such as SVM, Decision Tree, and Logistic Regression, the system enhances risk prediction accuracy, helping investors and financial analysts make informed decisions. The automated nature of the system reduces manual analysis efforts, improves risk assessment efficiency, and ensures real-time monitoring of market trends. With its ability to process large volumes of financial data, identify potential risks, and generate

insightful visualizations, this system plays a crucial role mitigating investment risks and enhancing financial decision-making.

VII. References

- [1] CoinDesk, "How Cryptocurrency Volatility Affects Risk Management," www.coindesk.com/article Accessed on March 16, 2025. Investopedia, "Understanding Crypto Risk Models," www.investopedia.com, Accessed on March 16, 2025.
- [2] Binance Research, "2024 Crypto Risk Index: Trends & Insights", Binance Whitepaper, January 2024.
- [3] Lohre, H., Rother, M., & Schafer, R. (2019). Hierarchical Risk Parity: Accounting for Tail Dependencies in Multi-Asset Multi-Factor Allocations. SSRN.
- [4] **K Srinivas** et al "Computational approach to overcome overlapping of clusters by fuzzy k-means" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018
- [5] **Lorenzo, L., & Arroyo, J. (2023).** *Online Risk-Based Portfolio Allocation on Subsets of Crypto Assets Applying a Prototype-Based Clustering Algorithm*. Financial Innovation, 9(25).
- [6] **Jiang, Z., & Liang, J. (2016).** *Cryptocurrency Portfolio Management with Deep Reinforcement Learning*. arXiv.
- [7] **Meem, A. T. (2024).** *A Deep Learning Approach to Predict the Fall of Cryptocurrency Prices Long Before Its Actual 77 Fall*. arXiv.
- [8] **Shahbazi, Z., & Byun, Y. (2022).** *Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management*. IEEE Access.
- [9] **Srinivas K** et al, "Principles of Software Engineering for the Cost-Effective Prevention of Type 2 Diabetes (T2D)" International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, 2023, pp. 489–492.
- [10] **Ni, X., Härdle, W. K., & Xie, T. (2020).** *A Machine Learning Based Regulatory Risk Index for Cryptocurrencies*. arXiv.
- [11] **Indrabayu, T., Irianty, R., & Sidehabi, S. W. (2024).** *Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management*.
- [12] **Zhang, Y., & Wang, J. (2025).** *An Integrated Framework for Cryptocurrency Price Forecasting and Anomaly Detection Using Machine Learning*. Applied Sciences.