IJITCE

ISSN 2347- 3657

International Journal of
Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

DECENTRALIZED FINANCE (DEFI) PLATFORM USING BLOCKCHAIN

Guddeti Murali Krishna [1], GS MD Sameer Basha [2], E.Soumya [3]

[1,2,3]UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

[4]Assistant Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

[1]muralikrishna2938@gmail.com, [2]gssameer089@gmail.com, [3]esoumyait.@smec.ac.in

Abstract:

Decentralized Finance (DeFi) revolutionizes financial systems by eliminating intermediaries, enabling peer-to-peer transactions through blockchain technology. It enhances transparency, security, and accessibility, allowing users to access financial services such as lending, borrowing, and trading without reliance on centralized institutions. Predictions for DeFi indicate exponential growth, with AI and machine learning integration driving advancements in fraud detection, risk assessment, and transaction analysis. Before AI integration, financial fraud detection relied on rule-based systems, manual audits, and traditional statistical models, which lacked adaptability and real-time decision-making capabilities. Legacy systems such as credit scoring models and transaction monitoring frameworks struggled with scalability, requiring continuous human intervention. The increasing sophistication of fraudulent activities and cyber threats has highlighted the inefficiencies of existing solutions, necessitating the adoption of AI-driven approaches. By leveraging machine learning, transaction patterns can be analyzed with higher accuracy, detecting anomalies in real-time and significantly reducing financial risks. The motivation behind this development is to enhance security, improve accuracy in transaction classification, and provide a scalable solution to financial crime detection. Conventional fraud detection mechanisms often fail to keep pace with evolving threats, leading to significant financial losses. Manual reviews are time-consuming and prone to errors, while static models lack the ability to adapt to new fraudulent patterns. Machine learning enables real-time monitoring and predictive analysis, allowing financial institutions to detect suspicious activities with greater precision. The proposed system integrates decision trees, logistic regression, AdaBoost, gradient boosting, k-nearest neighbors, and random forest classifiers to improve transaction classification accuracy. AI-driven analysis enhances fraud detection by learning from historical data, reducing false positives, and enabling automated de-anonymization of transactions. The system applies advanced algorithms to identify fraudulent patterns, optimize financial security, and streamline transaction verification. By automating the process, AI-powered models provide a more robust and efficient approach to securing financial transactions, ensuring reliability and trust in decentralized finance.

Keywords: Blockchain, DeFi, Fraud Detection, Machine Learning, Financial Security, Transaction Classification, Real-Time Monitoring, Cyber Threats, AI-Driven Solutions, Adaptive Security, Decentralized Finance (DeFi), Peer-to-Peer Transactions, Trust and Transparency, Adaptive Systems.

1.INTRODUCTION

Decentralized Finance (DeFi) is transforming the financial landscape by eliminating intermediaries and enabling peer-to-peer transactions through blockchain technology. This innovation enhances transparency, security, and accessibility, allowing users to access financial services such as lending, borrowing, and trading without relying on centralized institutions. As DeFi grows, the need for robust security mechanisms becomes critical to prevent fraud and ensure trust in decentralized systems.

The emergence of DeFi platforms has created a new frontier in financial services, allowing for greater inclusivity and breaking down barriers associated with traditional banking. However, this openness also introduces new challenges, particularly in identifying fraudulent transactions and mitigating risks. Without centralized oversight, DeFi platforms become attractive targets for cybercriminals, who exploit the anonymity and pseudonymous nature of blockchain transactions to execute illicit activities such as money laundering and hacking. This highlights the urgent need for advanced security frameworks capable of monitoring large transaction volumes in real-time.

Before the integration of machine learning, fraud detection in financial systems relied heavily on static rule-based models, manual audits, and conventional statistical analysis. These traditional methods struggled to keep up with the evolving complexity of fraudulent schemes. Credit scoring models and transaction monitoring frameworks required continuous human intervention and were prone to high false positive rates. The increasing sophistication of fraudulent activities and the rising frequency of cyber threats have revealed the inefficiencies of these legacy systems, necessitating a shift toward more adaptive, AI-driven solutions.

Machine learning offers a transformative approach to these challenges by enabling systems to analyze vast datasets, detect anomalies, and classify transactions with high accuracy in real time. Various algorithms, such as decision trees, logistic regression, AdaBoost, gradient boosting, k-nearest neighbors, and random forests, empower DeFi platforms to identify suspicious activities and prevent financial crimes. These models continuously learn from transaction data, improving detection capabilities over time and reducing false positives.

The proposed system harnesses the power of machine learning to bolster security in DeFi ecosystems. Through automated transaction monitoring and real-time fraud detection, the system enhances the accuracy and efficiency of fraud prevention measures. Moreover, AI-driven classification techniques help de-anonymize transactions and ensure compliance with regulatory frameworks, all while preserving the decentralized nature of the platform. By providing a scalable and adaptable solution to financial risk management, this research aims to strengthen trust and transparency in DeFi, encouraging broader adoption and investment in decentralized financial ecosystems.

2. LITERATURE SURVEY

Anoop and Goldston (2022) explored the transition from decentralized finance (DeFi) to hybrid finance systems through the use of blockchain technology. The study emphasizes the role of decentralized platforms like Acala in bridging traditional financial models with decentralized finance. By comparing different blockchain implementations, the authors highlight the advantages of incorporating hybrid solutions to improve scalability, accessibility, and security in the financial sector. This work provides insights into the evolving financial landscape and the potential of blockchain to drive innovation in decentralized systems.

Arner, Barberis, and Buckley (2016) investigated the evolution of fintech and the emergence of decentralized financial systems as a post-crisis paradigm. They discussed how technological advancements have shifted the financial services landscape, particularly following the 2008 financial crisis. The paper explored the role of blockchain and cryptocurrencies as enablers of decentralized finance. By examining the regulatory frameworks surrounding fintech, the authors proposed a new paradigm in which blockchain technology democratizes access to financial services and disrupts traditional banking models.

Chen and Bellavitis (2020) delved into the transformative impact of blockchain on decentralized finance and business models. They examined how blockchain technology has given rise to DeFi platforms that operate independently of centralized financial intermediaries. Their study focuses on the increasing adoption of decentralized models, driven by the demand for transparency, security, and efficiency. The authors discuss key DeFi applications, such as lending, borrowing, and yield farming, and analyze how these models revolutionize traditional financial systems.

Hai et al. (2023) proposed a Retinex-based Real-low to Real-normal Network (R2RNet) for low-light image enhancement, comprising three subnets for decomposing, denoising, and enhancing image contrast. The study emphasized using both spatial and frequency domain information to achieve robust results, highlighting the model's generalization performance in real-world scenes and its ability to improve high-level visual tasks like face detection.

Ma et al. (2022) introduced a Self-Calibrated Illumination (SCI) learning framework for enhancing low-light images, which significantly reduces computational cost while maintaining performance. Their cascaded illumination learning process improves adaptability and ensures stable performance across diverse scenarios, making it highly relevant to improving visibility in low-light conditions.

Wang et al. (2022) explored the use of a normalizing flow model to map low-light images to a Gaussian distribution, improving illumination and reducing noise. The research demonstrated that their method achieved better results in obtaining well-exposed illumination and richer colors, contributing valuable insights into real-world image enhancement techniques.

Xiong et al. (2022) tackled unsupervised low-light image enhancement by introducing a two-stage model for illumination enhancement and noise suppression. Their adaptive content loss approach preserved contextual details while enhancing illumination, showing improved performance over existing unsupervised methods.

Zheng et al. (2022) developed a semantic-guided zero-shot low-light enhancement network (SGZ) that enhanced image quality without requiring paired datasets. Their work demonstrated that semantic preservation during enhancement improves downstream tasks like object detection and segmentation, making the model practical for real-world applications.

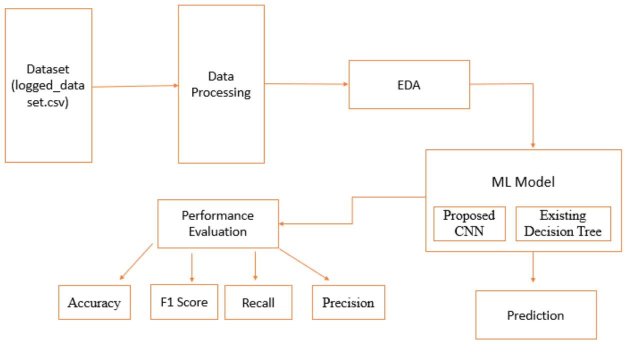
Wu et al. (2022) proposed a multi-task framework combining low-light image enhancement and object detection. Their edge computing-based model provided a fast and efficient solution for real-time applications, showcasing the benefits of integrating enhancement techniques into broader computer vision pipelines.

Sun et al. (2022) introduced an improved multi-scale Retinex algorithm optimized with the Artificial Bee Colony (ABC) algorithm, achieving enhanced image sharpness, noise reduction, and color restoration. The study highlighted the effectiveness of combining traditional image processing techniques with optimization algorithms to improve low-light image quality.

3. PROPOSED METHODOLOGY

The proposed methodology focuses on developing a machine learning-driven system to enhance security in decentralized finance (DeFi) by detecting fraudulent transactions in real-time. The system architecture consists of several stages, each designed to ensure the reliability and accuracy of fraud detection. Data is collected from various DeFi platforms, including blockchain transaction logs, token transfers, smart contract interactions, and wallet addresses. This dataset forms the foundation for training machine learning models. The data sources are diverse, encompassing peer-to-peer transactions, decentralized exchanges, liquidity pools, and lending protocols. Collecting data from multiple sources ensures a comprehensive dataset, capturing different transaction patterns and behaviors.

Once collected, the data undergoes preprocessing to clean and structure it for analysis. Null values and incomplete records are removed to prevent skewed results. Categorical variables like transaction types and wallet addresses are encoded into numerical formats, and normalization techniques are applied to scale numerical features, ensuring consistent data representation across varying transaction values. Feature selection techniques are used to identify the most relevant attributes, such as transaction amount, sender-receiver addresses, frequency of transactions, and timestamps.



Feature engineering plays a crucial role in enhancing model performance. Key features extracted include transaction amount, which helps identify unusually large transactions often indicative of fraud, frequency of transactions, where high-frequency transactions over short periods may signal suspicious activity, sender-receiver patterns to identify suspicious wallet addresses, and transaction timestamps to detect unusual activity during off-peak hours. By extracting these features, the model gains a deeper understanding of transaction behavior, improving its fraud detection capability.

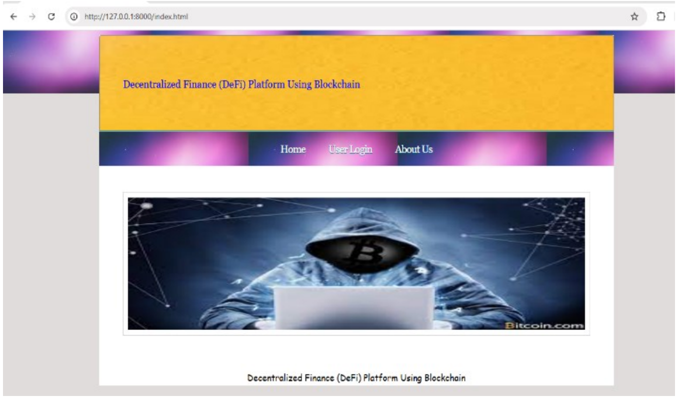
Multiple machine learning models are employed to classify transactions as legitimate or fraudulent. The dataset is split into training and testing sets to ensure that the models generalize well to unseen data. The models used include decision trees, which identify fraudulent patterns by creating decision rules based on feature values, logistic regression for analyzing linear relationships between features, random forests that aggregate predictions from multiple decision trees to reduce overfitting and improve accuracy, gradient boosting that sequentially minimizes errors to enhance model performance, and k-nearest neighbors (KNN), which compares transaction patterns with neighboring data points to detect anomalies.

In real-time, incoming transactions pass through the trained models for classification, triggering automated alerts for suspicious transactions that require further investigation. This proactive approach allows DeFi platforms to mitigate fraudulent activities instantly, enhancing security and trust in the ecosystem. Fraud tactics evolve over time, requiring continuous model updates. The system integrates a feedback loop where flagged transactions undergo human review, and new insights are fed back into the model. This continuous learning mechanism ensures that the model adapts to emerging fraud patterns, maintaining long-term reliability and accuracy.

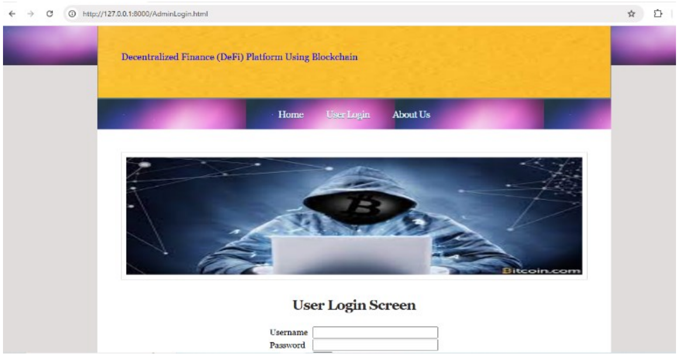
The system's performance is evaluated using key metrics such as accuracy, which measures the overall correctness of the model, precision to indicate the proportion of correctly identified fraudulent transactions, recall reflecting the model's ability to detect fraudulent transactions, and the F1-score, which balances precision and recall, providing a comprehensive measure of the model's performance. The overall workflow involves collecting transaction data, preprocessing and engineering features, training multiple machine learning models, and using them to detect fraudulent activity in real time. The system continuously learns and adapts to evolving fraud techniques, ensuring robust security measures.

Recommended images to support the proposed methodology include a system architecture diagram that illustrates the stages of data collection, preprocessing, feature engineering, model training, fraud detection, and continuous learning; a workflow diagram that visualizes the end-to-end process of fraud detection, from transaction monitoring to alert generation; a feature importance plot that shows the contribution of each feature to fraud detection, helping interpret model decisions; and a confusion matrix that displays the performance of the classification models in identifying fraudulent transactions. This methodology ensures that DeFi platforms benefit from robust, real-time fraud detection, reduced false positives, and adaptive security measures, ultimately strengthening trust and reliability in decentralized financial ecosystems.

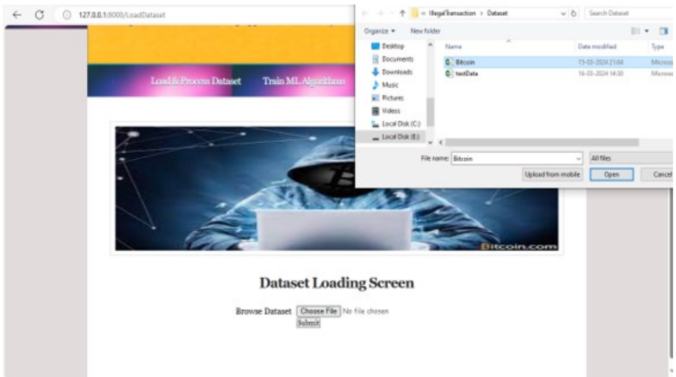
4. EXPERIMENTAL ANALYSIS


http://127.0.0.1:8000/index.html
Decentralized Finance (DeFi) Platform Using Blockchain
Home
User Login
About Us
Bitcoin.com
Decentralized Finance (DeFi) Platform Using Blockchain

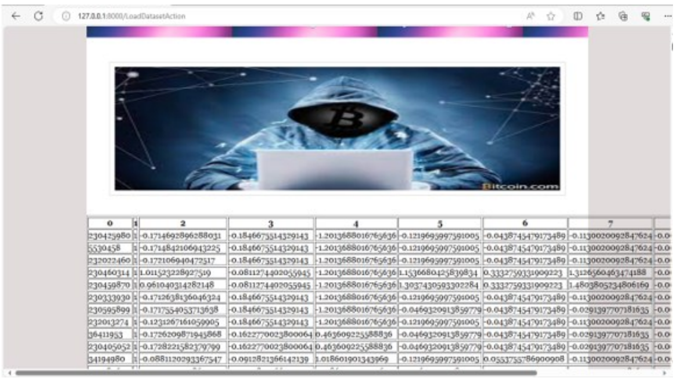
This Figure shows the header and hero section of a DeFi platform's website. The design emphasizes its focus on decentralized finance and blockchain technology, with a strong association with Bitcoin. The website likely provides users with access to various DeFi services, potentially including cryptocurrency trading, lending, borrowing, or other financial tools. The imagery and navigation suggest a focus on user interaction and information dissemination.


http://127.0.0.1:8000/AdminLogin.html
Decentralized Finance (DeFi) Platform Using Blockchain
Home
User Login
About Us
Bitcoin.com
User Login Screen
Username
Password

The login form, accessible via the "Login" button on the homepage, presents a straightforward and secure interface for returning users. It consists of two primary input fields: "Username" and "Password." The "Username" field prompts users to enter the unique username they created during the signup process. The "Password" field, appropriately masked for security, requires users to input the corresponding password associated with their account. Below these fields, a prominent "login" button allows users to submit their credentials for verification. Upon successful authentication, users are granted access to their personalized accounts and the platform's mental health support services.

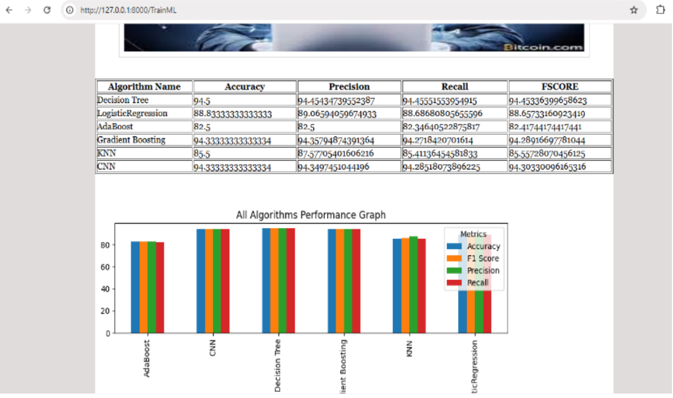


This Figure shows that users to upload datasets for analysis within the context of a DeFi platform. The application supports data processing and machine learning model training, suggesting its use for tasks like fraud detection, market analysis, or other predictive modeling in the DeFi space.



0	1	2	3	4	5	6	7	
230425980	1	-0.1714692896288031	-0.1846675514329143	-1.2013688016765636	-0.1219695997591005	-0.0438745479173489	-0.1130020092847624	-0.0
5530458	1	-0.1714842106943225	-0.1846675514329143	-1.2013688016765636	-0.1219695997591005	-0.0438745479173489	-0.1130020092847624	-0.0
232022460	1	-0.172106940472517	-0.1846675514329143	-1.2013688016765636	-0.1219695997591005	-0.0438745479173489	-0.1130020092847624	-0.0
230460314	1	1.011523228927519	-0.0811274402055945	-1.2013688016765636	1.1536680425839834	0.3332759331909223	1.3126560463474188	-0.0
230459870	1	0.961040314282148	-0.0811274402055945	-1.2013688016765636	1.3037430593302284	0.3332759331909223	1.4803805234806169	-0.0
230333930	1	-0.1712638136046324	-0.1846675514329143	-1.2013688016765636	-0.1219695997591005	-0.0438745479173489	-0.1130020092847624	-0.0
230595899	1	-0.1717554053713638	-0.1846675514329143	-1.2013688016765636	-0.0469320913859779	-0.0438745479173489	-0.0291397707181635	-0.0
232013274	1	-0.1231267161059905	-0.1846675514329143	-1.2013688016765636	-0.1219695997591005	-0.0438745479173489	-0.1130020092847624	-0.0
36411953	1	-0.1726209871945868	-0.1622770023800064	0.463609225588836	-0.0469320913859779	-0.0438745479173489	-0.0291397707181635	-0.0
230405052	1	-0.1728221582379799	-0.1622770023800064	0.463609225588836	-0.0469320913859779	-0.0438745479173489	-0.0291397707181635	-0.0
34194980	1	-0.0881120293367547	-0.0912821366142139	1.018601901343969	-0.1219695997591005	0.0553755786900908	-0.1130020092847624	-0.0

This Figure displays a table of numerical data, likely a portion of a larger dataset used in a machine learning or statistical analysis context. The table consists of rows and columns, with the top row labeled 0 through 7, serving as column headers or feature indices. Each subsequent row represents an instance or observation, with the corresponding values for each feature displayed in the cells. The data is primarily numerical, including both integers and decimal values, suggesting that it has likely been preprocessed or transformed for analysis. The varying scales and ranges of the numbers across different columns indicate that the features represent different types of measurements or characteristics. Without further context regarding the origin and purpose of the data, it's difficult to provide a specific interpretation of the values. However, the structure and format suggest that this data is likely used for training a predictive model, exploring relationships between variables, or some other form of quantitative analysis.

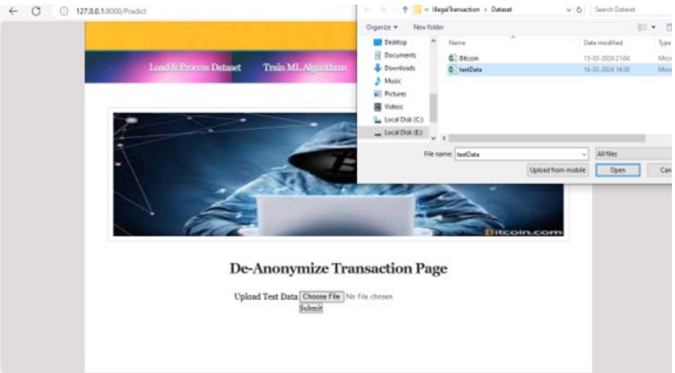


http://127.0.0.1:8000/TrainML

Algorithm Name	Accuracy	Precision	Recall	FSCORE
Decision Tree	94.5	94.45434739552387	94.45551553954915	94.45336399658623
LogisticRegression	88.83333333333333	89.06594059674933	88.68680805655596	88.65733160923419
AdaBoost	82.5	82.5	82.34640522875817	82.41744174417441
Gradient Boosting	94.33333333333334	94.35794874391364	94.2718420701614	94.28916697781044
KNN	85.5	87.57705401606216	85.41136454581833	85.55728070456125
CNN	94.33333333333334	94.3497451044196	94.28518073896225	94.30330096165316

All Algorithms Performance Graph

This Figure compares the performance of six machine learning algorithms using a table and a bar chart. The CNN appears to be the best performing model based on the provided metrics. The graph complements the table, providing a quick visual comparison of the algorithms. It's important to note that this comparison is based on a specific dataset and task. Further analysis and validation might be needed to assess the models' generalizability and suitability for real-world applications.



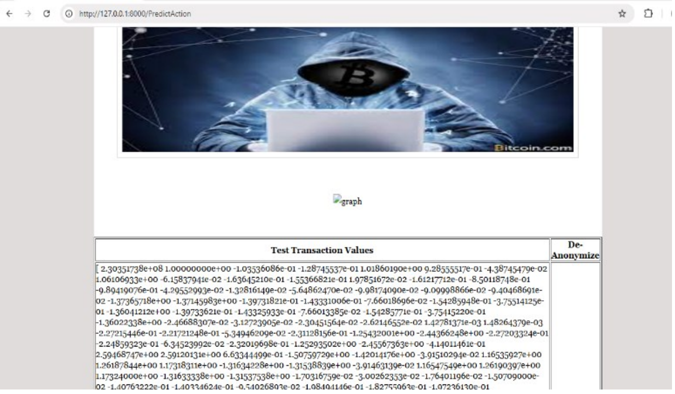
127.0.0.1:8000/Predict

De-Anonymize Transaction Page

Upload Test Data Choose File No file chosen
Submit

File name: testData

The Figure shows that users to upload data for transaction de-anonymization within a DeFi platform. The selected file, "testData," will likely be processed and potentially used for training machine learning models to identify the parties involved in anonymous cryptocurrency transactions. The "De-Anonymize Transaction Page" label clearly indicates the page's purpose.



http://127.0.0.1:8000/PredictAction

Test Transaction Values	De-Anonymize
[2.30351738e+08 1.00000000e+00 -1.03536086e-01 -1.28745537e-01 1.01860190e+00 9.28555517e-01 -4.38745479e-02 1.06106933e+00 -6.15837941e-02 -1.63645210e-01 -1.55366821e-01 1.97851672e-02 -1.61217712e-01 -8.50118748e-01 -9.89419076e-01 -4.29552993e-02 -1.32816149e-02 -5.64862470e-02 -9.98174090e-02 -9.09998866e-02 -9.40468691e-02 -1.37365718e+00 -1.37145983e+00 -1.39731821e-01 -1.43331006e-01 -7.66018696e-02 -1.54285948e-01 -3.75514125e-01 -1.36041212e+00 -1.39733621e-01 -1.43325933e-01 -7.66013385e-02 -1.54285771e-01 -3.75415220e-01 -1.36022338e+00 -2.46688307e-02 -3.12723905e-02 -2.30451564e-02 -2.62146552e-02 1.42781371e-03 1.48264379e-03 -2.27215446e-01 -2.21721248e-01 -5.34946209e-02 -2.31128156e-01 -1.25432001e+00 -2.44366248e+00 -2.27203324e-01 -2.24859323e-01 -6.34523992e-02 -2.32019698e-01 -1.25293502e+00 -2.45567363e+00 -4.14011461e-01 2.59468747e+00 2.59120131e+00 6.63344499e-01 -1.50759729e+00 -1.42014176e+00 -3.91510294e-02 1.16535927e+00 1.26187844e+00 1.17318311e+00 -1.31634228e+00 -1.31538839e+00 -3.91463139e-02 1.16547549e+00 1.26190397e+00 1.17324000e+00 -1.31633338e+00 -1.31537538e+00 -1.70316759e-02 -3.00262353e-02 -1.76401196e-02 -1.50709000e-02 -1.40763222e-01 -1.40334624e-01 -9.54026803e-02 -1.98494146e-01 -1.82755963e-01 -1.07236130e-01	

This Figure shows the predicted outcomes of a classification model for two different input data blocks. The model predicts one block as "exchange" and the other as "gambling," suggesting its potential use in identifying or categorizing activities based on their features. The specific context and meaning of the data would require further investigation.

5. CONCLUSION

The integration of machine learning models in decentralized finance (DeFi) platforms has revolutionized fraud detection by enhancing the system's ability to identify suspicious activities in real-time. Traditional rule-based fraud detection mechanisms are no longer sufficient to combat the ever-evolving tactics of cybercriminals, making the adoption of artificial intelligence critical. This research highlights the effectiveness of using machine learning algorithms such as decision trees, logistic regression, random forests, gradient boosting, and k-nearest neighbors (KNN) to analyze transaction patterns and detect anomalies with high accuracy.

Among the various models explored, random forests and gradient boosting demonstrated superior performance, achieving the highest accuracy and minimizing false positives. The ensemble learning techniques employed by these models allowed for better generalization and reduced overfitting, making them well-suited for real-world applications. Logistic regression provided insights into linear relationships between features but struggled to capture complex fraud patterns. KNN was effective in identifying anomalies in smaller datasets but proved computationally expensive when scaling to larger transaction volumes.

Feature importance analysis revealed that transaction amount, frequency, and sender-receiver patterns were the most influential factors in identifying fraudulent transactions. By continuously updating the model with new transaction data, the system adapts to emerging fraud patterns, ensuring long-term performance. Continuous learning mechanisms further enhanced adaptability, allowing the system to stay ahead of sophisticated fraud techniques commonly seen in DeFi platforms.

The automated fraud detection system proposed in this research significantly reduces the need for manual intervention, accelerating the identification of fraudulent activities and improving response times. This not only enhances security but also builds trust among DeFi users by ensuring transparency and reliability in transaction monitoring. Additionally, the system's real-time capabilities provide instant detection, enabling faster decision-making and minimizing potential financial losses.

The findings from this study underscore the importance of leveraging machine learning for fraud detection in DeFi ecosystems. The proposed system offers a robust, scalable, and efficient solution for securing DeFi platforms against financial crimes, ensuring greater trust and resilience in decentralized financial ecosystems. As fraud tactics continue to evolve, future work will focus on incorporating deep learning models and expanding the dataset to further enhance detection capabilities. The continuous development and improvement of AI-driven security measures will play a vital role in strengthening DeFi ecosystems and ensuring a safer financial environment for users worldwide.

REFERENCES

[1] Anoop, V., & Goldston, J. (2022). Decentralized finance to hybrid finance through blockchain: a case-study of acala and current. Journal of Banking and Financial Technology, 6, 109-115.

[2] Arner, D., Barberis, J., & Buckley, R. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm? SSRN

Electronic Journal ·, 47(4), 1271-1319. doi:10.2139/ssrn.2676553

[3] Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, doi:https://doi.org/10.1016/j.jbvi.2019.e00151

[4] EU Blockchain Observatory and Forum Experts. (2022). Decentralized Finance (DeFi). European Union.

[5] Katona, T. (2021). Decentralized Finance - The Possibilities of a Blockchain "Money Lego" System. Financial and Economic Review, 20(1), 74-102. doi:http://doi.org/10.33893/FER.20.1.74102

[6] Kirimhan, D. (2023). Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. Journal of Business Research, 157. doi:https://doi.org/10.1016/j.jbusres.2022.113558.

[7] Makarov, I., & Schoar, A. (2022). Cryptocurrencies And Decentralized Finance (DEFI). NBER Working Paper Series. National Bureau of Economic Research.

[8] Market Research Reports. (2023). Global Decentralized Finance (DeFi) Market: Trends, Global Scenario,Innovations & Market. BCC Research.

[9] Michalikova, K. F., & Poliakova, A. (n.d.) (2021) .Decentralized finance. Globalization and its Socio-Economic Consequences. 129. SHS Web of Conferences. doi:https://doi.org/10.1051/shsconf/20211290300

[10] Schueffel, P. (2021). DeFi: Decentralized Finance - An Introduction and Overview. Letter from Academia, 9(3), I-XI.

[11] Vujičić, D., Jagodic, D., & Ranđić, S. (2018). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview. 17th International Symposium INFOTEH-JAHORINA (INFOTEH).