**DETECTION OF SUSPICIOUS TRANSACTIONS**

**USING SUPERVISED MACHINE**

**LEARNING**

*A Project Report Submitted*

*to*

**MANIPAL ACADEMY OF HIGHER EDUCATION**

*For Partial Fulfillment of the Requirements for the*

*Award of the Degree*

*Of*

**Bachelor of Technology**

*in*

**Computer and Communication Engineering**

*by*

**Aditya Nayal - 210953019**

**Harshith Nagaraj - 210953052**

**Arman Singh - 210953354**

*Under the guidance of*

**Prof. Chethan Sharma** **Prof. Raghavendra S**

Assistant Professor Assistant Professor

Department of ICT Department of ICT

Manipal Institute of Technology Manipal Institute of Technology

**TABLE OF CONTENTS**

1. Introduction page 1
2. Literature Survey page 3
3. Methodology page 6
4. Results page 9
5. Conclusion and Future Work page 12

## **CHAPTER 1**

**INTRODUCTION:**

In the realm of financial transactions, subtle cues hold significant implications. Our project navigates suspicious transaction detection within concise financial data, leveraging Logistic Regression, Random Forest, and Support Vector Machine (SVM) algorithms. Logistic Regression serves as a simple baseline, while Random Forest captures complex relationships, and SVM excels in high-dimensional spaces.

We aim to refine understanding using Machine Learning (ML) advancements, evaluating these models for anomaly detection, classification, and clustering. Advanced techniques, like attention mechanisms, enhance model performance. This study offers practical insights into transaction monitoring, comparing the efficacy of these models in identifying potential risks within financial headlines.

**1.1 MOTIVATION:**

In the ever-evolving landscape of financial transactions, uncovering and deciphering suspicious activities stands as a riveting challenge. In this era of condensed information, where financial headlines encapsulate intricate stories, the detection of suspicious transactions emerges as a profound puzzle. Much like unravelling sarcasm in language, decoding financial anomalies requires a keen understanding of subtle cues within the vast sea of transaction data. This project transcends the boundaries of conventional transaction monitoring, focusing on three prominent machine learning algorithms: Logistic Regression, Random Forest, and Support Vector Machine (SVM). It aims not only to elevate ML capabilities in anomaly detection but also to shed light on the intricate interplay between financial dynamics and technological vigilance.

Much like the dual significance found in decoding sarcasm in language, this endeavour holds a twofold purpose. Firstly, it aspires to advance the efficacy of Logistic Regression, Random Forest, and SVM models in unravelling suspicious transactions, contributing to the development of smarter algorithms for financial security. Secondly, it seeks to deepen our comprehension of the impact of technological vigilance on financial language dynamics.

As we delve into the captivating realm of transaction detection, we embark on a journey to enrich our understanding of the intricate language woven into financial data and the critical role Logistic Regression, Random Forest, and SVM play in safeguarding financial integrity. This project illuminates the captivating interplay between financial transactions and machine learning, unveiling new dimensions in our quest for heightened security and comprehension in the financial landscape.

**OBJECTIVES**

• Create a robust machine learning framework to detect suspicious transactions using Logistic Regression, Random Forest, and Support Vector Machines (SVM).

• Compare the effectiveness of these models within financial datasets. • Use advanced preprocessing like outlier removal and feature engineering for data standardization.

• Merge diverse transactional data sources to enhance pattern diversity. • Employ advanced feature engineering techniques to boost precision and accuracy in financial anomaly detection.

**1.2 ORGANIZATION OF REPORT:**

The arrangement of our report unfolds as follows: Commencing with Chapter 2, we embark on an exhaustive literature survey to establish the context for our research. In Chapter 3, we elucidate our methodology, offering insights into the implementation of machine learning models for suspicious transaction detection. Progressing to Chapter 4, we showcase the results and outcomes derived from our comprehensive experiments. Chapter 5 encapsulates our concluding remarks, summarizing key findings, and delineates potential directions for future research in the domain of suspicious transaction detection using machine learning. The compilation of references for our study is presented in Chapter 6.

**CHAPTER 2**

**LITERATURE SURVEY:**

The paper by Nitesh Kumar et al,[1] proposes a supervised machine learning approach for enhancing security in the Ethereum blockchain, focusing on the detection of malicious activities within cryptocurrency transactions and decentralized applications. The authors employ sophisticated algorithms such as XGBoost for Externally Owned Accounts (EOA) and smart contract account analysis, achieving high accuracy rates of 96.54% and 96.82%, respectively. The ensemble model demonstrates robust performance in detecting malicious EOA addresses and newly identified threats. However, the study faces challenges, such as a limited exploration of labelling non-malicious addresses, leading to potential bias in the dataset. While the paper reports high accuracy, it lacks a comprehensive evaluation of key metrics like precision, recall, and F1-score, critical for assessing the models' performance in anomaly detection. Additionally, the study's focus on specific time frames and addresses raises concerns about the generalizability of the proposed models to different periods or address types. Addressing these limitations would strengthen the paper's contribution to the field of blockchain address analysis.

The paper by Zhiyuan Chen et al,[2] addresses the global concerns surrounding machine learning and its potential risks to the economy and security. The paper explores the application of machine learning algorithms to detect suspicious transactions, employing methodologies such as typologies, link analysis, and behavioral modeling. The algorithms utilized include Decision Tree, Expectation Maximization, Sequence Matching, and Minimum Spanning Tree, showcasing a diverse set of techniques for transaction analysis. The research aims to assess advanced Anti-Money Laundering (AML) solutions, focusing on quality assurance, detection accuracy, scalability, and processing speed for handling suspicious transactions. The system in question is designed to oversee information processes efficiently, covering preparation, transfer, and review. Despite advancements, the study highlights a significant limitation in existing AML methods, emphasizing a lack of attention to ensuring data quality and reliability. The drawbacks and gaps identified in the research include the challenge of analyzing enormous volumes of raw data from financial institutions and the increasing complexity introduced by the growing volume of customer transactions.

Addressing these challenges would enhance the effectiveness of AML processes and contribute to the broader field of machine learning applications in transaction analysis.

The research paper authored by Madhuparna Bhowmik, Tulasi Sai Siri Chandana, and Dr. Bhawana Rudra et al,[3] scrutinizes the impact of fraudulent transactions in blockchain networks, emphasizing the critical need for effective detection methods. The study employs a comparative analysis of machine learning algorithms, including Decision Trees, Naive Bayes, Logistic Regression, and Multi-Layer Perceptron, to assess their proficiency in identifying fraudulent transactions. Applying eight supervised learning algorithms with trust and rating information from nodes, the research identifies Logistic Regression, Ada Boost, Support Vector Machine (SVM), and Random Forest Classifier as top-performing algorithms, achieving impressive accuracy rates of 97%. The paper suggests the potential for a combined approach, integrating scores and decisions from Ada Boost, SVM, and Random Forest Classifier to enhance fraud detection accuracy. Overall, the findings highlight the promise of machine learning in detecting fraudulent transactions within blockchain networks, offering a potential solution to strengthen security and trust, while indicating future research directions for unsupervised algorithms and comprehensive investigations into private blockchains' fraudulent activities.

The paper authored by Sirine Sayadi, Sonia Ben Rejeb, and Ziéd Choukair et al,[4] addresses the surging prevalence of electronic transactions, particularly in Bitcoin and other cryptocurrency systems built on blockchain technology. Despite the widespread adoption of blockchain, the research underscores significant anomalies and risks associated with cryptocurrencies, advocating for enhanced security measures. The paper introduces a novel model utilizing machine learning techniques, employing the One-Class Support Vector Machines (OCSVM) algorithm for identifying outliers and the K-Means algorithm to categorize similar outliers based on anomaly types. In Stage 1, the model's confusion matrix revealed effective detection of 15 transactions with anomalies, though it generated a notable 54 false positives. In Stage 2, the model successfully detected various attacks, including DDOS, double spending, and the 51% vulnerability attack, with an accuracy of 0.93. However, the research acknowledges limitations, including a high false positive rate, focus on specific attack types, and the need for a broader set of evaluation metrics for a comprehensive assessment of the model's performance. Addressing these drawbacks is crucial for ensuring the security and credibility of cryptocurrencies.

The research paper authored by Adam Turner and Angela Samantha Maitland Irwin et al,[5] delves into the investigation of de-anonymizing Bitcoin transactions by analyzing the Bitcoin blockchain and associated transactions. The study explores the application of graph analysis and modern social media technology to unveil the identities of Bitcoin users. Employing algorithms such as the Random Forest Classifier and Deep Neural Network, the research found that heuristics and graph analysis techniques contribute to building a behavioral profile of Bitcoin addresses and transactions. The study suggests that existing typologies of illicit behavior can be applied to identify potential red flag indicators. Additionally, the paper proposes methods to augment Bitcoin data with big data and social media information, utilizing machine learning to rank and cluster suspicious transactions. The research results in the development of a functional software architecture theoretically capable of detecting suspicious illicit transactions on the Bitcoin network. However, the inherent anonymity of the Bitcoin system poses a challenge in reliably attributing transactions to individuals, given that pseudonymous Bitcoin addresses do not reveal personally identifiable information (PII).

The research conducted by Hyochang Baek, Junhyoung Oh, Chang Yeon Kim, and Kyungho Lee et al,[6] acknowledges the evolving landscape of financial fraud alongside advancements in the financial sector, specifically the emergence of blockchain technology. Focusing on addressing the challenges introduced by blockchain technology in financial transaction obfuscation, the study centers its investigation on suspicious transactions within Binance, an open-source cryptocurrency platform. Utilizing an unsupervised learning approach with the Expectation Maximization (EM) algorithm, the study clusters a dataset of 38,526 wallets to identify patterns and relationships among them. Anomaly detection is then performed using the Random Forest (RF) algorithm after feature engineering based on the unsupervised learning results. The EM algorithm's Gaussian mixture model engineers nine distinct features for each wallet, derived from data within each blockchain block. The RF approach effectively labels wallets with suspicious activities, demonstrating a high level of precision in the process. While the research highlights these achievements, it underscores the importance of considering additional evaluation metrics such as recall, F1-score, or AUC for a more comprehensive assessment of model performance.

The paper by Kumar Mohanta, Debasish Jena, Soumyashree Panda, and Srichandan Sobhanayak et al,[7] explores the decentralized and persistent nature of blockchain technology, highlighting its diverse applications across domains. While addressing security and privacy concerns such as double spending and privacy leakage, the paper falls short in providing specific details on implementation issues and scalability challenges. It acknowledges the need to address security and privacy but lacks discussion on regulatory issues, a comparative analysis of blockchain platforms, and the broader social and economic impact. These gaps limit the paper's ability to offer a comprehensive understanding of the practical implications and challenges associated with adopting blockchain technology.

The paper authored by Helen Mary Varghese, Dhwani Apurva Nagoree, Anshu, and N. Jayapandian et al,[8] delves into the rapid growth of cryptocurrency since its inception in 2009, emphasizing a 300% increase in cryptocurrency exchanges worldwide by 2020. The abstract provides an insightful overview of cryptocurrency types, investment opportunities, a comparative analysis with gold, and security concerns. The problem statement highlights crucial aspects, including the use of encryption algorithms for security, security issues such as thefts and ransomware attacks, and the challenge of forgotten passwords in the absence of centralized recovery mechanisms. The performance analysis underscores the reliance on blockchain technology for secure transaction records and the substantial growth and potential of Bitcoin, the leading cryptocurrency. Despite these insights, the paper acknowledges certain drawbacks and gaps, such as the limited coverage of mitigation strategies for cryptocurrency security issues and a brief mention of high-tech companies' reluctance to support cryptocurrency on mobile platforms without delving into potential implications and solutions, leaving a gap in addressing industry challenges.

The paper authored by Ammar Oad, Abdul Razaque, Askar Tolemyssov, Munif Alotaibi, Bandar Alotaibi, and Chenglin Zhao et al,[9] introduces a Blockchain-based Transaction Scanning (BTS) approach designed to detect malicious behavior associated with financial transactions and criminal organizations. By setting rules for anomaly detection and swift action, the BTS method aims to prevent abnormal behavior in the business, particularly addressing money laundering concerns in debit cards and money transfers. The paper emphasizes the automation of the transaction investigation process to enhance efficiency and limit illicit financial activities. Despite the apparent effectiveness highlighted in the results, the article lacks explicit mention of drawbacks or inconsistencies in the proposed BTS method, making it challenging to assess its limitations and potential shortcomings comprehensively.

The paper authored by Tehreem Ashfaq, Rabiya Khalid, Adam Sani, Sheraz Aslam, Ahmad Taher Azar, Safa Alsafari, and Ibrahim Hameed et al,[10] presents a security fraud model that leverages machine learning and blockchain to address fraud and corruption issues within the Bitcoin network. Utilizing XGBoost and Random Forest (RF) machine learning algorithms, the model aims to detect changes and validate predictions, integrating blockchain technology for enhanced fraud detection. The article evaluates the proposed method's accuracy and Area Under the Curve (AUC), conducts a security analysis of smart contracts, and designs an attacker model to safeguard against potential threats. Simulation results, including responses to modern network attacks like Sybil and dual-use attacks, are also provided. The problem statement highlights the impact of cybercrime on the financial sector, emphasizing the limitations of traditional fraud detection methods and the persistent security challenges of blockchain technology. While the paper proposes a secure and efficient model, it acknowledges existing issues in the financial system, blockchain, and Bitcoin network, outlining the need for an integrated solution. The drawbacks and gaps emphasize the ongoing challenges in privacy, stealth attacks, and double spending within blockchain networks, emphasizing the necessity of the proposed model to address these issues effectively.

**CHAPTER 3**

**METHODOLOGY**

**3.1 DATA COLLECTION:**

In our initial customer transaction analysis, we loaded 'customer\_transaction.csv' into a DataFrame 'df' using Python's pandas library. This dataset contains key attributes like 'is\_Alerted,' 'is\_Suspicious,' 'transaction\_amount,' 'correspondent\_bank,' 'debit\_credit,' 'Account\_type,' 'Account\_Classification,' 'Risk\_level,' 'Annual\_income,' and 'is\_noncitizen.' From these attributes, we derived 'df\_features,' a subset crucial for our analysis, focusing on alerts, transaction details, bank information, and account classifications. To prepare for machine learning, we applied one-hot encoding to categorical variables in 'df\_features,' resulting in 'df\_transformed.' Visualizations like correlation heatmaps, joint plots, and pair plots helped uncover relationships between variables. Lastly, the dataset was split using 'train\_test\_split' to create distinct training and testing sets, laying the groundwork for subsequent model implementation.

**3.2 DATA PREPROCESSING:**

After collecting the data, our focus shifted to preprocessing 'customer\_transaction.csv' for model readiness. Key features like 'is\_Alerted,' 'is\_Suspicious,' 'transaction\_amount,' 'correspondent\_bank,' 'debit\_credit,' 'Account\_type,' 'Account\_Classification,' 'Risk\_level,' 'Annual\_income,' and 'is\_noncitizen' were extracted into a pandas DataFrame. One-hot encoding expanded categorical variables for a comprehensive analysis. Visualizations like a correlation matrix heatmap and joint plots highlighted relationships and patterns. Using 'train\_test\_split,' the dataset was split for model training and testing. This stage ensured proper formatting and readiness for in-depth analysis.

**3.3 FEATURE EXTRACTION:**

After preliminary preprocessing, feature extraction began using 'df\_transformed.' 'is\_Alerted' and 'is\_Suspicious' were target variables, others were features. 'train\_test\_split' partitioned data for model training. Logistic Regression, Random Forest Classifier, and Support Vector Machine (SVM) models were used for classification. Models were trained and tested, and evaluation metrics like classification reports and confusion matrices were employed. Metrics such as accuracy and recall assessed models' effectiveness in detecting suspicious transactions. Results revealed model accuracy and recall, crucial for evaluating their performance in identifying suspicious activities in customer transactions.

**3.4 MODEL SELECTION:**

In the context of customer transaction analysis, various machine learning models were chosen to discern and classify suspicious activities. Three distinct models were considered:

**a) Logistic Regression**: This linear model is well-suited for binary classification tasks and was applied to discern the likelihood of a transaction being suspicious.

**b) Random Forest Classifier:** An ensemble learning method, combining multiple decision trees to enhance overall predictive performance. It was employed to evaluate its effectiveness in identifying suspicious transactions.

**c) Support Vector Machine (SVM):** A potent classification algorithm that determines hyperplanes in an N-dimensional space to segregate data into distinct classes. SVM was utilized to discern patterns indicative of suspicious activities.

**3.5 MODEL TRAINING:**

The training phase for the selected models involved leveraging the preprocessed and feature-extracted customer transaction data to enable these models to learn inherent patterns and relationships within the dataset. The training configurations for each model were as follows:

**a) Logistic Regression:** The 'liblinear' solver was employed for Logistic Regression, and a substantial number of iterations (max\_iter=1000000) were set to ensure comprehensive learning.

**b) Random Forest:** Training the Random Forest model involved using 100 decision trees (n\_estimators=100) within the ensemble, optimizing predictive performance.

**c) Support Vector Machine (SVM):** SVM was trained using the SVC class with default parameters, tailoring the model to the characteristics of the dataset.

These specific training setups aimed to maximize the learning potential of each model, taking into account their individual strengths and requirements. The subsequent evaluation of these models provided insights into their effectiveness in identifying and classifying suspicious transactions in the customer transaction dataset.

**3.6 EVALUATION METRICS:**

• Accuracy: Measures overall correctness by comparing correctly predicted instances to total instances.

• Confusion Matrix: Provides a detailed breakdown of model performance, showing true positive, true negative, false positive, and false negative predictions.

• Precision: Reflects the model's accuracy in identifying positive instances by calculating true positives against false positives.

• Recall (Sensitivity): Emphasizes the model's capability to capture actual positive instances, computed as true positives against false negatives. • F1-Score: Represents the balance between precision and recall, offering a combined measure.

**CHAPTER 4**

RESULTS AND DISCUSSIONS:

**Logistic Regression:**

The Logistic Regression model emerged as a strong contender in identifying suspicious transactions. The classification report unveils a noteworthy accuracy of {0.97} and a recall of {0.89} on the testing data. Complementing these metrics, the confusion matrix screenshots (refer to Figure below) provide a visual representation of the model's ability to correctly classify true positives (TP) and true negatives (TN). These screenshots offer a concrete depiction of the model's performance, aiding in the interpretation of its predictive capabilities.

A screenshot of a graph

Description automatically generated

**Random Forest Classifier:**

The Random Forest Classifier, leveraging ensemble learning techniques, demonstrated robust performance in our investigation. With an accuracy of {0.89} and a recall of {0.86}, the model showcased its effectiveness in identifying suspicious transactions. The confusion matrix screenshots (see Figure 2 below) provide a granular breakdown of the classifier's performance, offering insights into its ability to handle different classes. These visuals serve as valuable tools for a comprehensive understanding of the model's strengths.

A blue squares with white text

Description automatically generated

**Support Vector Machine (SVM):**

The SVM classifier, known for its efficacy in handling complex decision boundaries, also exhibited competitive results. The classification report indicates an accuracy of {0.99} and a recall of {0.89}. The confusion matrix below provide a detailed overview of the model's performance, offering insights into its capacity to correctly classify suspicious transactions. These visual representations enhance the interpretability of the SVM's predictive capabilities.

A blue squares with white text

Description automatically generated

**PERFORMANCE METRICS SUMMARY:**

To consolidate the evaluation of each algorithm, we present a summary table that includes accuracy, recall, precision, and F1 score metrics. This table serves as a concise reference for stakeholders to compare the overall performance of the three machine learning models.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Models** | **Accuracy** | **Precision** | **Recall** | **F1-Score** |
| Logistic Regression | 0.97 | 0.68 | 0.91 | 0.93 |
| Random Forest | 0.98 | 0.80 | 0.91 | 0.94 |
| Support Vector Machine | 1.00 | 1.00 | 0.89 | 0.94 |

**COMPARATIVE ANALYSIS:**

Comparing the three algorithms, it is evident that each model has its unique strengths. Logistic Regression offers simplicity with effectiveness, Random Forest excels in handling complex relationships, and SVM provides robust performance with intricate decision boundaries. The choice of algorithm depends on specific requirements, and the inclusion of confusion matrix screenshots aids in presenting a holistic view of the models’ performance.

In conclusion, our study underscores the applicability of machine learning algorithms in detecting suspicious financial transactions. The inclusion of confusion matrix screenshots enhances the visual representation of each model’s performance, providing a comprehensive and accessible way for stakeholders to evaluate and interpret the results.

**LIMITATIONS AND DRAWBACKS:**

Despite the promising outcomes of our machine learning-based approach to detecting suspicious financial transactions, it's important to acknowledge certain limitations that may impact the broad applicability of our findings. One key limitation pertains to the quality and representativeness of the dataset. The efficacy of machine learning models is contingent on diverse and comprehensive data, and a dataset lacking in these aspects may hinder the models' ability to generalize effectively.

Another factor to consider is the dynamic nature of financial transactions and evolving tactics employed by potential threats. The models developed in this study might not fully capture emerging patterns or adapt quickly to new challenges, necessitating ongoing monitoring and regular model updates.

Interpreting the results should be approached cautiously. While metrics like accuracy, recall, precision, and F1 score offer valuable insights, they may not entirely reflect the real-world impact of false positives or false negatives. Understanding the consequences of misclassifications is crucial, warranting a more nuanced evaluation of model performance.

Additionally, the choice of features and their relevance is critical. In certain cases, incorporating domain-specific features or external data sources may improve model performance. The interpretability of complex models, such as Random Forest or SVM, could pose challenges in explaining predictions, limiting their application in contexts where interpretability is vital.

In conclusion, while our approach holds promise, addressing these limitations is crucial for refining the models and ensuring their real-world effectiveness. Future iterations of this research should focus on overcoming these challenges to enhance the models' robustness and applicability.

**CHAPTER 5**

**CONCLUSION:**

In wrapping up this exploration of machine learning's role in detecting suspicious financial transactions, our findings illuminate both triumphs and challenges. The distinctive performances of Logistic Regression, Random Forest Classifier, and Support Vector Machine offer valuable insights, showcasing commendable accuracy and recall. However, amidst the applause, the shadows of dataset limitations and the dynamic nature of financial threats demand our attention.

As we navigate the intricate landscape of financial security, these identified limitations act as guideposts, steering us toward a more nuanced understanding of our models and urging us to pursue continuous refinement. Beyond the current challenges lies a path toward future progress. This journey underscores the necessity of ongoing model updates, the exploration of new features, and a holistic approach to comprehending the tangible implications of our predictive models. While we conclude this study, it serves as a launchpad for future endeavors—a call to refine, innovate, and shape the trajectory of effective financial security measures in the times ahead.

**REFERENCES**

[1] Kumar, Nitesh, Ajay Singh, Anand Handa, and Sandeep Kumar Shukla. "Detecting malicious accounts on the Ethereum blockchain with supervised learning." In Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, Be'er Sheva, Israel, July 2–3, 2020, Proceedings 4, pp. 94-109. Springer International Publishing, 2020.

[2] Chen, Z., Van Khoa, L.D., Teoh, E.N., Nazir, A., Karuppiah, E.K. and Lam, K.S., 2018. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems, 57, pp.245-285.

[3] Bhowmik, M., Chandana, T.S.S. and Rudra, B., 2021, April. Comparative study of machine learning algorithms for fraud detection in blockchain. In 2021 5th international conference on computing methodologies and communication (ICCMC) (pp. 539-541). IEEE.

[4] Sayadi, S., Rejeb, S.B. and Choukair, Z., 2019, June. Anomaly detection model over blockchain electronic transactions. In 2019 15th international wireless communications & mobile computing conference (IWCMC) (pp. 895-900). IEEE.

[5] Turner, A. and Irwin, A.S.M., 2018. Bitcoin transactions: a digital discovery of illicit activity on the blockchain. Journal of Financial Crime, 25(1), pp.109-130.

[6] Halpin, H. and Piekarska, M., 2017, April. Introduction to Security and Privacy on the Blockchain. In 2017 IEEE European symposium on security and privacy workshops (EuroS&PW) (pp. 1-3). IEEE.

[7] Mohanta, B.K., Jena, D., Panda, S.S. and Sobhanayak, S., 2019. Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, p.100107.

[8] Varghese, H.M., Nagoree, D.A. and Jayapandian, N., 2021, July. Cryptocurrency Security and Privacy Issues: A Research Perspective. In 2021 6th International Conference on Communication and Electronics Systems (ICCES) (pp. 902-907). IEEE.

[9] Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B. and Chenglin, Z., 2021. Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. Electronics 2021, 10, 1766.

[10] Ashfaq, T., Khalid, R., Yahaya, A.S., Aslam, S., Azar, A.T., Alsafari, S. and Hameed, I.A., 2022. A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), p.7162.