IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AMLBOT: AN AI POWERED TRANSACTIONAL NETWORK AND BEHAVIOUR ANALYSIS TO DETECT AND PREVENT MONEY LAUNDERING ACTIVITIES.

S.S. Vasantha Raja[1]

A.Vijayanarayanan[2] Vidhya.D[3] Nithya Nandhini N.J[4] S.R.Noble Lourdhu Raj [5]

AssistantProfessor[1,2,3,4,5]

Department of Computer Science and Engineering

PERI INSTITUTE OF TECHNOLOGY

ABSTRACT

Money laundering is the process of disguising the proceeds of illegal activities as legitimate funds. Money laundering is a significant problem that poses serious threats to the integrity of the financial system, as it enables criminals to profit from illegal activities and finance further criminal endeavors. Money laundering is also linked to other crimes, such as drug trafficking, terrorism financing, and corruption. To combat money laundering, governments and financial institutions have implemented variousmeasures, such as Know Your Customer (KYC) regulations, Anti-Money Laundering (AML) laws, and the use of financial intelligence units.

Keywords—Anti-Money, Laundering, criminal endeavors, Know Your Customer(KYC)

INTRODUCTION

Money laundering is the process of disguising the proceeds ofillegal activities as legitimate funds. Money laundering is a significant problem that poses serious threats to the integrity of the financial system, as it enables criminals to profit from illegal activities and finance further criminal endeavors. Money laundering is also linked to other crimes, such as drug trafficking, terrorism financing, and corruption. To combat money laundering, governments and financial institutions haveimplemented various measures, such as Know Your Customer (KYC) regulations, Anti-Money Laundering (AML) laws, and the use of financial intelligence units. The existing money laundering system is complex,

involving multiple agencies and regulations. This complexity makes it difficult to detect and prevent money laundering activities. Many existing money laundering systems rely on outdated technology and manual processes, which can be time-consuming and prone to error.Money laundering is a serious crime that poses significant threats to the integrity of the financial system. To combat money laundering, there is a need for effective detection and prevention systems that can identify suspicious transactions and patterns of behavior. This project aims to prevent and detect money laundering activities by identifying suspicious transactions and monitoring the movement of funds through the financial system. In this project, we propose a transactional network and behavior analysis system that utilizes Long Short-Term Memory (LSTM) to detect and prevent money laundering activities. The proposed system uses historical financial data in a time-series format to train the LSTM network and identify patterns and trends that are associated with money laundering activities. By analyzing the data in a time-series format, LSTMcan identify unusual patterns of transactions and flag them for further investigation. The transactional network and behavior analysis system can also predict future trends in financial data, allowing for the detection and prevention of potential money laundering activities before they occur. The system provides a more efficient and accurate method for identifying potential money laundering activities, ultimately leading to a more effective and efficient anti-money laundering system.

The aim of the project "AML Bot: An AI Powered Transactional Network and Behavior Analysis to Detect and Prevent Money Laundering Activities" is to develop an advanced system that leverages artificial intelligence and machine learning techniques to enhance the detection and prevention of money laundering activities.

To developanAI-powered transactional network that can identify suspicious patterns of behavior in financial transactions. Transactional Network Analysis: AMLBot will analyze financial transactions within a network to identify patterns and relationships that may indicate potential money laundering activities. It will consider various factors such as transaction amounts, frequency, geographic locations, and relationships between different entities involved in the transactions.

Behavioral Analysis: AMLBot will employ AI algorithms to analyses the behavior of individuals and entities involved in financial transactions. It will establish base line patterns of behavior and identify any deviations or anomalies that may indicate suspicious activity. This analysis may include factors such as sudden changes in transaction volumes, unusual transaction patterns, or connections to high-risk jurisdictions.

Real-time Monitoring: AML Bot will continuously monitor financial transactions in real- time, allowing for immediate detection and response to suspicious activities. It will provide alerts and notifications to relevant stakeholders, such as financial institutions and regulatory bodies, to enable timely action and investigation.

Integration with Existing Systems: AML Bot can be integrated with existing banking and financial systems to leverage transaction data and historical records. This integration enables seamless analysis and detection of money laundering activities without disrupting the normal operations of financial institutions.

Compliance Support: AMLBot will assist financial institutions in meeting their regulatory compliance requirements. Scalability and Adaptability: AML Bot should be designed to handle large volumes of financial transactions across different types of financial institutions. It should be adaptable to changing money laundering techniques and evolving regulatory requirements.

User-Friendly Interface: AMLBot should have a user-friendly interface that allows investigators and compliance officers to interact with the system, review alerts, conduct further investigations, and document their findings.

LITERATURE SURVEY

The paper identifies the issue of money laundering and the challenges associated with combating it. The objective of the study is to investigate the effectiveness of the anti-money laundering (AML) system in a European bank and propose an improved machine learning approach to enhance the system's performance. The study uses a case study approach, and the authors propose a hybrid machine learning model that combines K-means clustering, principal component analysis (PCA), and decision trees. The authors use a real-world dataset from a European bank's AML system, which includes transactional data, customer information, and suspicious activity reports (SARs). The proposed machine learning approach provides a high accuracy rate for detecting suspicious transactions and reduces the number off also positives, thus improving the efficiency of the AML system. The study is limited to a single European bank, and the proposed model's generalizability to other banks may be limited.[1]

The paper identifies the challenges faced by small and medium-sized financial institutions in implementing effective anti-money laundering (AML) systems. The objective of the study is to propose an enhanced AI-based AML system that can effectively detect money laundering activities in small and medium-sized financial institutions. The authors propose a machine learning-based approach that combines supervised and unsupervised learning algorithms, including random forests, k-means clustering, and decisiontrees. The authors use a real-world dataset from a small and medium-sized financial institution in Canada, which includes transactional data, customer information, and SARs. The proposed AI-based AML system provides high accuracy rates for detecting money laundering activities and reduces false positives, thus improving the efficiency of the AML system. The system is also cost-effective and easy to implement for small and medium- sized financial institutions. The study is limited to a single financial institution in Canada, and the proposed model's generalizability to other institutions may be limited.[2]

The paper addresses the challenge of effectively detecting money laundering activities using advanced deep learning techniques. The objective of the study is to compare the performance of various deep learning models in detecting money laundering activities and identify the most effective approach. The authors compare the performance of three deep learning models, namely Convolutional

Neural Networks (CNN), Long Short-Term Memory (LSTM), andDeep Belief Networks (DBN), using a real-world dataset.The authors use a publicly available dataset from the UCI Machine Learning Repository, which contains synthetic financial transactions labeled as either money laundering or legitimate transactions. The study provides a comprehensive comparative analysis of different deep learning techniques for money laundering detection. It highlights the strengths and weaknesses of each model and did entities the most effective approach for detecting money laundering activities. The study is limited to a specific dataset, and the generalizability of the findings to other datasets or real-world scenarios may be limited.

Additionally, the paper does not consider other non-deep learning approaches, which could provide valuable insights for comparison. [3]. The paper addresses the challenge of detecting money laundering activities using association rule mining techniques The objective of the study is to propose a fuzzy association rule mining approach for money laundering detection and assess its effectiveness compared to traditional association rule mining methods. The authors propose a fuzzy association rule mining framework that considers sun certain and imprecise data related to money laundering activities. The framework is applied to a real-world dataset of financial transactions.

The authors use a publicly available dataset from the UCI Machine Learning Repository, which contains financial transaction data with labeled instances of money laundering and non- money laundering transactions. The study introduces a fuzzy association rule mining approach specifically tailored form one laundering detection, considering the uncertainty and imprecision associated with such activities. The proposed approach provides insights in to the underlying patterns and associations in money laundering activities. The study is limited to a specified at a set, and the generalizability of the findings to other datasets or real- world's scenarios may be limited. The performance of the proposed approach in terms of accuracy and efficiency compared to other methods is not extensively evaluated.[4] The paper addresses the challenge of effectively detecting money laundering activities in financial institutions using deep learning techniques. The objective of the study is to propose a deep learning-based approach for anti-money laundering (AML) and assess its effectiveness in improving detection accuracy the authors propose a deep learning model based on Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). The modelis trained using a real-world dataset comprising financial transaction data labeled as either money laundering or legitimate transactions. The authors use a proprietary data set provided by a financial institution, which contains historical transactional data with labels for money laundering and legitimate transactions.

The study introduces a deep learning-based approach specifically designed for anti-money laundering, utilizing the capabilities of CNN and RNN. The proposed model demonstrates improved detection accuracy compared to traditional methods, providing enhanced efficiency in detecting money laundering activities. The study's findings are based on a proprietary dataset, limiting the generalizability of the results to other data sets or financial institutions. The paper does not extensively discuss the interpretability of the deep learning model, which may be important for regulatory compliance and decision-making processes. [5]

The paper addresses the challenge of detecting money laundering activities in financial transactions using machine learning algorithms. The objective of the study is to compare the performance of various machine learning algorithms in detecting money laundering and identify the most effective approach. The authors compare the performance of several machine learning algorithms, including Random Forest, Support Vector Machine, and Naive Bayes, using a real-world dataset of financial transactions. The authors use apublicly available dataset from the UCI Machine Learning Repository, which contains labeled instances of money laundering and non- money laundering transactions. The study provides a comprehensive comparison of different machine learning algorithms form one laundering detection, highlighting their strengths and weaknesses. It provides insights into the performance and suitability of different algorithms in real-world scenarios. The study's findings are based on a specific dataset, and the generalizability of the results to other datasets or financial institutions may be limited. The paper does not explore the impact of feature engineering or ensemble methods, which could potentially improve detectionaccuracy.[6]

IMPLEMENTATION

EXISTING SYSTEM

Existing Anti-Money Laundering (AML) systems encompass a range of technological solutions designed to detect and prevent money laundering activities. These systems leverage various techniques, such as data analysis, pattern recognition, and risk assessment, to identify suspicious transactions and mitigate the risk of money laundering. Here are two examples of existing AML systems Name screening systems are widely used in financial institutions and regulatory bodies to combat money laundering. These systems compare names, addresses, and other relevant information against watch lists, which contain known individuals, entities, and countries associated with money laundering, terrorism financing, or other financial crimes. The systems employ fuzzy matching algorithms and sophisticated search capabilities to identify potential matches and generate alerts for further investigation. Name screening systems contribute to the early detection of suspicious activities and enhance compliance with regulatory requirements.

PROPOSED SYSTEM

Proposed System: "AMLBot: An AI Powered Transactional Network and Behavior Analysis to Detect and Prevent Money Laundering Activities using LSTM" The objective of AMLBot is to leverage the power of artificial intelligence, specifically Long Short-Term Memory (LSTM) networks, to analyze transactional data and detect potential money laundering activities. By utilizing LSTM, the system aims to capture long-term dependencies and sequential patterns in transactional behavior, enabling more

accurate and timely detection of suspicious activities. AMLBot utilizes LSTM, a type of recurrent neural network (RNN), to process sequential transactional data. LSTM networks are designed to effectively model temporal dependencies and retain long-term information. The system analyses transactional features such as transaction amounts, frequencies, time stamps, and relationships between entities to train the LSTM model. The model learns to identify patterns indicative of money laundering and generates alerts when suspicious activity isdetected.

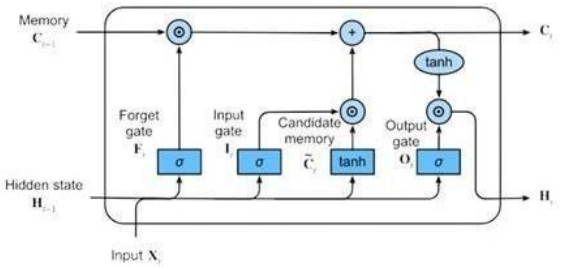

Fig1: Overview

A large data set of historical transactional data, encompassing various transaction attributes and known instances of money laundering, is used to train the LSTM model. The dataset includes legitimate transactions as well as labeled instances of money laundering for supervised learning. The dataset should be representative of real-world transactional behavior and encompass a diverse range of money laundering scenarios.

SYSTEM ARCHITECTURE DESCRIPTION

System Architecture Description of "AMLBot: An AI Powered Transactional Network and Behavior Analysis to Detect and Prevent Money Laundering Activities using LSTM":The architecture of AMLBot consists of two main components: the core system and the AMLBot API. The core system encompasses the data collection, pre-processing, feature selection, feature extraction, and classification using LSTM. The AMLBot API acts as an interface to continuously receive bank transactions, make predictions, and generate alerts and notifications to regulatory authorities. The system architecture of AMLBot consists of two major components- the Admin interface and the AMLBotAPI.

AdminInterface

Data Collection: The first step involves collecting the transactional data from banks and financial institutions. The data is collected in real-time and stored in a database for further processing. Import, Explore, and Visualize Dataset: The next step involves importing the data into the system and exploring it to gain insights. The data is visualized using various tools to identify any patterns or anomalies.

AMLBotAPI

The AMLBot API is responsible for continuous monitoring of bank transactions and predicting

potential money laundering activities Overall, the AMLBot system architecture uses advanced machine learning techniques to detect and prevent money laundering activities in real- time, providing a proactive approach to combating financial crimes.

Overall, the AMLBot system architecture uses advanced machine learning techniques to detect and prevent money laundering activities in real-time, providing a proactive approach to combating financialcrimes.

SYSTEM ARCHITECTURE

"AMLBot:AnAI Powered Transactional Network and Behavior Analysis to Detect and Prevent Money Laundering Activities using LSTM" is a system designed to leverage artificial intelligence and LSTM(Long Short- Term Memory) networks for the detection and prevention of money laundering activities. The proposed system "AMLBot: An AI Powered Transactional Network and Behavior Analysis to Detect and Prevent Money Laundering Activities using LSTM" utilizes various technologies and tools to build a comprehensive anti-money laundering system. The system architecture involves various components such as data collection, import, exploration, and visualization. The data collected undergoes pre-processingto handle null values, missing values, misspelled data, andredundant rows or columns. Feature selection is carried outusing the Chi-square test, and feature extraction is done using the co-currencematrix.

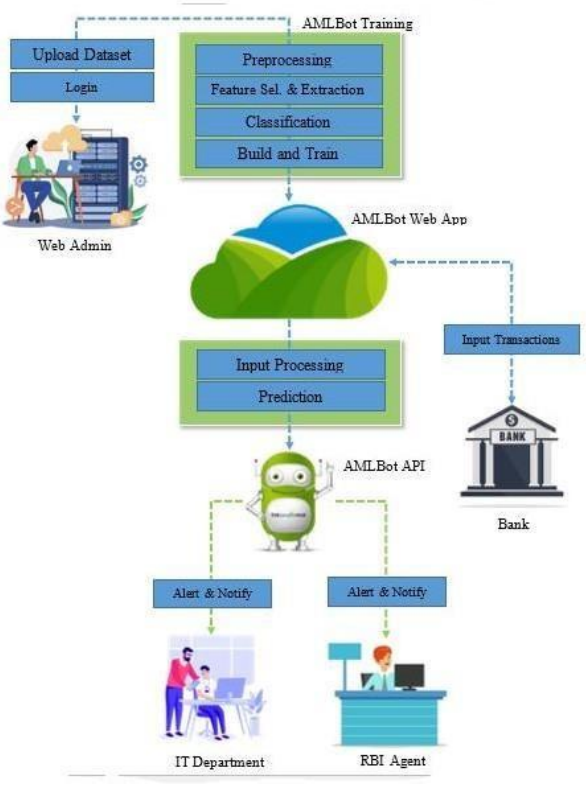

Fig2: System Architecture

MODULESDESCRIPTION

AML BoT Web App1. Front End

The front-end development of the AMLBot web app module involves creating the user interface and designing the visual elements that users will interact with. In this case, Python Flask is used as the web framework to build the front-end of the application. Flask provides a simple and efficient way to develop web applications using Python. HTML, CSS, and Java Script are used to create the user interface, design layouts, and add interactivity to the web app. The front-end components are responsible for displaying the AMLBot system's features and functionality to theusers.

BackEnd

The back-end development of the AMLBot web app module is responsible for processing user requests, executing business logic, and communicating with the database. Python Flask is also used for the back-end development as it provides a robust framework for building web applications.The back-end components handle user inputs, interact with the AMLBot system's functionality, and generate responsesto be displayed on the front-end. They are responsible for coordinating the different modules of the system and ensuring smooth operation

MONEY LAUNDERING ACTIVITY CLASSIFICATION ALGORITHMS

1 .Long Short Term Memory Networks (LSTMs)

LSTMs can be defined as Recurrent Neural Networks (RNN) that are programmed to learn and adapt for dependencies for the long term. It can memorize and recallpast data for a greater period and by default, it is its sole behavior. LSTMs are designed to retain over time and hence forth they are majorly used in time series predictions because they can restrain memory or previous inputs. This analogy comes from their chain-like structure consisting of four interacting layers that communicate with each other differently. Besides applications of time series prediction, they can be used to construct speech recognizers, development in pharmaceuticals, and composition of musicloops as well. LSTM work in a sequence of events. First, they don't tend to remember irrelevant details attained in the previous state. Next, they update certain cell-state values selectively and finally generate certain parts of the cell-state as output. Below is the diagram of their operation.

LSTMs retain information over time. They are useful in time-series prediction because they remember previous inputs. LSTM shave a chain-like structure where four interacting layers communicate in a unique way. Besides time-series predictions, LSTMs are typically used for speech recognition, music composition, and pharmaceutical development.

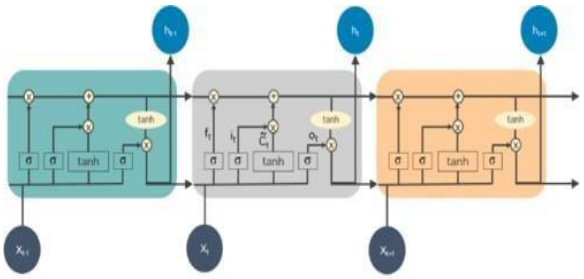

Fig3: Long Short Term Memory Networks (LSTMs)

FEATURE SELECTION

The Feature Selection module in the AMLBot system employs various formulas and equations to identify the most relevant features from the pre-processed transactional dataset. This module aims to select a subset of features that will optimize the performance of the LSTM model for money laundering detection. The Feature Selection module leverages these formulas and equations to determine themost relevant features for money laundering detection. By utilizing statistical tests, information gain, and recursive elimination techniques, this module ensures that the LSTM model is trained on a subset of features that optimize its performance and enhance the system's ability to detect and prevent money laundering activities.

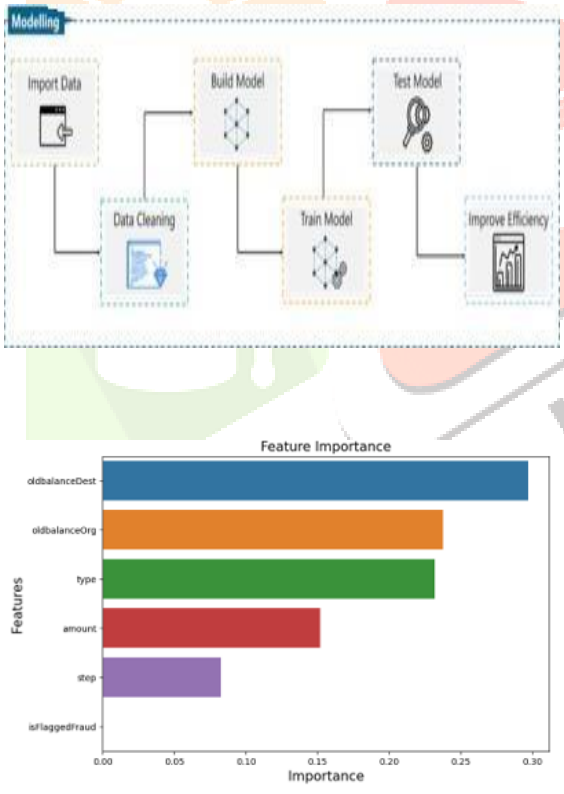

Fig 4: Features selection

EXPERIMENTAL RESULTS

HOME PAGE:

Fig5:Home screen

LOGIN PAGE:

Fig6: Login Page

DATASET LOADING:

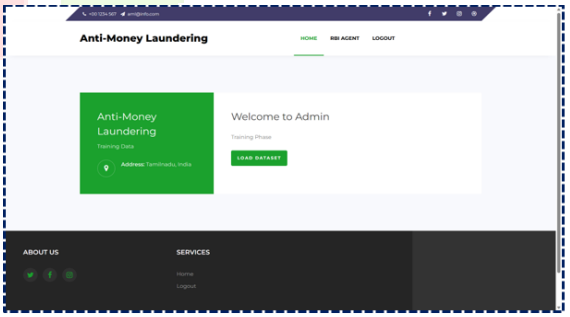

Fig A.2.3: Dataset Loading

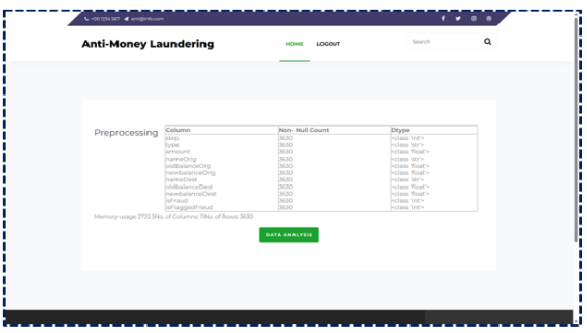

Fig7:Dataset Loading and Processing

CONCLUSION

In conclusion, "AMLBot: An AI Powered Transactional Network and Behaviors Analysis to Detect and Prevent Money Laundering Activities using LSTM" is sophisticated system designed to address the challenges of detecting and preventing money laundering activities in banking transactions. The system leverages LSTM (Long Short-Term Memory) neural networks, along with various data pre-processing and feature engineering techniques, to achieve accurate classification of transactions into legitimate and potential money laundering categories. The performance of AMLBot is evaluated using various evaluation metricssuch as accuracy, precision, recall, and F1-score. Confusion matrix analysis provides a detailed breakdown of true positives, true negatives, false positives, and false negatives, helping to assess the system's performance in detecting money laundering activities.

The results and discussion module provides an in-depth analysis of the system's performance, including the interpretation of findings, identification of limitations, and recommendations for improvement. This analysis serves as a basis for further research and development to enhance the system's capabilities and address any identified challenges. In summary, "AMLBot: An AI Powered Transactional Network and Behaviors Analysis to Detect and Prevent Money Laundering Activities using LSTM" demonstrates promising potential in effectively detecting and preventing money laundering activities in banking transactions. By leveraging advanced AI techniques and robust data analysis, the system contributes to strengthening the efforts to combat financial crimes and maintain the integrity of the banking system.

FUTURESCOPE

The future scope of "AMLBot:An AI Powered Transactional Network and Behaviour Analysis to Detectand Prevent Money Laundering Activities using LSTM" isvast and offers several possibilities for further enhancementand expansion. Here are some potential areas for futuredevelopment:

Integration with External Data Sources: In corporate external data sources such as regulatory databases, watchlists, or public records to enrich the feature set and enhance the model's ability to detect suspicious activities.

Real-time Monitoring and Alerting: Develop a real-time monitoring system that continuously analyses incoming transactions and provides immediate alerts and notifications when potential money laundering activities are identified. This allows for proactive intervention and timely prevention of illicit transactions.

Integration with Anti-Money Laundering Systems: Integrate AML Bot with existing anti- money laundering systems used by banks and financial institutions to provide a comprehensive solution for money laundering detection and prevention.

Global Expansion: Extend the reach of AMLBot beyond the domestic market and adapt it to cater to international financial systems. This would involve addressing regional variations in money

laundering patterns and regulatory frameworks.

Expansion to other industries: While AMLBot was developed for the banking industry, the same approach could be applied to other industries where fraud and money laundering are prevalent, such as insurance, healthcare, and e-commerce.

REFERENCES

1. Kershenbaum, D. (2019). Anti-Money Laundering: AComparative and Critical Analysis of the UK and UAE's Financial Intelligence Units. International Company and Commercial Law Review, 30(8), 353-363
2. Lim, D.,& Sun,P.Y.(2018).Combating Money Laundering: A Comparative Analysis of the EU and US Anti- Money Laundering Directives. Journal of Financial Crime, 25(4), 1035-1050.
3. Ciora, C., &Belu, D. (2019). The Role of Artificial Intelligence in Anti-Money Laundering Systems. Procedia Computer Science, 149, 303-310.
4. Rios-Bolivar, H. (2019). Money Laundering, Terrorism Financing and the Rise of Crypto currencies: Challenges for Developing Countries. Journal of Money Laundering Control, 22(4), 626-642.
5. Siripanich,P.(2020).Effectiveness of Anti-Money Laundering Compliance Systems: Evidence from Thai Commercial Banks. Journal of Money Laundering Control, 23(1), 102-122.
6. Mazurek, M., &Gorczyńska, A. (2020). Application of Artificial Intelligence in Anti-Money Laundering Systems. Central European Journal of Management,28(2),1-20.
7. Fatsaeva, A., & Fazekas, M. (2019). Money Laundering Risk Assessment in Public Procurement: Evidence from Hungarian Local Governments. Crime, Law and Social Change, 72(5),561-582.
8. Chowdhury, A., & Kirkpatrick, G. (2020). The Risk-Based Approach to Combating Money Laundering: A Critical Analysis. Journal of Money Laundering Control,23(2), 265-287.
9. Masciandaro, D. (2018). The Role of Fintech in Anti-Money Laundering. Economics of Security Working Paper, 46, 1-25.
10. Bainbridge,S.(2019).Anti-Money Laundering Compliance and the Law Firm. Journal of the Professional Lawyer, 2019,1-12.
11. Gilder, T., &Sotiropoulos, A. (2018). The Role of Technology in Combating Money Laundering and Terrorist Financing. Journal of Money Laundering Control, 21(4), 479-489.
12. Liu, L., & Tucker, J.(2020). China's Anti-Money Laundering (AML) Regulation and Its Enforcement: A Critical Analysis. Journal of Money Laundering Control, 23(4), 753-772.
13. Bossuyt, J., &Gielen, K. (2019). Money Laundering through Trade: An Overview of the Risks and the Response of Customs Administrations. Crime, Law and Social Change, 72(2), 225- 247.
14. Passas,N.(2018).Anti-Money Laundering: International Law and Practice. Cambridge University Press.
15. Anees, A., & Mohammed, N. (2020). The Challenges of Implementing Anti-Money Laundering

Regulations in the UAE: A Comparative Analysis. Journal of Money Laundering Control, 23(3), 580-600.

16. Levi. (2016).Money laundering. The Annual Review of Criminology, 1(1), 21-40.
17. Chiu, H., Yang, C. C., & Liao, S. Y. (2017). Improving the efficiency of anti-money laundering systems: An empirical study. International Journal of Accounting InformationSystems, 26, 1-18.