Research Output Journal of Engineering and Scientific Research 4(1): 71-78, 2025

ROJESR Publications Online ISSN: 1115-9790

https://rojournals.org/roj-engineering-and-scientific-research/ Print ISSN: 1115-6155

https://doi.org/10.59298/ROJESR/2025/4.1.7178

A Review of Money Laundering Detection Systems

[1]Nnenna S. Nnam, [2]Obikwelu R. Okonkwo, [3]Ihuoma Johnsoon and [4]Godspower Akawuku

[1,2,3,4]Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria

ABSTRACT

Money Laundering is a major challenge and a threat to both financial institutions and government. People steal money from public treasury and launder it to unknown destination. Most often the laundered money is integrated back into the financial system concealing the illicit sources. Most of the money laundered is used to finance terrorism. Terrorism today has become a global threat to the security of every individual. Terrorism clearly has a very real and direct impact on human rights, with devastating consequences for the enjoyment of the right to life, liberty and physical integrity of victims. In addition to these individual costs, terrorism can destabilize Governments, undermine civil society, jeopardize peace and security, and threaten social and economic development. An effective Anti-Money Laundering technique is necessary as it helps in uncovering evidence of criminal activity through identification of suspicious movements of financial assets in the financial institutions. As money laundering is getting more and more sophisticated making it difficult for financial institutions to detect this criminal activity, financial institutions and governments require equally sophisticated systems that are adoptive and flexible to be able to continue detecting money laundering activities. Most of the existing system has some defects which include: Threshold is used to check the volume of money an individual or company can transact in a single transaction. This is defective as the transaction can be broken into pieces to avoid being detected. There is no automatic reporting system to the Anti-money laundering agencies as banks are only mandated to report transactions that exceed the set threshold to the Anti – Money Laundering Authorities. Often banks can renegade on this due to personal interest. This review is aimed at evaluating the success of the available money laundering detection systems, their limitations and gaps that need to be addressed so that the menace of money laundering can be reduced to the barest minimum.

Keywords: Anti-money laundering, Suspicious Transaction Reporting, Threshold

INTRODUCTION

Money laundering (ML) is the term used to describe the method in which fraudsters process illegal money derived from the proceeds of an illegal activity through a succession of transfers and deals until the source of illegally acquired funds is obscured and the money takes on the appearance of legitimate funds or assets. The money laundered can be the proceeds of fraud, insider trading, drug-dealing, human trafficking, embezzlement, bribery, theft or tax evasion. Money laundering can also be seen as a deliberate, complicated and sophisticated process by which the proceeds of crime are made to appear as if they were earned by legitimate means [1]. Money laundering is a three-stage process: The illegally acquired funds must be detached from the predicate crime generating it by generating a series of transactions to distance the proceeds from their illegal source and prevent an audit trail. The process of transferring the proceeds from illegal activities into the financial system in such a manner as to avoid detection by financial institutions and government authorities. The criminal proceeds are then reinvested in furtherance of the business objectives of the launderer. Laundering is the practice of integrating the proceeds of criminal enterprises into the legitimate mainstream of the financial system [2]. It is a technique designed to make illicit acquisition appear legitimate, usually by disguising the property's illegal origin. Money laundering reveals a practice whereby funds obtained from illegal transactions are transferred into secret accounts to shield their detection and possible sanctions [3]. According to International Monetary Fund (IMF), estimated aggregate size of money laundering in the world could be between 2 and 5 percent of global gross domestic product (GDP) [4]. Today, money laundering has become more and more sophisticated and a trait to national peace. Most of the money laundered is used to finance terrorism, religious crises, overthrowing of government, etc. This criminal activity poses a serious threat not only to financial

institutions but also to nations and can result to existential trait. Most countries have established anti money laundering agencies and banks and other international financial institutions and financial agents have been implementing Anti Money Laundering solutions. However, most of the existing commercial solutions are not effective enough as they concentrated on transaction threshold. Those solutions need a lot of customization to directly implement Anti Money Laundering rules, regulations and procedures, and therefore are not full-fledged solutions, especially for detecting and analyzing suspicious transaction.

REVIEW OF RELATED LITERATURES

The review carried uncovers knowledge based anti-money laundering, ontology based expert system for suspicious transaction, money laundering detection using synthetic data, fast detecting suspicious money laundering and an investigation into data mining approaches for anti-money laundering. According to [5] in a paper titled "A Multi-agent Based Approach to Money Laundering Detection and Prevention", the daily bank operations involve huge amount of money and this makes it extremely difficult for financial institutions to detect money laundering related operations. So, the paper presented a multi-agent-based technique for detecting money laundering. They defined a multi-agent system designed to help financial institutions in this task by developing agent architecture, and characterize the different types of agents, considering the distinct roles they play in the process. In the system, they defined a set of entities (agents) with autonomy to perform specific tasks and to engage in communication with others in order to accomplish a certain set of goals. Each agent has its own knowledge and must be able to reason and decide in an intelligent manner. The agents were divided into two groups according to their role in the process. The first group of agents is responsible for the capture of suspicious transactions (CST), whilst the second agents perform the analysis of suspicious transactions (AST) signaled by the agents of the first group. The result of the work shows an explicit integration of learning components and in the inclusion of product specific agents for monitoring money laundering activities. Also, the multi-agent system was the basis of the new decision-making process and it can initiate learning of new rules and parameters that will serve as valuable resources for the agents defined. [6], in their work, A semantic rule based digital fraud detection proposed a solution for curbing digital fraud in the finance industry. According to them, Fraud detection is a reactive process, and it usually incurs a cost to save the system from an ongoing malicious activity. They proposed the use of an Intimation Rule Based (IRB) alert generation algorithm. These IRB alerts are classified based on severity levels. The solution uses a richer domain knowledge base and rule-based reasoning. The work proposed an ontology-based financial fraud detection and deterrence model. [3], presented knowledge-based anti-money laundering software agent bank application first developed to control money laundering and is currently in use among financial institutions to handle complex financial transactions and services, including ML. Knowledge based AML which can be used by intelligent agents in a single bank. Intelligent agent is nothing but a computer system in a bank designed to flexibly and autonomously perform activities to meet specific objectives where flexibility includes properties such as autonomy, social capability, reactivity, and pro activity. Intelligent agents can collaboratively deal with complex problems and vast information in dynamic and unpredictable environments. Knowledge based AML through computer intelligent agents is possible because the agents are versatile with strategies and rules governing business so that actions taken against ML can be justified on legal grounds. In other words, the schema with which intelligent agents function monitoring, diagnosis and reporting activities of ML is compatible with a given business law or organizational culture. For instance, intelligent agents detect transactions made by customers in Sanctions list or with controversial background as potential ML activity. Likewise, accounts, and transactions made with that account, with wire transfers but lacking clear business are detected as high ML risks. However, intelligent agents are not concerned with every detail in transactions since the strategy is to focus on critical components such as client ID, transaction type, transaction date, value data, counter party, etc. The interest to diagnosis and reporting by intelligent agents are: transactions with cash value at or above a certain figure (i.e., large amount transaction); transactions with a special transaction type (i.e., high-risk transaction types defined by FATF, such as wire transfer); transactions with a special counter party (i.e., high-risk customers and business entities, like casino owner or somebody from high-risk countries); and transactions of certain frequencies (i.e., high frequency transactions suggest high-risk customer behavior). Knowledge based AML intelligent agents work in the framework of multiple agents to combat the complex nature of the problem. Although the system is integrated with the entire banking and other financial establishments, it does not interfere with the usual business activities. The Data collecting agent is responsible to collect transaction data based on which to monitoring agents track on the transaction processes. To materialize the multi agent AML framework, the researchers built a prototype in Java so that agents can run on heterogeneous platforms and make use of lightweight applets as temporary agents. But, for prototype evaluation purposes, they used a number of real-world ML cases. The moment ML scheme is detected, the diagnosing agent initiates identification of the problem. The result shows AML platform that focuses on internal data monitoring in a bank, but incapable of monitoring multi-bank transactions and this is the weakness for the research.

[7], stated that the frequency of money laundering cases detected in different countries has generated a wide range of policies with limited results. So they proposed a deep learning strategy to create synthetic data that facilitates the simulation of money laundering schemes using an agent-based model. The applied generative adversary neural network (GAN) methodology that creates synthetic data that is statistically significant to simulate money laundering situations in a network of non-banking correspondents. They built a set of procedures based on special rules to develop the simulation-based in traditional behaviors of suspicious agents. Those procedures identify features that support the robustness of the method to consolidate some recommendations against money laundering because the data is the big problem to fight against this phenomenon. For the agent-based model simulation development for a non-bank correspondent, they needed the environment's definition, business rules, and the identification of suspicious transactions. Those components are defined by agents interacted with non-banking correspondents used through different services. Second, properties are factors that describe the nonbanking correspondents such as deposits, withdrawals, transfers, time, day, and month. Third, the rules are defined to identify risk factors and patterns. However, one of the main rules by the financial institution is that every transaction carried out is subject to a schedule from 8am to 4pm. The range of deposits is between one to five million naira, and withdrawals and transfers are between one to ten million naira. Additionally, for the agents' identification and suspicious transactions, they defined five rules.

1. Transaction Frequency by agent carried out during the year
2. Transaction Frequency by agent and month.
3. Transaction Frequency by agent, branch, and month.
4. Transaction Frequency by agent, branch, month, day, and transaction type.
5. Transaction Frequency by agent, branch, month, time, and transaction type.

Each rule has a greater degree of complexity that allows strengthening the identification of suspicious money laundering transactions. The result from the system proves that the GAN networks generate good quality synthetic data that are statistically consistent. Using this synthetic data with an agent-based model facilitates the creation of robust methodologies for money laundering control on non-bank correspondents. In addition, agent-based models allow a technical explanation of how they carry out money laundering among non-bank correspondents without generating any alert or suspicious activities.

[8], proposed the use of a Bayesian network based on rules from the State Bank of Pakistan and regulations of Pakistan to measure the suspected behavior of customers by assigning them a score. Then, the deviation is computed between the assigned score and the historical behavior of the customer. Once the deviation is significant from defined rules and regulations of normal behavior, the transaction is marked as suspicious and requires further investigation to explain the difference in behavior. The Bayesian network does not allow us to model complicated structures, such as money laundering typologies, but it provides an easy-to-understand visualization of money laundering occurrences.

[9], in his paper proposed a method focused on the relationship between financial accounts based on the social network analysis performed. The paper builds on the assumption that for illegal activities to happen, the interaction between multiple social actors is required. Therefore, the relationships between actors are analyzed by assigning individual weights to actors based on geographical, transactional, and economic factors. Since the study is based on transactions from an Italian factoring business, geographical weights are assigned a risk score depending on the region in Italy. The transactional weight is based on the importance, frequency, and amount of transactions between two actors. The economic factor is referring to historical activities. Similar weight scores, as the scores of each actor, are assigned to the transactions, based on the in-, out-, and all degree of transactions. It concludes that social network analysis is indeed valuable when defining risk profiles and when detection suspicious patterns and transactions. The research also mentioned the increase in informative power when analyzing multiple networks.

Ontology Based Expert-System for Suspicious Transactions Detection was proposed by [4] and it is essential for development of AML software. Because computer science researchers adopt similar standards in their fields of study, the ontology of AML has become sharable and reusable. This has led to the development of expert system AML in which the knowledge based and rules based modeling is integrated to detect suspicious transaction detection. Ontology construction, Ontology reasoning and Query on inferred ontology are the three essential components of the expert system. Ontology Construction includes domain knowledge and rule construction which is done after eliminating noisy data through the stage of pre-processing data. Data pre-processing involves: avoidance of irrelevant data related to transactions below the threshold of Money Laundering guidelines, grouping data (based on amount, date, mode of transaction-debit or credit) and determining frequency of transaction and account status (active or dormant). Ontology Construction relates to establishing the pattern of customers" transactions based on the computation of behavior in the pre-processing stage so that any deviation from the established pattern implies suspicious activity. Establishing a customers" pattern is carried out using Web Ontology Language (OWL) such as class hierarchy, data type properties, object properties, domain range restrictions of each property and instances. Rule construction is the other scene for

Ontology Construction which is presented in Semantic Web Rules Language (SWRL) to identify suspicious transactions. Based on the anti money laundering guidelines the rules for large amount, threshold, dormant account, frequent and mode of transaction should be examined and written into SWRL. The second component is Ontology reasoning, which is applied on the new transaction records. Ontology reasoning is the process of deriving new knowledge that is not explicitly expressed in the initial formulation of customers‟ behavior, using in-built reasoning engines called Pellet reasoning engine. The inference engine infers the class membership as deduced by the rules and populates the Suspicious Transaction class hierarchy. The last component is Query on inferred ontology which can be performed using SPARQL- the standard query language to query ontology. The SPARQL query displays suspicious transactions. The system was tested using multi million bank data taken over a year and resulted in a two percent suspicious transaction. Both suspicious and non-suspicious transactions are the input for the system and the system does not automatically validate suspicious transactions before applying the rules to detect it. Validation of suspicious transactions is the weakness of this research. In proposed framework the suspicious transactions are validated using incidence identification and surveillance of ML processes in individual transactions.

Research from [10], proposes a combination of clustering and classification techniques to detect investment transactions. The paper researches customer behavior in investment activities, seemingly to be fairly complicated to the many factors involved as fund prices, market climate, currency exchange rates, and the political environment. The paper examines two investment values: subscription value, being the value wherefore existing shareholders can participate in company rights offerings. The second value, the redemption value, is the price wherefore an issuing company could buyback securities before the maturity date - the end date of a security. In order to reflect the relationship, the paper uses the following parameters: the proportion of redemption value of the subscription value and the proportion of redemption value of the total value of investors' shares. Using these parameters, the paper tries to cluster groups to detect suspicious transactions. The paper also emphasizes the importance of automation in detection monitoring, since the volume of financial transactions that have to be investigated by financial institutions is increasing. [10], provide promising results of the detection of suspicious transactions using clustering but on the other hand the model requires validation on larger datasets to draw better conclusions.

An interpretable method of machine learning is the Decision Tree. The Decision Tree machine learning technique creates a tree-like structure having one root node and multiple leaf nodes representing categories, including distribution of those categories. It is a prediction and classification method dealing with production rules decided by the Decision Tree itself. [11] use Decision Trees to identify rules of money laundering based on customer profiles of a commercial bank in China. It concludes that Decision Trees are useful to generate anti-money laundering rules from customer profiles. A predictive method of Decision Trees is provided by [2] to discover money laundering patterns and rules. It states to identify suspicious transactions more effectively than rule-based methods.

Money Laundering has a lot of negative implications on the nation's finances and may lead to an increase in the funding of criminal activities [9]. Reasons being that because the large amount of transactions and the variety of techniques money launders uses it is hard for the authorities to discover money launders and prosecute them. So the work proposed an approach, based on Multi-Agent Based Simulation (MABS). The main aim and contribution of their paper work was to study the generation and use of synthetic data as an approach for developing methods for money laundering detection. A case study of different literary work was used as a scientific methodological approach. This leads to the identification of measures on how to detect and control that which could be applied in similar circumstances. The task at hand is to develop an approach that detects suspicious activities that are indicative of money laundering. With the issue of large amount of transactions taking place in a financial service, it is a task to find specific transactions that should be questionable. The suspicious activity needs to be aided with tangible evidence that allows government agencies to investigate more on the reported money laundering. Several machine learning techniques have been used for the detection of fraud, and more specifically money laundering. Data mining based methods have also been used to detect fraud. This leads to the findings that machine learning algorithms can identify methods of fraud by detecting those transactions that are different in comparison to the transactions. Supervised algorithms have been used on synthetic data to prove the performance of outlier's detection in a different domain.

[11], introduced fast detection of suspicious money laundering [5]. In order to develop a new solution for international investment bank, they proposed a data mining-based solution for Anti-money laundering (AML). In this work they focused on heuristics approach to improve the performance for this solution. Getting money laundering pattern is one of the goals of this research and important to support AML software. Data mining techniques are best suited for identifying trends and patterns from large datasets from banks. According to the researcher's perspective, all previous works regarding ML and data mining have poor performance which can be improved through clustering approach basing on some heuristics from AML experts. They considered that only the maximum (redemption) and minimum (subscription) transactions are important to calculate suspicious

transaction. But they divided transaction datasets into two: individual and corporate, although they focused on the corporate datasets. Then they applied a two-step procedure: suspicious screening and clustering process. Suspicious screening is the process of taking suspicious data from the whole data set while center based clustering technique is applied for simplicity and effectively. Applying heuristics in suspicious screening process is done by changing the parameters as many times as possible to determine the suspicious group using clustering algorithm. Suspicious and non-suspicious groups are then fed into a neural network for training and their results are stored in a knowledge-base. The drawbacks of this work is classifying the transactions and taking only corporate data. But there exist ML cases from the individual transactions. So that the proposed framework recommended finding suspected transactions from both corporate and individual transactions.

[12], in their research analyzed the implications of machine learning techniques to detect money laundering. To do so, they used a set of supervised algorithm generated synthetic data from a company providing mobile phone financial transactions [12]. The system was developed to combat ML encountered in three levels of transactions: normal, suspicious and misclassified as anomalies. The researchers used IDAS data and scenario generator tool to generate synthetic data based on the relationship between customer attributes and their statistical distributions. Besides, they adopted Gao's work about AML terms like legal transaction, usual transaction, unusual transaction, suspicious transaction and illegal transaction [13]. The method proved effective in successfully distinguishing high True Positives from law False Positives. Next to learning the problem is data pre-processing which includes data cleaning and adding some necessary attributes like Customer ID, Profile, Date of the Transaction, type of transaction Amount of the Transaction and city. Once the attributes are formulated, data is labeled anomalous if the amount of withdrawal and deposit is too large or small relative to predefined threshold then drops the small amounts transactions and uses too large amount transactions. Synthetic data was used to train the classifier and test the improvement of detection rate (True Positive) and reduce the misclassification rate of benign data (False Positive). The possible algorithm for detection is analyzed based on Decision Tree Learning and Clustering Techniques. Decision Tree learning algorithm for the domain of mobile money AML is the possibility for an investigator to determine common rules that classify suspicious behavior. Besides, Clustering Techniques such as distance and density based detection were implemented but it is difficult to find abnormal behavior of the clusters. Due to the lack of real data in this work they used synthetic data, which is important to analyze class imbalance or class overlap proposed by the research. But using synthetic data has its own impact on the research. So that the researcher proposes Multi agent based simulation. One of the main drawbacks of this research is generating the synthetic data which might not represent the real data. And the output from machine learning would bias to use as an output.

The research in [10], seeks to develop a data mining framework for Anti Money Laundering by generating rules and models which are useful for business performance and creating patterns. In addition, the framework helps to investigate money laundering activities. Banking and financial institutions use two kinds of data, one is the archived and stored as historical data and the other is live transaction data. Both archived and live transaction data handled daily and becomes too huge. The process of customer transaction details in individual level is quite difficult. Managing and analyzing effectively this transaction data upon the request using traditional way is much beyond human capacity. Moreover, traditional investigative techniques and approaches are labor intensive and consume numerous man-hours. Definitely, the daily volume of banking transactions has increased in various ways daily which means that approaches need to be supported by automated tools for detecting and investigating money laundering's pattern. Accordingly, this research work is motivated to show how data mining techniques should be applied successfully in AML through developing an AML solution based on Data Mining. Data Mining Prediction can perform different techniques of clustering, classification, regression, association rule discovery and sequential pattern discovery. AML task involves the detection of unusual behavior of all dimensions in transactions, accounts, product types, etc. In AML, from data mining clustering is normally used for grouping transactions of accounts into clusters based on their similarities of their features transaction types. This technique helps in building patterns of suspicious sequence of transactions and detecting risk patterns of customers holding accounts. Above all the researcher observed that there are challenges in implementing data mining framework to investigate money laundering. Data quality, data volume and heterogeneity of data and the nature of ML are the main challenges to use the framework. To improve the data quality issue there must be data mining preprocessing techniques applied. Data heterogeneity and distribution of data in different places, is solved by data mining integration techniques recommendations and implementations. The nature of ML can differ with technological advancement of using financial instruments which is a challenge for all kinds of frameworks and AML solution development. For the realization of the objectives of this study, the researcher hypothesizes that classification and clustering are the two important mining methods that can efficiently be applied for AML. Furthermore, rule based AML solutions have been replaced by artificial intelligent approach for AML; unsupervised learning with a small set of training data is suitable for building Data Mining based solutions for AML. In order to exploit Data Mining techniques efficiently, they need to be integrated in a

framework for detecting Money Laundering. The weak point in this research is because of nature of ML it is difficult to identify ML activities from the transaction data.

Table 1: Summary of Methods Applied for Money Laundering Detection

AUTHORS	TITLE	METHOD USED	LIMITATIONS
[12]	Money Laundering Detection using Synthetic Data,	Supervised Algorithm synthesized data	Not tested on real data
[6]	A semantic rule based digital fraud detection.	Intimation Rule Based (IRB) alert generation algorithm	Not specific on money laundering fraud.
[3]	Hiding Money Laundering with an Intelligent Multi-Agent System Simulation	Multi-agent based technique	This research assumed that detecting at least one of the money laundering transactions will result in finding the complete network, however in reality this is most likely not the case.
[5]	A Multi-agent Based Approach to Money Laundering Detection and Prevention	Multi-agent based technique	Unable to monitor transaction of individuals indifferent banks
[14]	A data mining-based solution for detecting suspicious money laundering cases in an investment bank.	Data mining	Tested for small dataset. May not be very effective with very large data set.
[4]	Knowledge-based anti-money laundering: A software agent bank application	Knowledge-based	Monitors single bank at a time.
[7]	Deep Learning-based Synthetic Data for Money Laundering Control Simulations.	generative adversary neural network (GAN) generative adversary neural network (GAN) methodology	Date availability to consolidate the fight against ML.
[8]	A Bayesian approach for suspicious financial activity reporting.	Bayesian network based on rules	Dedicated to an institution per time.
[11]	money laundering detection based on improved minimum spanning tree clustering and its application.	Spanning tree clustering Method	One bank at a time.
[9]	Ontology Based Expert-System for Suspicious Transactions Detection,	Ontology Based Expert System	The expert system does not automatically validate the suspicious transactions rather it applies the rules to detect suspicious transaction.
[11]	A Money Laundering Risk Evaluation Method Based on Decision Tree	Decision Tree	Based on customer profile, may not handle smurfing appropriately

[9]	Using social network analysis to prevent money laundering.	Network analysis technique	Analysis of the tacit links existing among different companies who share the same owner or representative.

SUMMARY OF LITERATURE REVIEW AND RESEARCH GAP

From the literatures reviewed, we can see that anti money laundering policies, procedures and researches not only contribute towards the safety and systematic way of controlling ML but also assist the protection of the integrity of the financial systems. The multi agent for tackling money laundering to achieve knowledge-based solution proposed by researchers allows integrating anti-money laundering techniques with specific knowledge about business rules and business strategies. But it is implementable only in one bank transactions hence cannot be implemented in multiple banks. The other related work belongs to Expert system using ontology which is a good choice for incorporating both knowledge base and rule-based modelling. However, the expert system does not automatically validate the suspicious transactions rather it applies the rules to detect suspicious transaction. Detection of money laundering through machine learning using synthetic data represents an improvement of detection rate (True Positive) and reduces the misclassification rate of benign data (False Positive). However, this system has not been tested for accuracy based on real data. From this review we detect the need to deploy a system which can integrates the various features of models discussed above and can also be integrated on the network to monitor all financial institutions for money laundering activities and report suspicious transaction to Anti- Money Laundering agencies.

REFERENCES

1. Norman Mugarura, 2020. "Anti-money laundering law and policy as a double edged sword," Journal of Money Laundering Control, Emerald Group Publishing Limited, vol. 23(4), pages 899-912, March.
2. Sullivan, K. (2018), Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business, 1st Edition, A Press, Berkeley, CA.
3. Nlerum, O. (2017)_'Regulation of money Laundering in Africa; The Nigerian and Zambian approaches" Journal of Money Laundering Control
4. Financial Action Task Force (FATF) (2018), "Basic facts about money laundering", available at: www. fatf-gafi.org/document/29/0,3343,en_32250379_32235720_33659613_1_1_1_1,00.html#howmuch moneyislaunderedperyearm (accessed March 2024)
5. Claudio, A. & Joao, B. (2020) A Multiagent Based Approach to Money Laundering Detection and Prevention. DOI: 10.5220/0005281102300235 In Proceedings of the International Conference on Agents and Artificial Intelligence (ICAART-2020), pages 230-235 ISBN: 978-989-758-0,73-4
6. Ahmed M, Ansar K, Muckley C. B, Khan A, Anjum A. & Talha M. 2021. A semantic rule based digital fraud detection. PeerJ Comput. Sci. 7:e649 http://doi.org/10.7
7. Edwin, G. , Olmer, G. & Oscar, M. G. (2019) Deep Learning-based Synthetic Data for Money Laundering Control Simulations. Department of Industries and Digital Technologies, Universidad Jorge Tadeo Lozano, Bogotá, Colombia
8. Khan, N. S., Larik, A. S., Rajput, Q. & Haider, S. (2019). A Bayesian approach for suspicious financial activity reporting. International Journal of Computers and Applications, 181- 187.
9. Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. Expert systems with Applications, 49-58.
10. Le Khac, N. A., Markos, S., & Kechadi, M.-T. (2020). A data mining-based solution for detecting suspicious money laundering cases in an investment bank. Second International Conference on Advances in Databases, Knowledge, and Data Applications, 235-240.
11. Wang, S.-N., & Yang, J.-G. (2017). A Money Laundering Risk Evaluation Method Based on Decision Tree. International Conference on Machine Learning and Cybernetics, 283- 286.
12. Le-Khac, N., Sammer, M. and M-Tahar, K. (2019) A Heuristics Approach for Fast Detecting Suspicious Money Laundering Cases in an Investment Bank. World Academy of Science, Engineering and Technology 60, 2019.
13. Dennis, M. A. (2024). Cybercrime. Encyclopedia Britannica, Retrieved from: https://www.britannica.com/topic/cybercrime. Accessed 7 October 2024.
14. Liu, R., Qian, X.-l., Mao, S. & Zhu, S.-z. (2018). Research on anti-money laundering based on core decision tree algorithm. Chinese Control and Decision Conference, 4322- 4325.

CITE AS: Nnenna S. Nnam, Obikwelu R. Okonkwo, Ihuoma Johnsoon and Godspower Akawuku (2025). A Review of Money Laundering Detection Systems. Research Output Journal of Engineering and Scientific Research 4(1): 71-78.https://doi.org/10.59298/ROJESR/2025/4.1.7178