International Journal of Entrepreneurship and Management Practices
IJEMP
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

INTERNATIONAL JOURNAL OF ENTREPRENEURSHIP AND MANAGEMENT PRACTICES (IJEMP)
www.gaexcellence.com/ijemp

ALGORITHMIC MECHANISMS IN ANTI-MONEY LAUNDERING SYSTEMS: A SYSTEMATIC REVIEW OF EFFECTIVENESS AND PERFORMANCE

Roshima Said[1*], Salwa Zolkaflil[2], Nur Zharifah Che Adenan[3]

[1]Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Kedah, Kampus Sungai Petani, Kedah, Malaysia
roshima712@uitm.edu.my https://orcid.org/0000-0003-3262-4566
[2]Accounting Research Institute, Universiti Teknologi MARA, Selangor, Malaysia
salwazolfaflil@uitm.edu.my https://orcid.org/0000-0002-1039-3448
[3]Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Kedah, Kampus Sungai Petani, Kedah, Malaysia
zharifah@uitm.edu.my https://orcid.org/0009-0002-9816-4371
*Corresponding Author

Article Info:

Article history:
Received date: 28.01.2026
Revised date: 15.02.2026
Accepted date: 26.03.2026
Published date: 31.03.2026

To cite this document:

Said, R., Zolkaflil, S., & Che Adenan, N. Z. (2026). Algorithmic Mechanisms in Anti-Money Laundering Systems: A Systematic Review of Effectiveness and Performance. *International Journal of Entrepreneurship and Management Practices, 9*(33), 633-651.

Abstract:

This study provides a comprehensive review and classification of the current literature on algorithmic approaches for combating money laundering. A systematic literature review (SLR) was conducted using the Universiti Sains Malaysia (USM) Digital Library. After applying the inclusion and exclusion criteria, 27 relevant publications published between 2015 and 2020 were selected for analysis. A classification framework was developed to analyse the selected studies, which includes solutions, machine learning, data sources, assessment techniques, implementation tools, sampling approaches, and study regions. The findings provide insights into the current research landscape of algorithmic anti-money laundering (AML) systems and identify trends, gaps, and opportunities for future research.

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

DOI: 10.35631/IJEMP.933038 **Keyword:**

Algorithms, Anti-Money Laundering Systems, Detection, Machine Learning, Systematic Literature Review

Introduction

Money laundering is a significant issue that governments across the globe are debating. Money laundering is the world's third-largest industry, representing approximately 2.7 percent of global GDP, behind only the currency exchange and the automobile sectors (Soltani et al., 2016; Le-Khac et al., 2016). The International Monetary Fund (IMF) estimates that money laundering revenues make up from 2% to 5% of global GDP (Syed Mustapha Nazri et al., 2019). Furthermore, the United Nations Office on Drugs and Crime (UNODC) estimates that annual global money laundering ranges from $500 billion to $1 trillion, with drug trading accounting for between $400 billion to $450 billion of that amount (Le-Khac et al., 2016).

The act of disguising the illegal origins of ill-gotten profits while passing them off as legitimate and legal is referred to as money laundering (Le-Khac et al., 2016). Furthermore, money laundering is the process of cleansing "dirty" money, which includes cash acquired via illicit or unlawful activities such as drug trading, prohibited gambling, and tax fraud (Salehi et al., 2017; Soltani et al., 2016). The "process of turning untraceable funds into traceable funds" is another term for money laundering (Suresh et al., 2016). Money laundering can be divided into three phases: placement, layering, and integration. Placement's first phase involves the illegal purchase and entry of money into the financial system. The money source is then concealed throughout the layering step by dividing it among numerous intermediaries. Finally, the illicit money is handed to the owner during the integration stage (Savage et al., 2017; Salehi et al., 2017; Suresh et al., 2016; Soltani et al., 2016; Alexandre & Balsa, 2015). Since both the illegal and the legitimate sources of funds are connected, law enforcement officials have found it incredibly difficult to determine the actual degree of money laundering due to the intricate structure of money laundering operations. As international commerce, the international financial system, and technological progress continue to expand; criminals have access to a source of money, opportunities to launder it, and methods to do so. Many businesses see it as a once-in-a-lifetime opportunity since it significantly boosts the likelihood of their success when they reach the global market. As a direct result of this issue, the Financial Action Task Force (FATF) devised international legislation, standards, and public awareness campaigns to combat money laundering and the financing of terrorist organizations.

When financial institutions began informing governments of significant transactions, money laundering was first identified. To pinpoint machine learning trends in the late 1990s, statistical techniques including Bayesian models and temporal sequence matching were used. A similar approach was applied using machine learning in 2004. Models of the radial-based function neural network, support vector machine (SVM), and C4.5 decision tree (DT) are the most widely utilized methods for identifying machine learning activities (Soltani et al., 2016). Anti-money laundering is a term used to describe a system that prevents money laundering (AML).

Money laundering was first identified in 1970 when financial institutions began reporting large transactions to governments. Statistical approaches such as Bayesian models and temporal sequence matching were used to discover machine learning trends in the late 1990s. In 2004, a similar strategy was used using machine learning. The C4.5 decision tree (DT), the support vector machine (SVM), and the radial-based function neural network model are the methods that are most frequently utilised for identifying machine learning activities (Soltani et al., 2016). Anti-money laundering (AML) is a system that prevents money laundering.

The Financial Action Task Force (FATF) seeks to establish norms and reinforce judicial, administrative, and operational safeguards against the funding of terrorism, money laundering, and other dangers to the global financial system [FATF 2020]. In essence, most governments are constantly striving to improve their systems in order to minimize or eradicate money-losing illegal operations (Syed Mustapha Nazri et al., 2019). Furthermore, governments all around the globe have introduced legislation and issued guidelines to fight money laundering. For example, the Financial Transactions and Reports Analysis Centre is in charge of establishing laws and policies that impact Canadian accountants, banks, and real estate companies. The Financial Crimes Enforcement Network (FinCEN) supervises and provides recommendations to financial institutions in the United States of America. FinCEN carries out its goal by storing and maintaining financial transaction data, analyzing and distributing such data for law enforcement purposes, and encouraging international cooperation with equivalent agencies in other nations. Furthermore, international organizations such as the FATF formulate regulations and make suggestions on money laundering prevention (Soltani et al., 2016).

The current pandemic scenario has had catastrophic health and economic consequences worldwide due to the COVID-19 outbreak. To make things worse, criminals seek ways to profit from the calamity. According to a Financial Action Task Force (FATF) (2020) analysis from 2020, criminals continue to profit from the pandemic's opportunities across the globe, with more incidences of counterfeiting medical goods, investment fraud, integrated cyber-crime schemes, and exploitation of government economic stimulus programs. Furthermore, the report reveals that there have been cases of online child exploitation due to an increase in virtual time spent, property crime due to vacant properties, and medical supply contract corruption. Criminals benefit from chaos and are only concerned with their own personal and financial gain in a bleak situation. In addition, the UNODC reported in 2020 that money laundering remains a crucial enabler of COVID19-related organized crime, with a significant increase in fraud such as the purchase of fraudulently obtained genuine medical equipment and medicines; the non-delivery of advertised equipment; and the redirection, interception, and misuse of funds.

International Journal of Entrepreneurship and Management Practices
IJEMP
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

Money laundering has far-reaching implications for businesses, economies, and society. The effects of money laundering on the political and economic systems of developing nations were analyzed by Aluko and Bagheri (2012), who also looked at the efficiency of the legal procedures in place to counteract the threat of money laundering. According to the research, money laundering and other financial crimes have deep cultural roots in Nigeria. They can only be eradicated with the full force of the law, sound governance, and joint efforts worldwide. The research concluded that economic and financial crimes in Nigeria had become a pernicious trend, ranging from serious to premeditated. The study recommended that the country's constitutional and administrative boundaries be re-evaluated to control, restrain, and regulate financial crimes properly, so they do not hinder growth.

Due to the severe consequences of money laundering for businesses, economies, and society, this paper attempts to conduct a systematic review of the literature (SLR) focusing on the efficacy of existing anti-money laundering (AML) strategies that employ machine learning and other methodologies to detect fraudulent activity. Furthermore, only a few studies systematically analyze current literature, and a few SLRs focus on exploring the effectiveness of anti-money laundering (AML) methods that employ machine learning and other approaches to identify suspicious transactions.

Literature Review

Focus and Scope of the Research

This study's objective is to evaluate the effectiveness of different detection methods proposed by researchers as well as anti-money laundering (AML) procedures. Machine learning applications, social network analysis, deep learning, and other AML solutions are the main focus.

Research Framework

The state of the art in AML approaches was determined using an SLR analysis and the research question is “What tools and tactics are being used to identify money-laundering activities?”

The SLR was executed with the assistance of the Digital Library as well as English-language resources such as Springer, IEEE Xplore, Science Direct, Emerald Insight, and the ACM. Most of the articles in the sample were published between 2015 and 2020, with two from 2010 and one from 2011. Keywords like "anti-money laundering," "money laundering," "money laundering detection," and "anti-money laundering systems" were used to search the digital library for relevant articles. After excluding documents that were not included in the scope of the study, the final sample size was 27 documents.

Screening

Numerous criteria are established for eligibility and exclusion. Only empirical article journals are considered, meaning that review articles, book series, books, book chapters, and conference proceedings are excluded. Second, the search efforts focused exclusively on English-language articles to avoid ambiguity and difficulty in translation. Thirdly, a timeline

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

of five years (between 2015 and 2020) is chosen because it allows sufficient time to observe the evolution of research and related publications.

Due to the review process's emphasis on adapting practices to money laundering, only articles indexed in Elsevier BV's Emerging Sources Citation Index, Clarivate Analytics Social Science Citation Index, and Journal Citation Reports/Social Sciences Edition indexes were considered. In comparison, articles from a hard science index (Science Citation Indexed Expanded) were excluded. Table 1 and Figure 1 detail the screening criteria and frameworks.

Table 1: The Inclusion and Exclusion Criteria

Criterion	Eligibility	Exclusion
Literature Type	Journal (research articles)	Journals (systematic review), book series, book, chapter in book, conference proceeding
Language	English	Non-English

Outputs

The publication status of all outputs in peer-reviewed journals was the only criterion for evaluation. There are no patent applications, lecture notes/slides, software items, or information websites in the sample frame. Table 2 depicts the sample's temporal distribution in terms of when outputs were published.

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

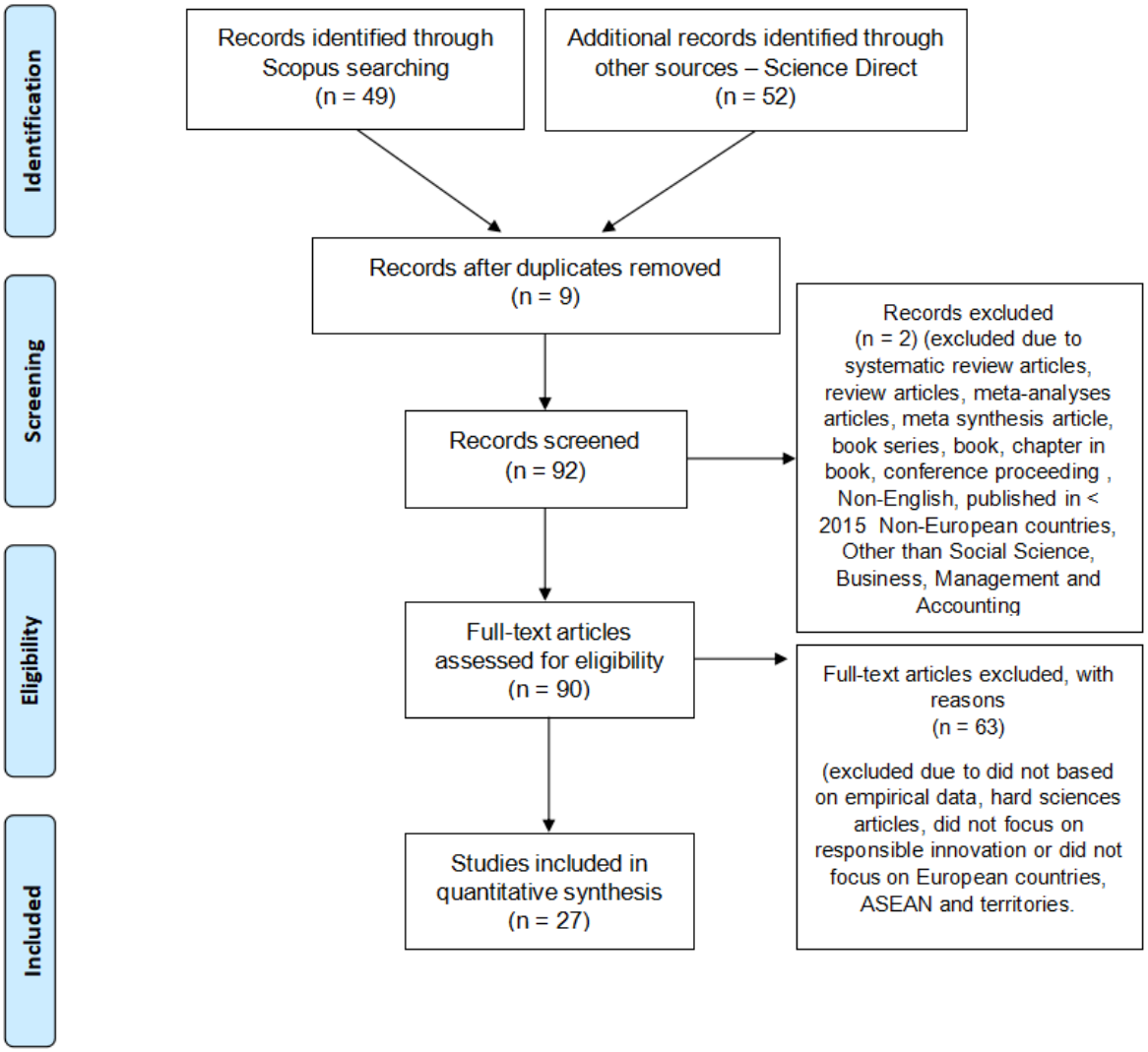

Figure 1: Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)

Table 2: Published Articles in Money Laundering Field with Years of Publication

Year	Publication
2010	Detecting Money Laundering using Filtering Techniques: A Multiple Criteria Index (Yang and Wei,2010)
	Application of Data Mining for Anti-Money Laundering Detection: A Case Study (Le Khac and Kechadi, 2010)
2011	Research on Anti-Money Laundering based on Core Decision Tree Algorithm (Liu at al., 2011)
2015	Comparison of Data Mining Techniques for Money Laundering Detection System (Rafa Drezewski et al., 2015b)
	Anti-Money Laundering using A Two-Phase System (Moustafa et al., 2015)
	The Application of Social Network Analysis Algorithms in A System Supporting Money Laundering Detection (Rafa Drezewski et al., 2015a)
	Multiagent based Approach to Money Laundering Detection and Prevention

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

	(Alexandre and Balsa, 2015)
2016	Integrating Client Profiling in An Anti-Money Laundering Multiagent based System (Alexandre and Balsa, 2016)
	Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering (Paula et al., 2016)
	An Efficient Search Tool for An Anti-Money Laundering Application of An Multi-national Bank's Dataset (Le Khac et al., 2016)
	A new Algorithm for Money Laundering Detection based on Structural Similarity (Solfani et al., 2016)
	A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering using Data Mining Techniques (Suresh et al., 2016)
2017	Detection of Money Laundering Groups: Supervised Learning on Small Networks (Savage et al., 2017)
	A Statistical and Machine Learning Model to Detect Money Laundering: An Application (Villalobos and Silva, 2017)
	Money Laundering Regularly Risk Evaluation using Bitmap Index-based Decision Tree (Jayasree and Siva Balan, 2017)
	Anti-fraud System on The Basis of Data Mining Technologies (Sapozhnikova et al., 2017)
	Autoregressive-based Outlier Algorithm to Detect Money Laundering Activities (Kannan and Somasundaram, 2017)
	Intelligent Anti-Money Laundering Solution based Upon Novel Community Detection in Massive Transaction Networks on Spark (Li et al., 2017)
	Using Social Network Analysis to Prevent Money Laundering (Colladon and Remondi, 2017)
2018	Deep Learning Approach for Intelligent Financial Fraud Detection System (Mubalaike and Adali, 2018)
	Combining Benford's Law and Machine Learning to Detect Money Laundering: An Actual Spanish Court Case (Badal-Valero et al., 2018)
	Fighting Money Laundering with Technology: A Case Study of Bank X in the UK (Demetis, 2018)
	Analysing and Detecting Money-Laundering Accounts in Online Social Networks (Zhou et al., 2018)
	Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection (Zhang and Trubey, 2018)
2019	Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity (Singh and Best, 2019)
	Fraud Detection Decision Support System for Indonesian Financial Institution (Lawrencia and Ce, 2019)
2020	Detecting Money Laundering Transactions with Machine Learning (Jullum et al., 2020)

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

Result: Research Outputs' Categorise

Anti-money Laundering Practices

This section deliberated AML systems that custom novel outlines or approaches not classified as machine learning or deep learning. Soltani et al. (2016) offer a one-of-a-kind framework for analysing bank account transactions and compiling a list of potentially illegal transactions The process begins with analysing input data and identifying transactions with similar characteristics (e.g., parallel deposit and drawing amounts). The system then creates a visual representation of all similar transactions. The score is then used to improve accounts and transactions using a network-based approach. The approach leverages clustering to identify questionable clusters. The framework's output would then reconstruct and classify the apprehensive communities.

Moreover, Le-Khac et al. (2016) developed an anti-money laundering (AML) system that is compatible with bank databases. Using an index tree, the author built a search engine and linked Web services, resulting in a system that is accessible to either end administrators or users. Their solution assists banks in addressing data quality issues and providing a consolidated view of all customer data without requiring organisations to change their current database architecture. Social networks were created and tested using data from banks and the National Court Register to explore machine-learning scenarios. In collaboration with the Polish National Police, the Money Laundering Detection System (MLDS) was developed to help police investigations (Rafa Drez ewski et al., 2015a).

In addition, a two-phase plan-based framework for AML systems was created. Without such a requirement, the monitoring phase is utilized to detect potential money laundering. It employs various methods, including rule-based analysis, feature extraction, clustering, and cycle detection. Furthermore, as Moustafa et al. (2015) demonstrated in their research, the STRIPS-based phase is utilized to strengthen perceptions of suspicious transactions. Moreover, Singh and Best (2019) describe how link analysis may be utilized to analyze bank transactions and detect suspicious behavior using visualization techniques. The prototype was created in four stages: job analysis, which identified the issue to be solved; system design, which clarified the data, procedures, and interactions; implementation, which intended to operationalize the system as a proof of concept; and running tests, which ascertained whether the system achieved its goal. The prototype is known as AML2ink.

Kannan and Somasundaram (2017) formerly recommended a three-sided boundary-based outlier detection (TBOD) and an autoregressive-based outlier algorithm for detecting money laundering in an online bank transaction data set (AROMLD). Outliers are identified using two different models, TBOD and AROMLD. By segmenting the data into risk and product user groups, the TBOD method applies a triangle area map to customer profiles to identify correlations between transactional information. AROMLD was an alternative technique that comprised mean, zero mean, auto regression, and interquartile range (IQR) processes; these processes would detect machine learning (ML) activities during data extraction and then differentiate between normal and outlier transactions using the regression deviation-based IQR as a threshold. As a result, if the regression value exceeds the cut-off value, it is classified as an outlier. Otherwise, the value would be considered standard.

International Journal of Entrepreneurship and Management Practices
IJEMP
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

In contrast, Yang and Wei (2010) created multiple detection methods (MDA) for identifying machine learning phases based on data evidence (placement, layering, and integration). The MDA is made up of three models. The first step is to use an outlier identification methodology to analyse transaction volume and frequency. The second model was a trading correlation test that was designed to help businesses identify unusual trades or transactions. Using Benford's law, the final model detected financial fraud. The outputs of all three models are added together to yield a score ranging from 0 to 3 (indicating no machine learning suspicion) (high ML suspicion).

Demetis (2018) adds another significant contribution by refining the valid positive rate (TPR) of transaction monitoring systems using data from a case study bank; AML evaluation metrics are then created for AML system decision-makers. Furthermore, the study offered a conceptual foundation for detection through machine learning. By improving a temporal-directed Louvain algorithm on the Spark GraphX platform, Li et al. (2017) developed a method for identifying suspicious activity in massive transaction networks. Individuals with a high-risk score would therefore be deemed abnormal. Furthermore, Colladon and Remondi (2017) presented predictive models based on social network metrics (SNA) to evaluate the risk associated with customer profiles; the approach allowed visual examination of previously undiscovered connections between companies owned by the same individual. As a result, the researchers concluded that this approach might be used to anticipate risk profiles.

Supervised Machine Learning

Friedman et al. (2001) define supervised learning as "predicting the value of an output measure given a variety of input measurements." The term "teaching with a teacher" is also used. Savage et al. (2017) created an end-to-end solution to this approach by automating machine learning identification through group behavior analysis in bank transactions. The system, which is designed for use by the Australian Transaction Reports and Analysis Centre, employs network analysis as well as supervised learning [through support vector machine (SVM) and random forest (RF) classifiers] (AUSTRAC). Similarly, Zhang and Trubey (2018) provide empirical research that shows how machine learning can recognize unexpected events and machine learning operations. These researchers examined five algorithms: decision trees, reinforcement learning, support vector machines, artificial neural networks, and Bayes logistic regression (BLR).

Additionally, maximum Likelihood Logistic Regression (MLLR) was utilised by the researchers as a control in their regression model. Villalobos and Silva (2017) also created a classification model for suspect transactions that combines five different classification models: SVM, C5.0, C&RT, neural network, and chi-squared automatic interaction detector (CHAID). The most accurate findings came from C5.0.

A detection technique developed by Zhou et al. (2018) combined features with a statistical classifier like an SVM, RF, or logistic regression (LR). As well, three classifiers were added to a transactional monitoring system: a multilayer perceptron, a support vector machine, and a random forest (Sapozhnikova et al., 2017). Furthermore, Badal-Valero et al. (2018) showed that the suggested approach, which combines Benford's law with machine learning methods such as LR, DT, neural networks, and RF, assisted in identifying machine learning features in a real-world Spanish court case. Lawrencia and Ce (2019) developed a decision-support system to help financial organizations detect fraudulent transactions. Consequently, the

finished output is displayed in an easy-to-use dashboard style. The categorization is scenario-based, and three different classification techniques are used:

a) A SQL statement that validates the whole transaction amount;
b) SQL aggregate techniques that utilize a one-tail normal distribution to discover outliers and subsequently detect suspicious transactions; and
c) Outliers in the linear fit are identified using robust regression.

For assessing the hazards of financial machine learning, Jayasree and Siva Balan (2017) created the bitmap index-based decision tree (BIDT) method. A data structure called a bitmap index enables consumers to access enormous bank datasets. Indexing is utilised in BIDT to provide table row hints, and the DT method is used to break the decision down into smaller components to assess machine-learning activityA supervised machine learning model was used by Jullum et al. (2020) to track financial transactions at DNB Norway in order to spot money laundering operations and differentiate between reported and unreported transactions. The bank determines unlawful behavior in three stages: alert, case, and reporting. They used an incremental boosting framework in conjunction with a tree model. They fitted the model using tenfold cross-validation during the training stage, and they selected the hyperparameters via local and iterative grid search. As a result of the model's complexity, the researchers tried to combine an ensemble XGBoost model with RF, Glmnet, or another GBoost configuration but were unsuccessful.

Unsupervised Machine Learning

Unsupervised learning is defined by Friedman et al. (2001) as " a process with the goal of describing the relationships and patterns among a group of input variables but no outcome variable"

The researchers proposed a method for circumventing machine learning by association mining with a hash-based technique over an Apriori algorithm, followed by graphical theoretic detection of suspicious activity. By introducing a knowledge-based method, Le Khac and Kechadi (2010) expanded the concept of suspicious transaction detection. This approach is made up of two parts: analysis and inquiry. The K-means clustering method was used in research. The resultant set would be labeled as suspicious or untrustworthy (a few data objects in the suspect group and the majority in the untrustworthy group). A genetic algorithm with single-point crossover would then be used to increase the number of data items in the suspect set. The output would be fed into the neural network during training. In addition, the DT would signify and store the outcome in the knowledge base to assist machine learning experts in making an educated choice throughout the inquiry process.

Meanwhile, the MLDS was built using the Apriori, PrefixSpan, FP-growth, and Eclat algorithms. The Apriori approach categorizes money transfers based on actions done at a particular time or with a specified amount. PrefixSpan is a pattern recognition method that detects sequential patterns in a database. FP-growth is a practical approach for frequently identifying recurring items. The Eclat methodology should be used when the database is essential since it is a greater association rule algorithm in these conditions (Rafa Drez ewski et al., 2015b).

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

AutoEncoder has also shown unsupervised deep learning and dimensionality reduction using principal component analysis (PCA) (Paula et al., 2016). The reason why AutoEncoder is the most widely used technique for anomaly identification is because the researchers discovered that PCA was more computationally expensive than it was. A stacked auto-encoder (SAE), a limited Boltzmann machine, and other learning and deep learning Mubalaike and Adali (2018) to create an efficient financial fraud detection system (RBM) used techniques. Liu et al. (2011) used a DT based on balanced iterative reduction and hierarchical clustering (BIRCH) and K-means clustering algorithms to identify abnormal behaviors. To split n items into k groups, K-means clustering was employed, while BIRCH hierarchical clustering was used to accommodate substantial data sets. The BIRCH method was insensitive to noise and underperformed with financial data; the K-means technique outperformed in all areas however it was too slow for large data sets. Due to these reservations, the core DT was constructed utilizing previously developed clustering methods.

Furthermore, financial organisations can handle two important issues: volume and rule improvement, by employing a multi-agent-based approach to machine learning operations. Agents are categorised by the system based on how involved they are in the process. While the second agent is in charge of analysing and making decisions about suspicious transactions observed by the first agent, the first agent is responsible for documenting and reporting suspicious transactions (Alexandre and Balsa, 2015). By including classification and clustering methods, Alexandre and Balsa (2016) improved the approach described in Alexandre and Balsa (2015). Table 3 and Figure 2 summarize the methods utilized in the selected articles.

Table 3: Algorithms for Detecting Money Laundering.

Algorithms	Articles Research
SVM	Savage et al. (2017), Zhang and Trubey (2018), Villalobos and Silva (2017), Zhou et al. (2018), Sapozhnikova et al. (2017).
RF	Savage et al. (2017), Zhang and Trubey (2018), Zhou et al. (2018), Sapozhnikova et al. (2017), Badal-Valero et al. (2018).
DT	Zhang and Trubey (2018), Villalobos and Silva (2017), Badal- Valero et al. (2018), Mubalaike and Adali (2018), Jayasree and Siva Balan (2017), Liu et al. (2011) .
Neural Network	Zhang and Trubey (2018), Villalobos and Silva (2017), Badal-Valero et al. (2018).
BLR	Zhang and Trubey (2018).
Apriori Algorithm	Suresh et al. (2016), Rafał Dre_zewski et al. (2015b).
C&RT	Villalobos and Silva (2017).
CHAID	Villalobos and Silva (2017).
LR	Zhou et al. (2018), Zhang and Trubey (2018), Badal-Valero et al. (2018).
Multilayer Perceptron	Sapozhnikova et al. (2017).
K-means	Le Khac and Kechadi (2010), Liu et al. (2011),

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

	Alexandre and Balsa (2016).
Benford's Law	Badal-Valero et al. (2018), Yang and Wei (2010).
PrefixSpan, FP-growth, Eclat	Rafał Dre_zewski et al. (2015b).
AutoEncoder	Mubalaike and Adali (2018), Paula et al. (2016).
RBM	Mubalaike and Adali (2018).
Robust Regression	Lawrencia and Ce (2019).
Temporal-directed Louvain Algorithm	Li et al. (2017).
SNA	Colladon and Remondi (2017), Rafał Dre_zewski et al. (2015a).
Balanced iterative reducing and clustering using hierarchies (BIRCH)	Liu et al. (2011).
Gradient Boosting	Jullum et al. (2020).

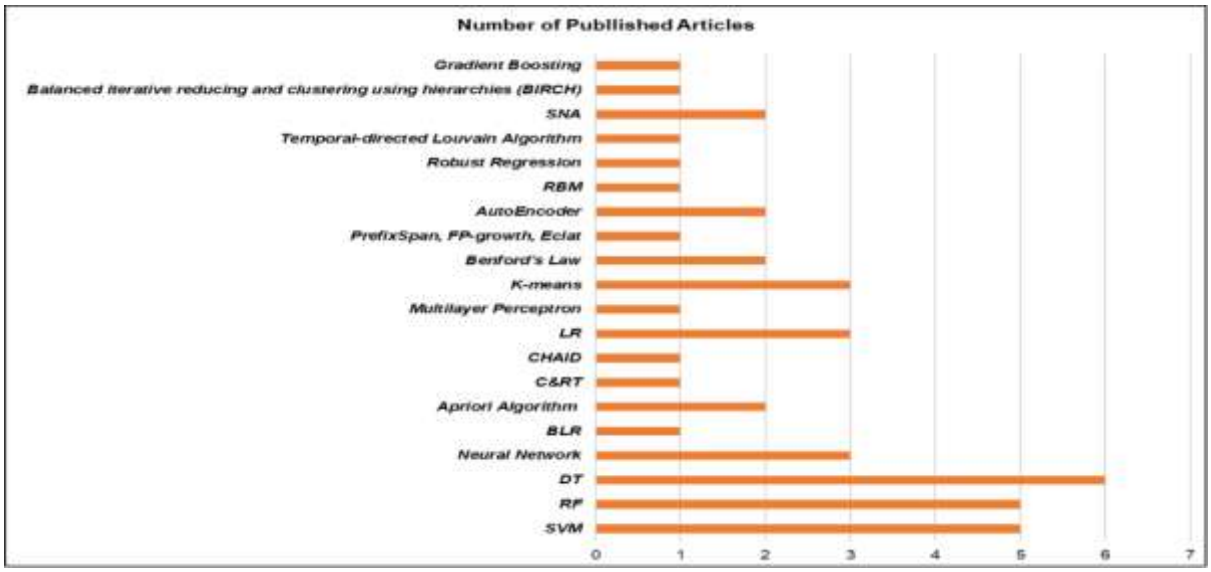

Figure 2: The Number of Articles Published of Algorithm Detection

Data Collection

This section discusses the author's collaborative machine learning (ML) approach for analyzing investment transactions in money laundering. This solution is used in the author framework's data mining and knowledge elements. As previously stated, transactions and accounting are inextricably linked. This system network must be activated to understand customer behavior comprehensively. Accounting transactions were analyzed to detect suspicious money laundering transactions using a collaborative relationship data filtering model in conjunction with decision classifiers stored in the transaction database.

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

For example, Zhou et al. (2018) examined Tencent QQ data, one of China's most extensive online social networks. Tencent QQ, including voice chat, online gaming, and online shopping, offers numerous services. There were 496,414 accounts in the data set (114,891 malicious and 381,523 benign) and a cluster of 54 characteristics that assisted in distinguishing benign from fraudulent accounts.

In contrast, Badal-Valero et al. (2018) examined an extensive database comprising 285,774 operations involving a business with a high likelihood of participating in machine learning activities and a group of over 643 suppliers. In stark contrast to the police expert's detection of just 23 forgeries, the research identified 335 companies with an unusually high number of activities. The data set's weakness was that only a small percentage of businesses were recognized as fraudulent compared to the total number of suppliers.

Implementations Instruments

Numerous tools are used to implement AML systems, as illustrated in Table 4 and Figure 3. Savage et al. (2017) and Zhang and Trubey (2018) conducted their analyses using the R statistical language, whereas Zhang and Trubey (2018) utilised SAS Proc Reg. Soltani et al. (2016) also built the suggested framework in their study by means of JAVA. Le-Khac et al. (2016) created a Web-based solution using C# and SQL Server 2005. MATLAB was used to conduct experiments in Sapozhnikova et al. (2017)'s study. Singh and Best's (2019) study used SQL queries to process data and the GraphViz tool to visualize it. Lawrencia and Cecilia conducted their investigation using SQL aggregates and Python (2019). Paula et al. (2016) used 0xdata's H2O software to analyze data, including a library of machine learning techniques.

According to Li et al. (2017), the suggested approach was built on the Spark GraphX platform, with all data stored in a Cloudera HDFS cluster. The Java programming language was used to develop BIDT (Jayasree and Siva Balan, 2017). Le Khac and Kechadi (2010) used the.NET platform to create a data warehouse with a tree design for customers and transactions. Jullum et al. also made use of the XGBoost library (2020). Finally, Alexandre and Balsa (2016) utilized the Waikato Environment for Knowledge Analysis to examine data. Figure 4 depicts a basic graph of commonly used tools.

Table 4: Instruments of AML System.

Instruments	Articles Research
R	Savage et al. (2017) and Zhang and Trubey (2018).
JAVA	Soltani et al.'s (2016) and (Jayasree and Siva Balan, 2017).
C#	Le-Khac et al. (2016).
Matlab	Sapozhnikova et al.'s (2017).
GraphViz	Singh and Best's (2019).
.NET	Le Khac and Kechadi's (2010).
H2O Software	Paula et al. (2016).
Python	Lawrencia and Ce (2019).
Spark	Li et al. (2017).
WEKA	Alexandre and Balsa (2016).

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

SQL	Le-Khac et al. (2016), Singh and Best's (2019), and Lawrencia and Ce (2019).
XGBoost Library	Jullum et al.'s (2020).

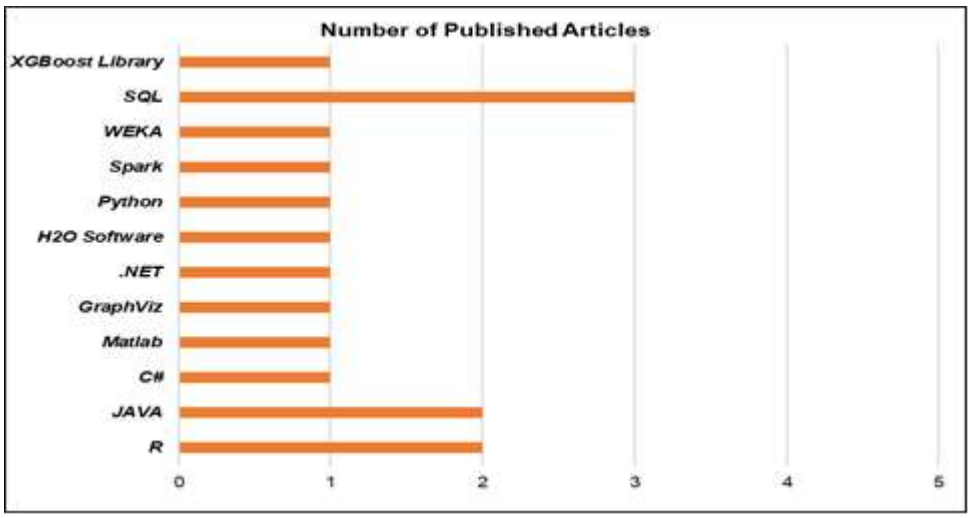

Figure 3: The Number of Articles Published of Implementations Instruments of AML System

Techniques of Sampling

The sampling technique used to determine the number of observations from raw data was covered in a number of articles. To ensure that the created sample had an adequate number of events, Zhang and Trubey (2018) used stratified bootstrap sampling, random bootstrap sampling, and random bootstrap sampling with replacement. The researchers attempted unstratified bootstrap sampling first but were unable to produce an analytically valid sample. The sample utilised by Badal-Valero et al. (2018) was split into two groups, and two different approaches were applied: the first involved cross-validation and tenfold division of the learning data, while the second employed a 70/30 split of the data for training and testing, respectively. In addition, Savage et al. (2017) employed a random sampling technique.

Jullum et al. (2020) fragmented the data into two sets: a training set for training the predictive model and a testing set for validating and evaluating the trained model's accuracy. The training set had 28,167 records, whereas the testing set included 4,967 records.

Study Area

This section outlines the geographical distribution of the sample in terms of the data used, the locations from which data were gathered, and the regions where AML systems were used. Table 5 shows that China is the leading country with four research programmes, followed by Poland with two and the other coloured nations with one.

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

Table 5: Money Laundering Systems Distribution

Country	Article Research
China	Zhou et al. (2018), Li et al. (2017), Liu et al. (2011), and Yang and Wei (2010).
Indonesia	Lawrencia and Ce (2019).
Australia	Savage et al. (2017).
Poland	Rafał Dre_zewski et al. (2015a) and Rafał Dre_zewski et al. (2015b).
Italy	Colladon and Remondi (2017).
Norway	Jullum et al.'s (2020).
Spain	Badal-Valero et al. (2018).
UK	Demetis (2018).
Brazil	Paula et al. (2016).

Conclusions

AML systems are categorized as either supervised or unsupervised machine learning systems or a hybrid of the two. While the most often used classification algorithms in supervised learning are DT, RF, and SVM, neural networks are among the most widely used applications in unsupervised learning. Precision, accuracy, and area under the curve are all standard measures for model assessment. Geographically, China had the most publications, with four articles mainly focused on money laundering crimes. This review research was carried out utilizing various commercial and open-source technologies, the most often used being SQL, followed by the R statistical language and JAVA.

The AML system's algorithm, the type of data used, the sample plan, and the region that was being studied were all factors that the researchers looked at when reviewing the studies that were included in this article. Although the present emphasis is on customer and financial transactions, it is prudent to include additional forms of data from various parties because money laundering is a synthesis of several crimes. The researchers found that the majority of the data came from banks. Experience from throughout the world shows that ML criminals use administrative authority gaps as a means of committing the crime. Money laundering crimes must be taken into account by concentrating on other industries that are frequently used for money laundering, such as restaurants, hotels, and law offices, and by tying together a number of indicators, such as the establishment's size, number of workers, both export and import values, and funds transfer.

As a result, future research may focus on developing an AML system that integrates data from multiple sources, as machine learning can solve various crimes. Additionally, global experience demonstrates that perpetrators of machine learning crimes exploit administrative flaws to conceal their actions and illicitly acquire money. This could have disastrous social ramifications and jeopardize the security of any country, large or small. It enables drug dealers, terrorists, illegal arms dealers, corrupt public officials, and other criminals to operate and expand.

International Journal of Entrepreneurship and Management Practices
IJEMP
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

Transition countries face inherent limitations and practical difficulties in implementing anti-money laundering measures, including the phenomenon of "adopt but not enforce" and "selective implementation" in relation to combating money laundering in transition countries, the political confrontation between transition countries and developed countries, and defensive reporting issues in transition countries. It is worthwhile analyzing the AML operating environment in transition countries and, as a result, to identify solutions to these constraints and difficulties. More importantly, against this backdrop, in-depth research into the AML implementation practices of transition countries is critical for future enhancements to the global AML working mechanism's effectiveness.

Acknowledgements: The authors would like to express their sincere gratitude to Kedah State Research Committee, UiTM Kedah Branch, for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.

Funding Statement: No Funding

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Entrepreneurship and Management Practices (IJEMP).

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Roshima Said was responsible for the conceptualization, methodology, and overall supervision of the study. Salwa Zolkaflil handled data collection, analysis, and interpretation of results. Nur Zharifah Che Adenan contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

International Journal of Entrepreneurship and Management Practices
EISSN : 2600-8750
Volume 9 Issue 33 (March 2026) PP. 633-651

References

About - Financial Action Task Force (FATF) (2020) "[WWW document]", available www.fatf-gafi. org/about/ (accessed 28 November 2018).

Alexandre, C. and Balsa, J. (2015), A Multiagent Based Approach to Money Laundering Detection and Prevention, ICAART (1). pp. 230-235.

Alexandre, C. and Balsa, J. (2016), Integrating Client Profiling in an anti-Money Laundering Multiagent Based System, in New Advances in Information Systems and Technologies, Springer, pp. 931-941.

Aluko, A., & Bagheri, M. (2012). The impact of money laundering on economic and financial stability and on political development in developing countries: The case of Nigeria. Journal of Money Laundering Control.

Badal-Valero, E., Alvarez-Jareño, J.A. and Pavía, J.M. (2018), "Combining Benford's law and machine learning to detect money laundering. An actual Spanish court case", Forensic Science International, Vol. 282, pp. 24-34.

Colladon, A.F., and Remondi, E. (2017), "Using social network analysis to prevent money laundering," Expert Systems with Applications, Vol. 67, pp. 49-58.

Demetis, D.S. (2018), "Fighting money laundering with technology: a case study of Bank X in the UK," Decision Support Systems, Vol. 105, pp. 96-107.

Drez_ewski, R., Dziuban, G., Hernik, Ł. and Pączek, M. (2015b), "Comparison of data mining techniques for money laundering detection system," 2015 International Conference on Science in Information Technology (ICSITech), IEEE, pp. 5-10.

Drez_ewski, R., Sepielak, J. and Filipkowski, W. (2015a), "The application of social network analysis algorithms in a system supporting money laundering detection," Information Sciences, Vol. 295, pp. 18-32.

Financial Action Task Force (FATF). (2020). COVID-19-related Money Laundering and Terrorist Financing-Risks and Policy Responses. https://www.unodc.org/documents/Advocacy-Section/UNODC_-_MONEY_LAUNDERING_AND_COVID19_-_Profit_and_Loss_v1.1_-_14-04-2020_-_CMLS-COVID19-GPML1_-_UNCLASSIFIED_-_BRANDED.pdf

Friedman, J., Hastie, T., and Tibshirani, R. (2001), The Elements of Statistical Learning, Springer series in statistics New York, NY.

Jayasree, V. and Siva Balan, R. (2017), "Money laundering regulatory risk evaluation using bitmap index-based decision tree," Journal of the Association of Arab Universities for Basic and Applied Sciences, Vol. 23 No. 1, pp. 96-102.

Jullum, M., Løland, A., Huseby, R.B., AAnonsen, G. and Lorentzen, J. (2020), "Detecting money laundering transactions with machine learning," J. Money Laund. Control.

Kannan, S. and Somasundaram, K. (2017), "Autoregressive-based outlier algorithm to detect money laundering activities," Journal of Money Laundering Control, Vol. 20 No. 2, pp. 190-202.

Lawrencia, C. and Ce, W. (2019), "Fraud detection decision support system for Indonesian financial institution," in 2019 International Conference on Information Management and Technology (ICIMTech). Presented at the 2019 International Conference on Information Management and Technology (ICIMTech), IEEE, Jakarta/Bali, Indonesia, pp. 389-394.

Le Khac, N.A. and Kechadi, M.-T. (2010), "Application of data mining for anti-money laundering detection: a case study," in 2010 IEEE International Conference on Data Mining Workshops. Presented at the 2010 IEEE International Conference on Data Mining Workshops (ICDMW), IEEE, Sydney, TBD, Australia, pp. 577-584.

Le-Khac, N.-A. Markos, S. O'Neill, M. Brabazon, A. and Kechadi, T. (2016), "An efficient search tool for an anti-money laundering application of a multinational bank's dataset," ArXiv Prepr. ArXiv160902031.

Li, X., Cao, X., Qiu, X., Zhao, J. and Zheng, J. (2017), "Intelligent anti-money laundering solution based upon novel community detection in massive transaction networks on spark," in 2017 Fifth International Conference on Advanced Cloud and Big Data (CBD). Presented at the 2017 Fifth International Conference on Advanced Cloud and Big Data (CBD), IEEE, Shanghai, China, pp. 176-181.

Liu, R., Qian, X., Mao, S. and Zhu, S. (2011), "Research on anti-money laundering based on core decision tree algorithm," in 2011 Chinese Control and Decision Conference (CCDC). Presented at the 2011 23rd Chinese Control and Decision Conference (CCDC), IEEE, Mianyang, China, pp. 4322-4325.

Moustafa, T.H., Abd El-Megied, M.Z., Sobh, T.S. and Shafea, K.M. (2015), "Anti money laundering using a two-phase system," Journal of Money Laundering Control, Vol. 18 No. 3, pp. 304-329.

Mubalaike, A.M. and Adali, E. (2018), "Deep learning approach for intelligent financial fraud detection system," in 2018 3rd International Conference on Computer Science and Engineering (UBMK), IEEE, pp. 598-603.

Paula, E.L., Ladeira, M., Carvalho, R.N. and Marzagao, T. (2016), "Deep learning anomaly detection as support fraud investigation in Brazilian exports and anti-money laundering," in 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, pp. 954-960.

Salehi, A., Ghazanfari, M., and Fathian, M. (2017), "Data mining techniques for anti-money laundering," Int. J. Appl. Eng. Res, Vol. 12, pp. 10084-10094.

Sapozhnikova, M., Nikonov, A., Vulfin, A., Gayanova, M., Mironov, K. and Kurennov, D. (2017), "Anti- fraud system on the basis of data mining technologies," in 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), IEEE, pp. 243-248.

Savage, D., Wang, Q., Zhang, X., Chou, P. and Yu, X. (2017), "Detection of money laundering groups: Supervised learning on small networks," in Workshops at the Thirty-First AAAI Conference on Artificial Intelligence.

Singh, K. and Best, P. (2019), "Anti-money laundering: using data visualization to identify suspicious activity," International Journal of Accounting Information Systems, Vol. 34, p. 100418.

Soltani, R., Nguyen, U.T., Yang, Y., Faghani, M., Yagoub, A. and An, A. (2016), "A new algorithm for money laundering detection based on structural similarity," in 2016 IEEE 7th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, pp. 1-7.

Suresh, C., Reddy, K.T. and Sweta, N. (2016), "A hybrid approach for detecting suspicious accounts in money laundering using data mining techniques," International Journal of Information Technology and Computer Science, Vol. 8 No. 5, p. 37.

Syed Mustapha Nazri, S.N.F., Zolkaflil, S. and Omar, N. (2019), "Mitigating financial leakages through effective money-laundering investigation," Managerial Auditing Journal, Vol. 34 No. 2, pp. 189-207.

Villalobos, M.A. and Silva, E. (2017), "A statistical and machine learning model to detect money laundering: an application."

Yang, S. and Wei, L. (2010), "Detecting money laundering using filtering techniques: a multiple-criteria index," Journal of Economic Policy Reform, Vol. 13 No. 2, pp. 159-178.

Zhang, Y. and Trubey, P. (2018), "Machine learning and sampling scheme: an empirical study of money laundering detection," Comput. Econ, pp. 1-21.

Zhou, Y., Wang, X., Zhang, J., Zhang, P., Liu, L., Jin, H. and Jin, H. (2018), "Analyzing and detecting money-laundering accounts in online social networks," IEEE Netw, Vol. 32 No. 3, pp. 115-121