




Machine Learning Models for Money Laundering Detection in Financial Institutions. A Systematic Literature Review

Juan J. Soria¹, Rodrigo Loayza Abal², Lidia Segura Peña³

^{1,2,3}Universidad Tecnológica del Perú SAC, Perú, c20723@utp.edu.pe, u18101212@utp.edu.pe, c19365@utp.edu.pe

Abstract– Financial crimes in institutions have grown exponentially over the years, detecting credit card fraud in which simple and hybrid machine learning have been used for detection. In the world of financial transactions, the development of predictive models in the detection of financial fraud has become a fundamental element for the success of a secure transaction in banking organizations; in this sense, the study aimed to systematize research with machine learning models in the detection of money laundering in financial organizations, the methodological design used was theoretical systematic review, the search explored two databases following the PRISMA statement (Scopus, Web of Science), 189 articles were found, of which, after the eligibility criteria, 25 were systematized. The results refer that work was done with Support Support Machine Models (SVM), Nearest Neighbors (KNN), Artificial Neural Networks (ANN), decision trees, Random Forests and Naive Bayes, which shows that the best accuracy in obtaining the laundering of assets was obtained by the SVM with an accuracy of 93.45%, in second place the Neural network with 92.14%; in the same way it was observed that Gezer, Ali et al. had the highest citation with 29, followed by Eachempati, Prajwal with 22 citations. It has been further revealed that money laundering affected many organizations engaged in being transactions in virtual form, in which artificial intelligence contributes in its support to detect this computer crime. These findings provide valuable information to improve the detection of financial fraud, highlighting the importance of addressing specific aspects that with the help of artificial intelligence can promote a better machine learning model that allows detecting suspicious transactions.

Keywords- Support Machine, Nearest Neighbors, Neural Networks, Active Washing, Decision Trees.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

I. INTRODUCTION

Internet Banking introduced by Citibank and Well Fargo Bank, adopted the use of credit cards through internet, which the volume of transactions increased exponentially in e-commerce and hence the fraud of financial transactions became more dangerous; for which it is necessary to know how artificial intelligence with the help of machine learning algorithms allows detecting the type of suspicious financial transaction, preventing banking crime [1] Supervised machine learning algorithms such as Naive Bayes, Support Vector Machine. Decision trees, logistic regression, neural networks are the most relevant in the detection of money laundering.

The increase in the global economy is due to the close relationship between investment, trade and productivity of a country, which makes a high volume of money involved in e-commerce transactions, by which fraudsters take advantage by committing computer crime, thus the importance of artificial intelligence in fraud prevention and detection becomes very relevant in current times, in which 64 fraud items were found of which card fraud was the most relevant [2].

The volume of financial transactions involves money laundering, which is why it is important to detect and automate the critical processes of detecting, flagging, and reporting suspicious customers. A multi-agent system incorporating machine learning was realized to identify and flag the suspicious banking customer, enabling bank managers to analyze the suspicious behavior of their financial customers[3].

To detect and predict fraud in credit card transactions, supervised machine learning algorithms such as logistic regression, decision trees, random forests were used. The categories of bankruptcy fraud, counterfeit fraud, solicitation fraud and behavioral fraud, fraudulent transactions were identified with logistic regression, Naive Bayes, Random Forest, K Nearest Neighbour, Gradient Boosting, Support Vector Machines, and neural network algorithms, in which Gradient Boosting had a better accuracy of 95.9% than the other algorithms[4].

II. METHODOLOGY

A. Methodological Design

The type of research was theoretical systematic review [5] because large volumes of information were synthesized and evaluated to make decisions regarding the topic of study [6], these were sufficiently complex for the generalization of the results.

B. Search Strategies

For the development of the study, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement [7], was considered; two main databases were selected, Scopus, Web of Science. Then the search process was

carried out, these together with the Boolean operators AND, OR were entered into the Title-Abst-Key search criteria. The search equations for Scopus (TITLE-ABS-KEY ("asset" OR "money" OR "laundering" OR "fraudulent commissions" OR "economic crimes") AND TITLE-ABS-KEY ("machine learning " OR "algorithms" OR "KNN" OR "SVM" OR "naive bayes" OR "Logistic regression" OR "Neural networks" OR "lasso" OR "Ridge") AND TITLE-ABS-KEY ("models" OR "Supervised" OR " unsupervised" OR "money") AND TITLE-ABS-KEY ("Accuracy" OR "F1 Score" OR "recall") AND TITLE-ABS-KEY ("banks" OR "financial" OR "credit" OR "institutions")) AND PUBYEAR > 2014 AND PUBYEAR < 2025 AND (LIMIT-TO (EXACTKEYWORD , "Machine Learning") OR LIMIT-TO (EXACTKEYWORD , "Learning Systems") OR LIMIT-TO (EXACTKEYWORD , "Financial Markets", for Web of Science (((ALL=("asset" OR "money" OR "laundering" OR "fraudulent commissions" OR "economic crimes")) AND ALL=("machine learning " OR "algorithms" OR "KNN" OR "SVM" OR " naive bayes" OR "Logistic regression" OR "Neural networks" OR "lasso" OR "Ridge")) AND ALL=("models" OR "Supervised" OR " unsupervised" OR "money")) AND ALL=("Accuracy " OR "F1 Score" OR "recall")) AND ALL=("banks" OR "financial" OR "credit" OR "institutions"). For the selection of the articles, inclusion criteria were applied, where only empirical articles were selected, between 2015-2023; Regarding the exclusion criteria, those gray literature studies and those documents that could not be accessed as full text at the end of the review were not taken into account. Furthermore, to guarantee the eligibility of the documents, the quality criteria established by the PRISMA declaration were considered.

C. Data Collection Techniques

For the collection of information, documentary analysis was considered[8], through the design of an information matrix, using a Microsoft Excel ® format that included information on the author, year of publication, country, ML models used, impact factor, number of citations and results; once the articles were systematized, they were reviewed by three independent researchers in order to identify whether they corresponded to the topic in question, which avoided bias.

D. Information processing

Descriptive statistics were applied by measuring averages and frequencies reached on the impact of the Machine Learning models found in the articles, this allowed the results to be generalizable, contributing to the formulation of research perspectives and to know the main results within the scientific literature. To characterize the articles, a double-entry table was used to record the main data of author and year, country of origin, the machine learning model used, the instruments; through this table, the origin of the studies and how they were composed were identified. Next, the results were detailed and related to each of the elements found to analyze how they

correspond to the money laundering detection models; finally, the percentage values of the accuracy and F1 Score of the models found in the articles reviewed were measured.

III. RESULTS

According to Figure 1, 189 articles were identified in the two databases, which after the first elimination for concepts of studies between 2015 and 2023 only 90 were screened, after the review of the titles only 35 documents were registered. After the review of the abstracts, 52 documents were recovered for their eligibility, where they were excluded due to the absence of access to full text, not having measured the money laundering models, not defining the precision, the objective differing from the requirements of the study as well as having been letter to the editor, only 21 documents were included, in addition to these, four articles were added after the web search and citation process; in total 25 articles were systematized that met the selection criteria established by the authors.

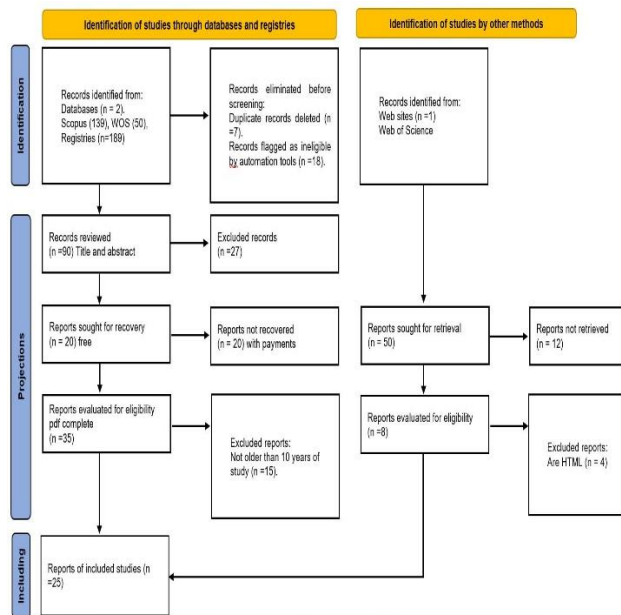


Fig 1. PRISMA Selection Diagram

The results of the articles screened are shown in Table I, showing the title of the article with its respective reference, the country and the machine learning models used in money laundering.

TABLE I
RESULTS OF REVIEW ARTICLES

Title	Reference	Country	Models ML
Una A time and frequency-based detection of suspicious activity to combat money laundering [9].	Ketenci, Utku Gorkem et al (2021)	Turquía	Transaction Feature; Time Frequency and CRM Features
Intelligent anti-money laundering fraud control using a graph-	Naveed, Nasir et al (2022)	Pakistan	Decision Tree (DT), Conditional Inference Tree (CT), Random

based machine learning model for the financial domain [10]			Forest (RF); Neural Network (NN)
CCNN: CCNN: an artificial intelligence-based classifier for a credit card fraud detection system with an optimized cognitive learning model. [11]	Vetrivendan L. et al Mayo (2023)	Noida, India	proposed cognitive convolutional neural network (CCNN) classifier. Existing classifiers such as logistic regression (LR), K-nearest neighbor (KNN), decision tree (DT) and support vector machine (SVM) were used to classify the proposed classifier. (SVM)
Dominant feature selection and machine learning-based hybrid approach to analyze Android ransomware. [12]	Gera, Tania et al. (2021)	Punjab, India	J48, Random Forest, LMT, Random Tree
Machine learning with belief rule-based expert systems to predict stock price movements. [13]	Emam Hossain et al. (2022)	Baltimore, EE.UU	Belief-Based Rule-Based Expert System (BRBES)
Application of the deep learning method in the TVP-VAR model under systematic financial risk monitoring and early warning. [14]	Huang, Anzhong et al. (2023)	China	Deep learning ; Early warning ; Information systems ; Supervision ; Information systems ; Systemic financial risk
Development of a predictive customer investment model using the conjoint learning technique. [15]	Kaewkiriya, Thongchai et al. (2022)	Thailand	Clustering, K-Nearest Neighbour Algorithm, Naïve Bayes Algorithm, Decision Tree Algorithm, Neural Network Algorithm,
Validating the impact of accounting disclosure on the stock market: a deep neural network approach. [16]	Eachempati, Prajwal (2023)	India	Deep neural networks with LSTM, Naive Bayes, Maximum Entropy, SVM, RNNR
Deep Learning criminal networks. [17]	Ribeiro, Haroldo V et al. (2023)	Brasil	Convolutional networks; GraphSAGE
DeLCluste: Protecting users against credit card transaction fraud through deep learning cluster ensemble. [18]	Aghware, Fidelis Obukohwo et al. (2023)	Agbor, Nigeria	DNN, PHMM, MNN, GANN ,DeLCluste.
Detection of manipulators in cryptocurrency markets based on forecast anomalies. [19]	Akba, Firat et al. (2023)	Turquía	SARIMAX, ARIMA, LSTM, SVM
Research on the application of machine learning for watch list filtering in the fight against money laundering. [20]	Qutqut, H et al. (2023)	Jordania	SVM, DT Y NB (Decision Tree) Naïve Bayes, Support Vector Machine
Unbalanced classification of fraudulent bank transactions using machine learning. [21]	Ruchay, Alexey et al. (2020)	Federation de Rusia	algorithms TPOT y Random Forest
Transactional network analysis and identification of China's central bank digital currency	Li, Ziyu et al. (2020)	China	GCN, EvolveGCN, GAT GraphSAGE, ChebNet-GRU

money laundering behavior. [22]			
Multilayer perceptron artificial neural network-based model for credit card fraud detection. [23]	Kasasbeh, Bassam (2020)	Jordania	Best Network Model
Money laundering detection using machine learning and deep learning. [24]	Alotibi, Johrha (2019)	Arabia Saudita	NB, RF, KNN, DNN
Exploiting machine learning algorithms to detect financial crime based on customer behavior. [25]	Kumar, Sanjay et al. (2022)	Suiza	decision tree (DT), random forest (RF) and k-nearest neighbor (KNN).
Predictive financial fraud detection analytics using Azure and Spark ML.[26]	Purushu, Priyanka et al. (2018)	Estados Unidos	LR, DF, DJ, SVM
A flow-based approach for Trickbot banking Trojan detection. [27]	Gezer, Ali et al. (2019)	Turquía	random forest, multilayer perceptron's, minimal sequential optimization and Logistic Models
Money laundering risk assessment of bank accounts using naive bayes classification. [28]	Islam, MA et al (2020)	Bangladesh	Level Search Method (RLFM) in the context of Money and Laundering Residence in Naive Bayes.
Research on the application of machine learning for watch list filtering in anti-money laundering. [29]	Asha RB, et al (2021)	India	Support Vector Machine (SVM), k-nearest neighbor (KNN) and artificial neural network (ANN)
Machine learning approaches for the construction of the national anti-money laundering index.[30]	Zhang, GK, et al (2023)	China	LASSO regression and random forests
Credit card fraud detection using a new hybrid machine learning architecture. [31]	Malik, EF, et al (2022)	Malasia	hybrid machine Learning models.
Detection of money laundering and terrorist financing using neural networks and an anomaly indicator. [32]	Rocha-Salazar, JDJ et al (2021)	España	integrated model
Money laundering governance and income transfer: evidence from Australian financial institutions..[33]	Baban Eulaiwi et al (2024)	Australia	Asset Laundering Control with AI

Table II shows the results of the articles with their keywords, showing the reference, country and keywords of the 25 articles screened.

TABLE II
RESULTS OF ARTICLES SCREENED BY WORDS

Reference	Country	Key words
Ketenci, Utku Gorkem et al (2021)	Turquía	Anomaly detection; anti-money laundering. compliance; random forest algorithm. time-frequency analysis; transaction monitoring

Naveed, Nasir et al (2022)	Pakistan	Anti-money laundering; Machine learning; Networks; Semi-supervised learning; Tensor flow; Proceedings
Vetrivendan L. et al Mayo (2023)	Noida, India	CCFD, machine learning, cross validation, support vector machine, classification, sub-sampling
Gera, Tania et al. (2021)	Punjab, India	Android (operating system); Crime; Feature extraction; Learning algorithms; Loss; Machine learning; Machine learning; Mobile security; Network security. Data files; Feature selection algorithm; Feature selection; Feature selection; Feature sets; Financial benefits; Financial loss; Hybrid approach; Machine learning; Performance; Smartphones..
Emam Hossain et al. (2022)	Baltimore, EE.UU	Stock prediction bolling band bollinger belief rule Expert Systems Machine Learning Time Series Analysis
Huang, Anzhong et al. (2023)	China	Deep learning; Early warning; Information systems; Supervision; Information systems; Systemic financial risk.
Kaewkiriya, Thongchai et al. (2022)	Thailand	Data preparation; Conjoint learning; Inversion; Machine learning
Eachempati, Prajwal (2023)	India	Analytics; Data intelligence; Deep learning; Disclosures; Financials; Forecasting; Machine learning; Private decision making; Stock market.
Ribeiro, Haroldo V et al. (2023)	Brasil	Complexity; Crime prediction; Convolutional network networks graphs; GraphSAGE; Organized crime.
Aghware, Fidelis Obukohwo et al. (2023)	Agbor, Nigeria	Cluster modeling; Credit card fraud; Deep learning ensemble; Financial inclusion; Fraud detection; Fraudulent transactions
Akba, Firat et al. (2023)	Turquía	Anomaly detection; Covid-19 pandemic; Cryptocurrency markets; Deep learning; Machine learning; Manipulator detection; Sentiment analysis; Time series analysis; Deep learning; Machine learning; Manipulator detection; Sentiment analysis; Time series analysis
Qutut, Mahmoud H et al. (2023)	Jordania	Anti-money laundering; monitoring of financial transactions; machine learning (ML); sanction control; watch list filtering
Ruchay, Alexey et al. (2020)	Federación de Rusia	banking transactions; fraudulent transaction detection; unbalanced classification; machine learning
Li, Ziyu et al. (2020)	China	behavioral identification; central bank digital currency (CBDC); money laundering; transaction network
Kasasbeh, Bassam (2020)	Jordania	Artificial neural networks; Credit card fraud; Machine learning; Multilayer perceptron on-line transaction
Alotibi, Johrha (2019)	Arabia Saudita	Anti-money laundering; Cryptocurrency; Machine learning; Supervised learning; Anti-money laundering; Cryptocurrency; Machine learning; Supervised learning
Kumar, Sanjay et al. (2022)	Suiza	credit card fraud; financial crime; fraud prediction; machine learning; nonperforming assets; outlier detection; fraud prediction; machine learning; nonperforming assets; fraud detection.

Purushu, Priyanka et al. (2018)	Estados Unidos	azure ; Big data ; Fraud detection ; Hadoop ; Machine learning ; Spark -sparking
Gezer, Ali et al. (2019)	Turquía	Traffic anomaly detection; Banking Trojan ; Dynamic analysis ; Machine learning ; Random forest ; Trucobot.
Islam, MA et al (2020)	Bangladesh	Anti-money laundering Classification Financial intelligence unit Money laundering Risk Level search method
Asha RB, et al (2021)	India	Artificial neural network Credit card Fraudek-nearest-neighbor machine learning machine and support vectors
Zhang, GK, et al (2023)	China	Anti-Money Laundering Index GAFILAZO Recommendations Random Forests Prediction.
Malik, EF, et al (2022)	Malasia	credit card classification credit card data processing hybrid fraud detection machine Learning.
Rocha-Salazar, JDJ et al (2021)	España	Money laundering Terrorist financing Unsupervised learning Detection Machine learning.
Baban Eulaiwi et al (2024)	Australia	AI models for money laundering detection.

Table III shows the effectiveness of the models used for the detection of money laundering, showing the respective machine learning models found with their F1 Score and accuracy.

TABLE III
RESULTS OF ARTICLES SCREENED FOR PERFORMANCE

Models used in money laundering	F1 SCORE	Model accuracy
Transaction Feature; Time Frequency and CRM Features.	59.37%; 72.19%	
Decision tree (DT), conditional inference tree (CT), random forest (RF); neural network (NN)	0.423 (DT) , 0.205 (CT) , 0.524 (RF), 0.414 (NN) . Acuracy 0.637 (DT) , 0.557 (CT) , 0.678 (RF), 0.693 (NN)	0.637 (DT), 0.557(CT), 0.678 (RF) , 0.693 (NN)
Proposed cognitive convolutional neural network (CCNN) classifier. Existing classifiers such as logistic regression (LR), K-nearest neighbor (KNN), decision tree (DT) and support vector machine (SVM) have been used. (SVM)	94% (LR), 93% (KNN), 93% (SVM), 90% (DR), 95.6% Cognitive CNN	Logistic Regression LR (94%), Knowledge nearest neighbour KNN (93%), Support Vector Machine SVM (93), Decision Tree Classifier DTC (90%) Cognitive CNN (CCNN) 95.6%

J48, Random Forest, LMT, Random Tree		J48 (0.97734), Random Forest (0.9863), LMT (0.9847), Random Tree (0.9837)
Belief-Based Rule-Based Expert System (BRBES)	BRB 93.50 ; RMSE 0.1233, R ² =48.06 AUC=0.984	
Deep learning ; Early warning ; Information systems ; Supervision ; Information systems ; Systemic financial risk		
Clustering, K-Nearest Neighbor Algorithm, Naïve Bayes Algorithm, Decision Tree Algorithm, Neural Network Algorithm,		
Deep Neural Networks with LSTM, Naive Bayes, Maximun Entropy, SVM, RNNR		Naive Bayes (0.64), SVM (0.67), RNAR(0.694), RNA Largo plazo (0.72)
Convolutional networks; GraphSAGE	0.88 ; 0.92 R ² ajustada de 0,64 a 0,90	
DNN, PHMM, MNN, GANN ,DelCluste.		DNN(0.92) PHMM (0.89) MNN(0.91) , GANN (0.78) ,DelCluste (0.96)
SARIMAX, ARIMA, LSTM, SVM	ARIMA (62.5) , SARIMAX (64.5), SVM (60.00) LSTM (60)	ARIMA (63) , SARIMAX (60), SVM (83) LSTM (70)
SVM, DT Y NB (Decision Tree) Naïve Bayes, Support Vector Machine		SVM (0.815), NB (0.804), DT (0.782)
TPOT and Random Forest algorithms	RandomForestClassifier (0.9610), TpotClassifier (0.9620)	RandomForesrClassifier(0.9999), TpotClassifier (0.9999)
GCN, EvolveGCN, GAT, GraphSAGE, ChebNet-GRU	GCN(0.960), EvolveGCN(0.961), GAT (0.962) GraphSAGE(0.968), ChebNet-GRU(0.971)	GCN(0.805), EvolveGCN(0.919), GAT (0.887) GraphSAGE(0.929), ChebNet-GRU(0.943)
Best Network Model	Best Network Model Accuracy (99.9505), RMSE(0.0218), F1(99.949, Specificity (79.710), AUC 0.8983	Fraud Measure F were 84,76%, 85,13% y 82,51% in one hidden layer, two hidden layers and three hidden layers,

NB, RF, KNN, DNN	NB(0.74) RF (0.99) KNN (0.97) DNN (0.98)	NB(0.99) RF (0.99) KNN (0.97) DNN (0.98)
decision tree (DT), random forest (RF) and k-nearest neighbor (KNN).	NB(0.90), DT (0.83) KNN(0.89) RF(0.90) SVM(0.90) LR(0.90)	NB(0.96), DT (0.83) KNN(0.96) RF(0.99) SVM (1) LR(0.99)
LR, DF, DJ, SVM	LR(1.000) DF (0.727) DJ (1.000) SVM (1.000)	LR(0.991) DF (0.995) DJ (0.997) SVM (0.993)
random forest, multilayer perceptron's, minimal sequential optimization and Logistic Models	random forest 0.939 multilayer perceptron's 0.667 minimum sequential optimization 0.997 Logistic Models . 0.998	random forest.0.999 multilayer perceptron's 0.997 minimum sequential optimization 0.995 Logistic Models . 0.996
Level Search Method (RLFM) in the context of Money and Laundering Residence in Naive Bayes	RLFM 0.94 Ingenuo Bayes 0.86	Naïve bayes 0.874
Model (SVM), k-nearest neighbor (Knn) artificial neural network (ANN)	SVM 94% KNN 92% ANN 90%	SVM 0.93 KNN 0.90 ANN 0.91
LASSO regression and random forests	Lasso 0.87 Random Forest 0.92	Lasso 0.976 Random Forest 0.987
hybrid machine learning models	Híbrido 0.86	H 0.987
integrated model	MI 0.87	MI 0.867
Deep Learning Artificial Intelligence Models	RNN 98.5%	Neural networks

Likewise in Figure 2, the frequency of the number of references by authors of the screened articles of the study in the years 2015 to the years 2024 is shown, showing Eachempati et al with 138 references, followed by Kumar, Snajay et al with 87 and in third place Aghware Fidelis with 79 references.

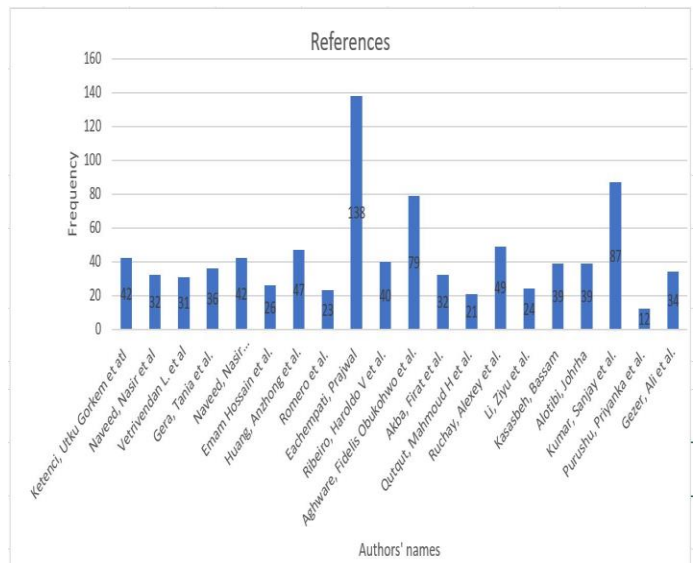


Fig.2. Number of references of articles screened.

In Figure 3 we observe the number of citations for each reference made in the study, where it is highlighted that Gezer Ali et al, obtained 29 citations, followed by Eachempati, Prajwal et al with 22, as well as Huang Anzhong et al with 20 citations and Gera Tania with 19.

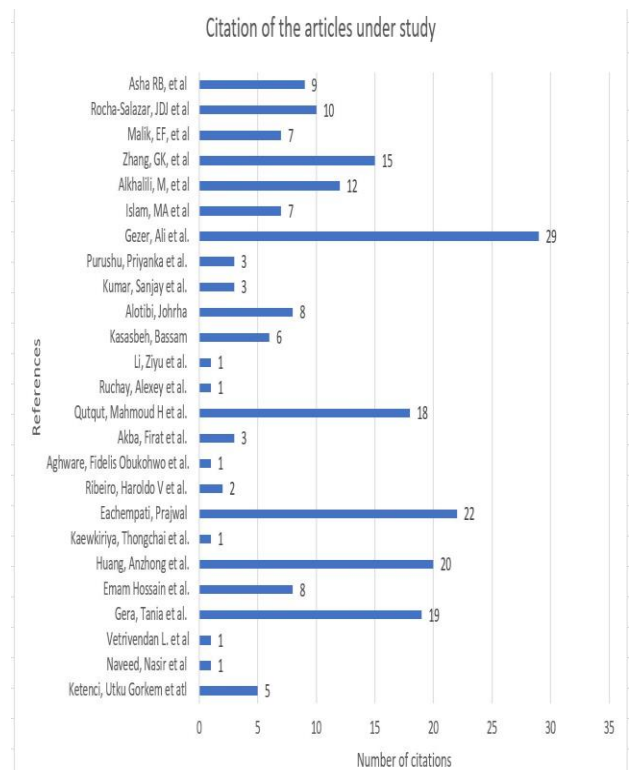


Fig.3. Number of citations of the articles screened.

Bibliometric analysis is the quantitative evaluation of scientific publications using statistical techniques, which provides an understanding of the past and present literature by mapping historical progress and current trends within a time frame [34].

A bibliometric analysis was applied in R studio software [35] to understand the past literature by graphically illustrating the results of the 25 articles screened, which are shown in the following images.

Figure 4 shows seven clusters of countries that have researched money laundering with machine learning, where China (Blue) is the country with the most research, followed by the United States (Purple), Brazil (Brown), Italy (Red), France (Yellow) and Saudi Arabia (Green).

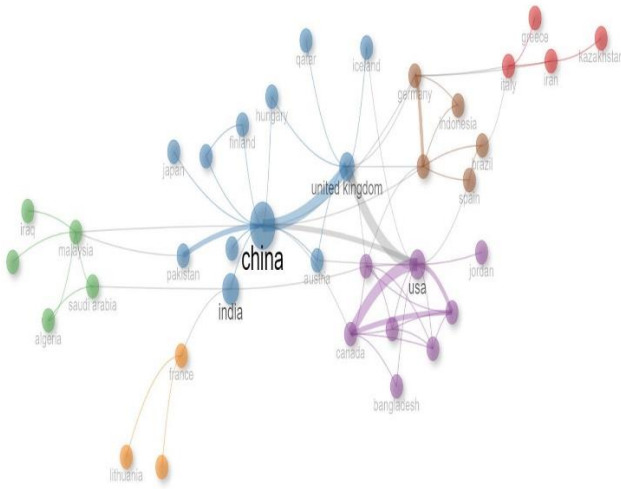


Fig.4. Network diagram of country co-occurrence.

Figure 5 shows the Machine learning models used in the articles screened in the left margin and in the central part the countries where these articles have been investigated and in the right margin the authors corresponding to these investigations are located.

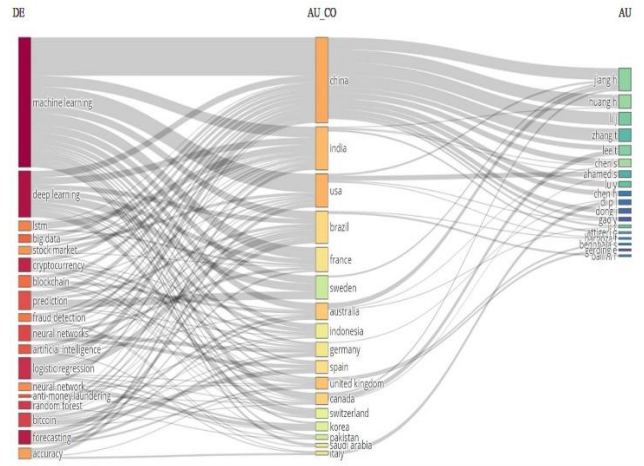


Fig.5. List of models, countries and authors screened

Figure 6 shows the N-gram of the most frequent words used in the research, highlighting machine learning, prediction, financial market, learning systems, e-commerce and investment, e-commerce and Investment.



Fig.6. N-gram of screened items

Figure 7 shows the geolocation map of the locations of the countries that have investigated the same pattern that are machine learning models for the money laundering.

Country Collaboration Map

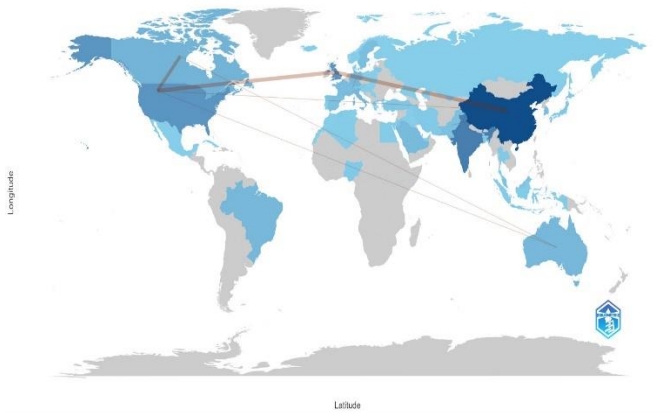


Fig.7. Geolocation map of the screened items

IV. DISCUSSION AND CONCLUSIONS

The systematic review (SR) of machine learning models reveals a number of significant findings, which contribute to understanding the situation and the level of development of organizations that frequently perform financial transactions, all, problem solving and the development of science in combination with practice and theory [36].

The inclusion of 25 studies in this SR reflects a wide variety of approaches and contexts in which they have been addressed, most studies belong to countries of the world, which is related to the data presented by [14] who found a greater number of research on predictive models corresponding to the countries mentioned above, this in relation to the regulatory framework of financial banking, because not only the manager must be knowledgeable about financial transactions, but must have the domain on the management of AI tools that allow detecting money laundering [19], have the ability to solve problems of money laundering, research and generate new productive knowledge to meet the challenges [20]. [19], have the ability to solve money laundering problems, research and generate new productive knowledge to meet the challenges [20].

The research [37], made a mapping of model risk in financial banking management analyzed with machine learning, finding the evolution of statistical techniques in the detection of money laundering determining three clusters in model risk in regulation, model risk and credit risk, model risk and new technologies.

The study [38] shows a bibliometric analysis of cryptocurrencies in the global financial system generating significant carbon emissions and energy consumption, finding that China is the leading contributor, with 348 with a frequency of 348 and a total number of citations of 1259, followed by the US, with 594 citations.

The research [39] posed the ABC- Recurrent Neural Network (RNN) unsupervised learning algorithm because fraud behavior changes continuously, posing a deep convolutional network model that identified anomalies of conventional fraud-focused competitive swarm optimization patterns that cannot be used with historical data or supervised learning, which classified fraud behavior and performed a comparison with current algorithms with an MSE of 97%, an MAE of 92% and an F1 score of 97%.

The research [40] designed an intelligent credit card fraud detection and classification system using the Garra Rufa Fish optimization algorithm with a joint learning model (CCFDG-GRFOEL), which determined the presence of fraudulent and non-fraudulent credit card transactions by selecting subsets of features based on GRFO-FSS, a joint learning process comprising an external learning machine (ELM), a bidirectional long-term memory (BiLSTM) and an automatic encoder (AE). The research [41] built a deep neural network model with multiple hidden layers with a quantitative detection algorithm in which the accuracy of financial fraud detection was improved, where encoders were used to extract behavioral features and reduce computational complexity, secondly the features were transformed into visual representations of behavior and finally sparse reconstruction errors were used to judge and detect financial fraud.

The research [42] developed a firefly swarm evolutionary dynamics (DEGSO) algorithm employing an adaptive step-size strategy and a directional mutation mechanism that improved search performance, which in combination with LSTM identified the accuracy of financial fraud risk.

In conclusion, 189 papers were identified in 2 databases, then, through various stages of review (titles, abstracts, full text access), the sample was further reduced to 90 eligible papers, which were then systematized only 25 of these. Eighty percent of the researchers evaluated the machine learning models using AI tools, which showed adequate levels of reliability, using measures such as accuracy and F1 Score.

The Support Vector Machine (SVM) model obtained the best accuracy, followed by k-nearest neighbors (KNN).

REFERENCES

- [1] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications*, vol. 193. Elsevier Ltd, May 01, 2022. doi: 10.1016/j.eswa.2021.116429.
- [2] V. F. Rodrigues *et al.*, "Fraud detection and prevention in e-commerce: A systematic literature

- review,” *Electron Commer Res Appl*, vol. 56, Nov. 2022, doi: 10.1016/j.elerap.2022.101207.
- [3] C. R. Alexandre and J. Balsa, “Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system,” *Expert Syst Appl*, vol. 217, May 2023, doi: 10.1016/j.eswa.2023.119500.
- [4] J. K. Afriyie *et al.*, “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” *Decision Analytics Journal*, vol. 6, no. November 2022, p. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.
- [5] P. Ranganathan and R. Aggarwal, “Study designs: Part 7 - Systematic reviews,” *Perspect Clin Res*, vol. 11, no. 2, pp. 97–100, Apr. 2020, doi: 10.4103/PICR.PICR_84_20.
- [6] O. Zawacki-Richter, M. Kerres, S. Bedenlier, M. Bond, and K. Buntins Eds, “Systematic Reviews in Educational Research.”
- [7] M. J. Page *et al.*, “The PRISMA 2020 statement: An updated guideline for reporting systematic reviews,” *The BMJ*, vol. 372. BMJ Publishing Group, Mar. 29, 2021. doi: 10.1136/bmj.n71.
- [8] M. Sánchez Bracho, M. Fernández, and J. Díaz, “Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo,” *Revista Científica UISRAEL*, vol. 8, no. 1, pp. 107–121, Jan. 2021, doi: 10.35290/rcui.v8n1.2021.400.
- [9] U. G. Ketenci, T. Kurt, S. Onal, C. Erbil, S. Akturkoglu, and H. S. Ilhan, “A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering,” *IEEE Access*, vol. 9, pp. 59957–59967, 2021, doi: 10.1109/ACCESS.2021.3072114.
- [10] N. Naveed, S. Munawar, and A. Usman, “Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain,” *Journal of Cases on Information Technology*, vol. 25, no. 1, 2023, doi: 10.4018/JCIT.316665.
- [11] L. Vetrivendan and G. Kumar, “CCNN: An Artificial Intelligent based Classifier to Credit Card Fraud Detection System with Optimized Cognitive Learning Model,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, pp. 159–171, May 2023, doi: 10.17762/ijritcc.v11i5s.6640.
- [12] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, “Dominant Feature Selection and Machine Learning-Based Hybrid Approach to Analyze Android Ransomware,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/7035233.
- [13] E. Hossain, M. S. Hossain, P. O. Zander, and K. Andersson, “Machine learning with Belief Rule-Based Expert Systems to predict stock price movements,” *Expert Syst Appl*, vol. 206, Nov. 2022, doi: 10.1016/j.eswa.2022.117706.
- [14] A. Huang, L. Qiu, and Z. Li, “Applying deep learning method in TVP-VAR model under systematic financial risk monitoring and early warning,” *J Comput Appl Math*, vol. 382, Jan. 2021, doi: 10.1016/j.cam.2020.113065.
- [15] T. Kaewkiriya and K. Wisaeng, “Development of Customer Predictive Model for Investment Using Ensemble Learning Technique,” *Journal of Computer Science*, vol. 19, no. 6, pp. 775–785, 2023, doi: 10.3844/jcssp.2023.775.785.
- [16] P. Eachempati, P. R. Srivastava, A. Kumar, K. H. Tan, and S. Gupta, “Validating the impact of accounting disclosures on stock market: A deep neural network approach,” *Technol Forecast Soc Change*, vol. 170, Sep. 2021, doi: 10.1016/j.techfore.2021.120903.
- [17] H. V. Ribeiro *et al.*, “Deep learning criminal networks,” *Chaos Solitons Fractals*, vol. 172, Jul. 2023, doi: 10.1016/j.chaos.2023.113579.
- [18] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, “DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble.” [Online]. Available: www.ijacsa.thesai.org
- [19] F. Akba, I. T. Medeni, M. S. Guzel, and I. Askerzade, “Manipulator detection in cryptocurrency markets based on forecasting anomalies,” *IEEE Access*, vol. 9, pp. 108819–108831, 2021, doi: 10.1109/ACCESS.2021.3101528.
- [20] M. Alkhalili, M. H. Qutqut, and F. Almasalha, “Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering,” *IEEE Access*, vol. 9, pp. 18481–18496, 2021, doi: 10.1109/ACCESS.2021.3052313.
- [21] A. Ruchay, E. Feldman, D. Cherbadzhi, and A. Sokolov, “The Imbalanced Classification of Fraudulent Bank Transactions Using Machine Learning,” *Mathematics*, vol. 11, no. 13, Jul. 2023, doi: 10.3390/math11132862.
- [22] Z. Li, Y. Zhang, Q. Wang, and S. Chen, “Transactional Network Analysis and Money Laundering Behavior Identification of Central Bank Digital Currency of China,” *Journal of Social Computing*, vol. 3, no. 3, pp. 219–230, Sep. 2022, doi: 10.23919/JSC.2022.0011.
- [23] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, “Multilayer perceptron artificial neural networks-based model for credit card fraud detection,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, pp. 362–373, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp362-373.
- [24] J. Alotibi, B. Almutanni, T. Alsubait, H. Alhakami, and A. Baz, “Money Laundering Detection using

- Machine Learning and Deep Learning.” [Online]. Available: www.ijacsa.thesai.org
- [25] S. Kumar *et al.*, “Exploitation of Machine Learning Algorithms for Detecting Financial Crimes Based on Customers’ Behavior,” *Sustainability (Switzerland)*, vol. 14, no. 21, Nov. 2022, doi: 10.3390/su142113875.
- [26] P. Purushu, N. Melcher, B. Bhagwat, and J. Woo, “Predictive analysis of financial fraud detection using Azure and Spark ML,” *Asia Pacific Journal of Information Systems*, vol. 28, no. 4, pp. 308–319, 2018, doi: 10.14329/APJIS.2018.28.4.308.
- [27] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, “A flow-based approach for Trickbot banking trojan detection,” *Comput Secur*, vol. 84, pp. 179–192, Jul. 2019, doi: 10.1016/j.cose.2019.03.013.
- [28] A. Islam, M. Kamal Nasir, M. A. Islam, and M. K. Nasir, “EVALUATION OF MONEY LAUNDERING RISK OF BANK ACCOUNTS USING NAIVE BAYES CLASSIFICATION,” 2020.
- [29] A. RB and S. K. KR, “Credit card fraud detection using artificial neural network,” *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltip.2021.01.006.
- [30] G. Zhang, Z. Gao, J. Dong, and D. Mei, “Machine learning approaches for constructing the national anti-money laundering index,” *Financ Res Lett*, vol. 52, Mar. 2023, doi: 10.1016/j.frl.2022.103568.
- [31] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, “Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture,” *Mathematics*, vol. 10, no. 9, May 2022, doi: 10.3390/math10091480.
- [32] J. de J. Rocha-Salazar, M. J. Segovia-Vargas, and M. del M. Camacho-Miñano, “Money laundering and terrorism financing detection using neural networks and an abnormality indicator,” *Expert Syst Appl*, vol. 169, May 2021, doi: 10.1016/j.eswa.2020.114470.
- [33] B. Eulaiwi, N. S. Khalaf, A. Al-Hadi, L. Duong, and G. Taylor, “Money laundering governance and income shifting: Evidence from Australian financial institutions,” *Econ Model*, vol. 132, Mar. 2024, doi: 10.1016/j.econmod.2024.106653.
- [34] N. Ye, T. B. Kueh, L. Hou, Y. Liu, and H. Yu, “A bibliometric analysis of corporate social responsibility in sustainable development,” *J Clean Prod*, vol. 272, Nov. 2020, doi: 10.1016/j.jclepro.2020.122679.
- [35] F. Hussin, S. A. N. Md Rahim, N. S. M. Hatta, M. K. Aroua, and S. A. Mazari, “A systematic review of machine learning approaches in carbon capture applications,” *Journal of CO2 Utilization*, vol. 71, Elsevier Ltd, May 01, 2023. doi: 10.1016/j.jcou.2023.102474.
- [36] J. Han, Y. Huang, S. Liu, and K. Towey, “Artificial intelligence for anti-money laundering: a review and extension,” *Digit Finance*, vol. 2, no. 3–4, pp. 211–239, Dec. 2020, doi: 10.1007/s42521-020-00023-1.
- [37] S. Cosma, G. Rimo, and G. Torluccio, “Knowledge mapping of model risk in banking,” *International Review of Financial Analysis*, vol. 89, Elsevier Inc., Oct. 01, 2023. doi: 10.1016/j.irfa.2023.102800.
- [38] V. Anandhabalaji, M. Babu, and R. Brintha, “Energy consumption by cryptocurrency: A bibliometric analysis revealing research trends and insights,” *Energy Nexus*, vol. 13, p. 100274, Mar. 2024, doi: 10.1016/j.nexus.2024.100274.
- [39] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, “Intelligent Financial Fraud Detection Using Artificial Bee Colony Optimization Based Recurrent Neural Network,” *Intelligent Automation and Soft Computing*, vol. 37, no. 2, pp. 1483–1498, 2023, doi: 10.32604/iasc.2023.037606.
- [40] M. Maashi, B. Alabdullah, and F. Kouki, “Sustainable Financial Fraud Detection Using Garra Rufa Fish Optimization Algorithm with Ensemble Deep Learning,” *Sustainability (Switzerland)*, vol. 15, no. 18, Sep. 2023, doi: 10.3390/su151813301.
- [41] J. Liu, X. Gu, and C. Shang, “Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data,” *Complexity*, vol. 2020, 2020, doi: 10.1155/2020/6685888.
- [42] P. Xia, Z. Ni, X. Zhu, Q. He, and Q. Chen, “A novel prediction model based on long short-term memory optimised by dynamic evolutionary glowworm swarm optimisation for money laundering risk,” *International Journal of Bio-Inspired Computation*, vol. 19, no. 2, pp. 77–86, doi: 10.1504/IJBIC.2022.121233.