IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 20, 2021, accepted May 31, 2021, date of publication June 4, 2021, date of current version June 15, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3086230*

# Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review

**DATTATRAY VISHNU KUTE[1], BISWAJEET PRADHAN[1,2,3], (Senior Member, IEEE), NAGESH SHUKLA[1], AND ABDULLAH ALAMRI[4]**

[1]Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT, School of Information, Systems and Modelling, University of Technology Sydney, Sydney, NSW 2007, Australia
[2]Department of Energy and Mineral Resources Engineering, Sejong University, Seoul 05006, South Korea
[3]Earth Observation Centre, Institute of Climate Change, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia
[4]Department of Geology and Geophysics, College of Science, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Biswajeet Pradhan (biswajeet.pradhan@uts.edu.au)

This work was funded in part by the Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT, University of Technology Sydney (UTS), Sydney, NSW, Australia, and in part by the Researchers Supporting Project, King Saud University, Riyadh, Saudi Arabia, under Project RSP-2020/14.

**ABSTRACT** Money laundering has been a global issue for decades, which is one of the major threat for economy and society. Government, regulatory and financial institutions are combating it together in their respective capacity, however still billions of dollars in fines by authorities make the headlines in the news. High-speed internet services have enabled financial institutions to deliver better customer experience through multi-channel engagements, which has led to exponential growth in transactions and new avenues for laundering the money for fraudsters. Literature shows the usage of statistical methods, data mining and Machine Learning (ML) techniques for money laundering detection, but limited research on Deep Learning (DL) techniques, primarily due to lack of model interpretability and explainability of the decisions made. Several studies are conducted on application of ML for Anti-Money Laundering (AML), and Explainable Artificial Intelligence (XAI) techniques in general, but lacks the study on usage of DL techniques together with XAI. This paper aims to review the current state-of-the-art literature on DL together with XAI for identifying suspicious money laundering transactions and identify future research areas. Key findings of the review are, researchers have preferred variants of Convolutional Neural Networks, and AutoEncoder; graph deep learning together with natural language processing is emerging as an important technology for AML; XAI use is not seen in AML domain; 51% ML methods used in AML are non-interpretable, 58% studies used sample of old real data; key challenges for researchers are access to recent real transaction data and scarcity of labelled training data; and data being highly imbalanced. Future research directions are, application of XAI techniques to bring-out explainability, graph deep learning using natural language processing (NLP), unsupervised and reinforcement learning to handle lack of labelled data; and joint research programs between research community and industry to benefit from domain knowledge and controlled access to data.

**INDEX TERMS** Money laundering, machine learning, deep learning, explainable AI, suspicious transaction.

## I. INTRODUCTION

Money laundering and terrorism financing has been one of the major threat to the integrity of international financial system since last five decades [1]. The United Nations Office on Drugs and Crime (UNODC) estimates the amount of money laundered every year is approximately 2 – 5% of global GDP which amounts to $800bn - $2 trillion [2] and it is one of the biggest threat for the global economy and its security [3]. To fight against finance crime, many countries have laid stringent Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) policies for organizations who deal in cash, bullion, cryptocurrencies and financial transactions, for example AML/CTF act 2006 in Australia [4], Bank Secrecy Act

The associate editor coordinating the review of this manuscript and approving it for publication was Yudong Zhang.

1970 in USA [5]. The regulatory requires these organizations to deploy effective controls to monitor and report cash transactions beyond threshold values, International Fund Transfer Instructions (IFTIs), suspicious transactions of any kind and many more [2].

There have been several cases where financial institutions are penalized for not maintaining effective controls. In 2009, Credit Suisse Group of Switzerland was fined $536 million [6], in the same year Lloyds Banking Group of UK was fined $350 million [7]. In 2012, HSBC was fined by US authorities a sum of $1.9bn in a settlement over money laundering [8], in the same year ING Bank group of Netherlands was fined a penalty of $619 million for enabling launderers to illegally move billions of dollars through US banking system [9]. In 2017, Commonwealth Bank of Australia was ordered to pay the penalty of $700 million under AML/CTF act [10]. In 2019, 58 AML penalties handed out globally totaling $8.14bn, which is double the amount of penalty that was handed out in 2018 [11]. Very recently, in 2020, Westpac Bank of Australia was ordered to pay record-breaking $1.3 billion fine for breaching countries AML/CTF law [12]. By looking at the penalties handed over to various financial institutes until today, it indicates that the existing systems and controls are inadequate and ineffective to fight against the finance crime.

To combat the finance crime and comply with anti-money laundering requirements, traditionally banks have been using rule-based AML systems [13], which helps to identify cash transactions beyond threshold values, international fund transfers and suspicious transactions. These systems detect the suspicious transactions based on the predefined rules and raise the alerts. Compliance officer investigates these alerts and if it is found to be positive, a Suspicious Matter Report (SMR) is prepared and submitted to regulatory to ensure compliance reporting. The false positive rate of these alerts is estimated over 98% [14], which results in a huge operational cost to banks. Due to recent advancement in communication and technology, many banking services are made available to customers through different online channels. This has caused an explosion in a number of transactions. Due to the increase in transactions and continuously changing regulatory landscape, staying ahead of finance crime and compliance risk has become more complex and expensive than ever before for financial institutions.

By realizing the complexity, volume of the transactions and the success of artificial intelligence in other fields to improve operational efficiency and prediction accuracy, few banks have started putting in the efforts to automate the data and time-intensive tasks using Artificial Intelligence/Machine Learning (AI/ML) technologies [15] for detection of suspicious transactions. There is always a trade-off between model accuracy and interpretability while selecting a machine learning model. The black-box models such as neural networks, gradient boosting models can predict highly accurate results however often lags on interpretability hence it is difficult to explain the rationale behind the decisions made. On the other hand, the white-box models such as decision tree, linear regression are highly interpretable and easier to explain the decisions made by models, but provide less accurate results. Usually black-box models are chosen considering the high accuracy expectation in suspicious transaction detection, however the lack of transparency on how decisions are made by these models to conclude a transaction is suspicious; and a mandatory ask by regulators to provide rationale of transaction being suspicious, is posing an impediment for adoption of AI/ML technology in finance crime units in financial institutes [16].

Considering the continuous increase in transactions, changing fraud patterns and regulatory landscape, a robust end-to-end framework utilizing AI/ML is required which can help, to accurately detect the suspicious money laundering transaction by reducing the false positives and generate the human interpretable explanation for the decisions made by ML. Having such a framework will not only increase the efficiency in AML operations but also reduce operational cost that goes into investigation of false positive alerts [15], [17]. It will also help the banks to manage the compliance risk and keep the brand reputations intact. The explanations of the ML decisions will help build the trust in the system, which can also be accepted as an effective AML control by regulators [18].

The solutions to detect the money laundering pattern have been evolving from statistical methods, data mining [19], [20] and ML [13], [21] to DL [22], [23]. There are several review papers in literature that demonstrates the application of these methods for detecting suspicious transactions [3], [13], [20], [21], [24]–[29], however lacks the focused review on deep learning techniques or XAI techniques in the same domain.

The objective of this paper is to review the existing literature published on DL and XAI methods to detect suspicious money laundering transactions in financial institutions.

## II. BACKGROUND

Money laundering is a criminal activity used to disguise the source of illegally obtained money and make them appear legitimate in the system. Typically, money laundering involves 3 steps [30], (i) the first step is ''placement'' where cash is introduced in the financial system, (ii) the second step is ''layering'' where the complex financial transactions are performed to disguise the illegal source of the cash and; (iii) the third step is ''integration'' where the benefits are acquired from the transactions of illegal funds. The best step to identify a suspicious transaction is a placement step, because beyond the first step it becomes complex to trace the transactions since the transactions are layered within and/or outside of the bank purview.

In the context of money laundering, banks are obliged to monitor the transactions to detect the suspicious activities, investigate it, and report the same to regulatory to ensure compliance with AML/CTF policy. Effective AML systems, controls, practices are critical to manage the compliance risk.

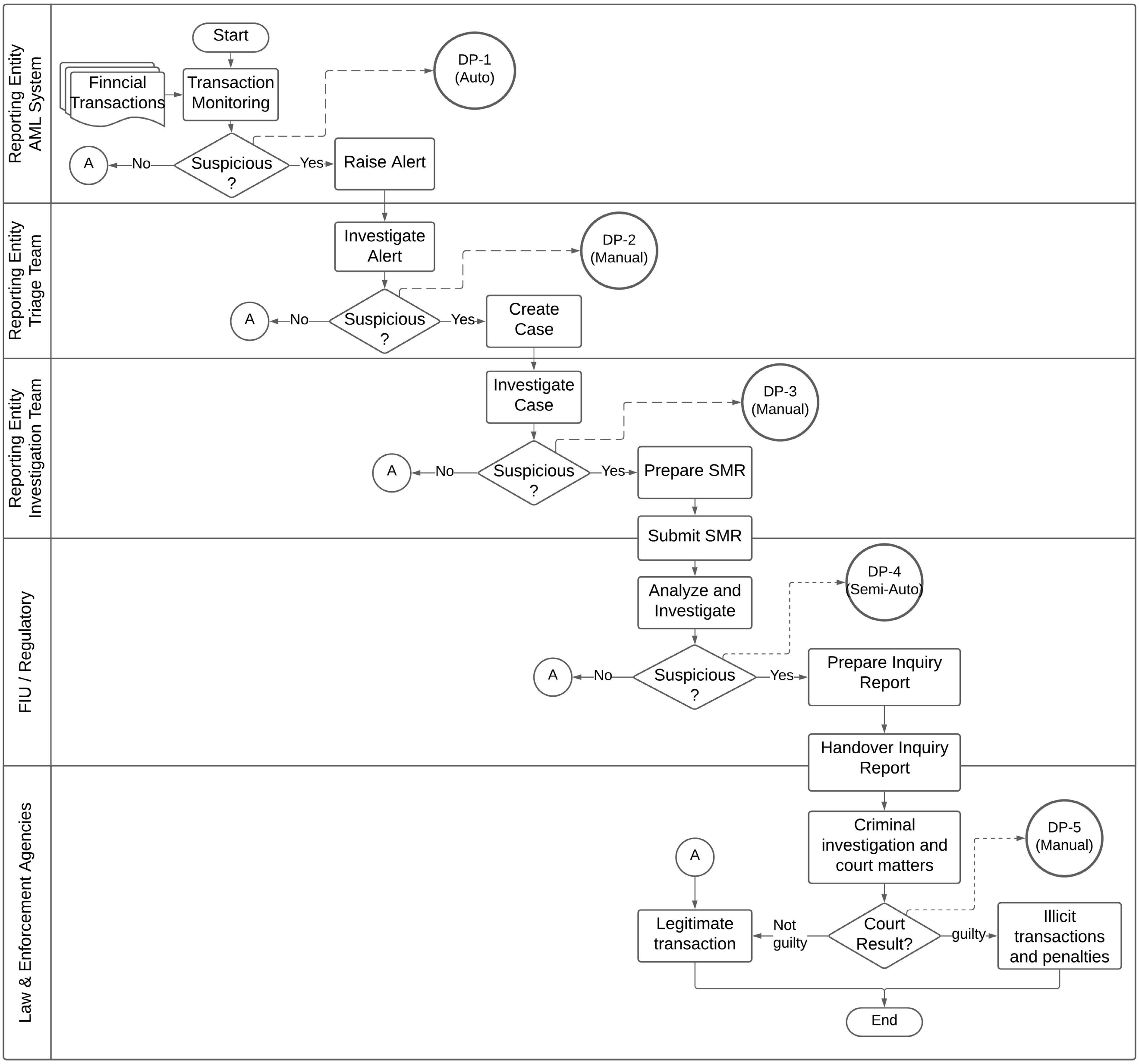


**FIGURE 1.** Anti-money laundering process.

FIGURE 1 represents a conceptual process followed in financial institutions for transaction monitoring, suspicious transaction detection and reporting the same to regulatory. It is evident that the suspicious transaction detection is a multi-step classification problem, because the confidence level of transaction being suspicious is built upon the investigation performed at each step from Alert to SMR and beyond the purview of financial institution. The decision of transaction being suspicious goes through 4 steps–(i) alert generation system (mostly automation), (ii) manual investigation at financial institution, (iii) investigation at FIUs, and (iv) the proceeds at court. Considering the efforts involved by various parties (Bank, FIU and Law & Enforcement agencies) it is important to get the detection of suspicious transaction correct to reduce the efforts. The whole scenario being highly sensitive and confidential in nature, the true suspicious transaction data is extremely difficult to find.

## III. RESEARCH METHODOLOGY

A review followed a standard 3 step review process described by Kitchenham and Charters [31]–Plan, Conduct and Report. Literature search is done using the combinations of the following keywords - “money laundering”, “suspicious transaction”, “anti-money laundering”, “deep learning”, “machine learning”, “data mining”, “statist*”, “explainable AI” and “XAI”. The papers were segregated based on the relevance to main topic and most relevant papers considered for review. The review focused on identifying the application of deep learning techniques for money laundering detection, reviewing the methods including machine learning to know if they are interpretable or not, identify if any explainable AI techniques are applied where non-interpretable methods are used and present the type of data used during model training and evaluations. Study also brought in the viewpoint of key review papers on "Machine Learning techniques on AML" and "Explainable AI techniques" subject from literature. Further paper discussed the findings, assessment and reported the key challenges and constraints for researchers, barriers for AI/ML adoption in AML domain. Finally, the paper concluded by identifying the state-of-art deep learning along with XAI techniques usage in AML domain, challenges and future research directions.

### A. AIM AND RESEARCH QUESTIONS

The key motivation for this work is, literature on money laundering detection shows the usage of statistical methods, data mining and machine learning techniques but lacks the focus on deep learning methods; interpretability of the methods is important from AML domain perspective but there isn't any comprehensive study that provides the details on current state of interpretability of the research published so far and the application of state-of-the-art XAI techniques in AML domain.

Hence the objectives of this review paper are - to identify the deep learning techniques applied in money laundering domain, determine the interpretability of the research published so far, identify the XAI techniques applied in AML domain to bring out the explainability; and answer the following questions:

- Is there an adequate research in data mining or machine learning to put it in practice?
- What DL methods are proposed to identify suspicious money laundering transactions?
- What XAI techniques are proposed to explain the decisions made by DL methods?
- Are the proposed methods trained, tested and validated on real data or synthetic data?
- Are there any evidences that shows the proposed methods are applied in the industry?

### B. SEARCH AND SELECTION PROCESS

The TABLE I below describes the combinations of keywords (money laundering, anti-money laundering, suspicious transaction, explainable AI, XAI, machine learning, deep learning, statist*) used to search for papers from Scopus library. The keyword search criteria was, "Search within: Article title, Abstract, Keywords" on Scopus library. Only published and peer-reviewed articles are considered for further review.

After skimming through the list of papers found in search results, the same was classified in 6 categories as shown in TABLE 2.

**TABLE 1.** Search queries and results.

| No. | Search Query | Papers |
|---|---|---|
| 1 | ("money laundering" OR "suspicious transaction" OR "anti-money laundering") AND ("explainable AI" OR "XAI") | 9 |
| 2 | ("money laundering" OR "suspicious transaction" OR "anti-money laundering") AND ("machine learning") | 75 |
| 3 | ("money laundering" OR "suspicious transaction" OR "anti-money laundering") AND ("deep learning") | 10 |
| 4 | ("money laundering" OR "suspicious transaction" OR "anti-money laundering") AND ("data mining") | 97 |
| 5 | ("money laundering" OR "suspicious transaction" OR "anti-money laundering") AND (statist*) | 7 |

**TABLE 2.** Literature classification.

| Paper classification | Statistical methods | Data mining | Machine learning | Deep learning | XAI methods |
|---|---|---|---|---|---|
| Duplicate papers | 1 | 20 | 5 | - | 1 |
| Non-relevant to finance | - | 14 | 10 | 3 | - |
| General finance crime papers | 2 | 5 | 4 | - | 2 |
| Review papers | 1 | 7 | 8 | - | 3 |
| Methods in non-AML fraud | 2 | 15 | 13 | 2 | 3 |
| Methods in AML | 1 | 36 | 35 | 5 | - |

Out of total 198 papers, 27 papers were found as a duplicate due to different queries, hence they are excluded. Another 27 papers are found as non-relevant to money laundering topic hence they are excluded. 13 papers found on finance crime topic in general, few are referred to establish the context as necessary. 19 review papers are found and are considered for discussions. 35 papers are found which are relevant to finance domain such as fraud but not related to money laundering, hence they excluded. 77 papers found that are directly related to money laundering that includes detection of suspicious money laundering transactions, patterns, and groups, they are considered for further review.

The information from the following category was used to establish the context. These papers are searched separately through independent sources including UTS library, internet and websites specific to organizations.

- *Regulatory and industry*–policy documents describing the compliance requirement, typologies and case study reports describing money laundering cases.
- *Penalties for non-compliance*–media newspaper, respective financial institute's websites, regulatory websites. This source of information indicates the effectiveness of the current solutions being used to fight money laundering without getting much into details explicitly.

## IV. RESULTS

In financial institutions, all transactions data coming from several internal banking systems such as retail banking, consumer banking, wealth management, institutional banking, etc.; flows through the rule based AML system, where each transaction is assessed against the pre-defined rules to identify (a) the transactions of $10,000 or more, (b) money transferred to and from overseas, and (c) suspicious activities involving money laundering or financial frauds. While rule-based systems are essential in banks and work well for identifying transactions as per pre-defined rules (category 'a' and 'b'), but it struggles to detect the emerging fraud patterns (category 'c'). If the transaction matches with the rule, a red flag or alert is raised, which is processed and reported to regulatory. The basis for rule definition is threshold amounts for different type of transactions based on the regulatory requirements [4], [5] and the recommendations given by FATF [1].

The key issues with rule-based systems from 'suspicious transaction detection perspective' are, keeping the rules up-to-date and relevant at all the times, and weighing different rules is almost impossible [32], generation of a large number of false positive alerts–up to 98% [33] and inability to handle a high volume of different type of structured data, semi-structured data or unstructured data [13]. More alerts means more efforts by the compliance officer to scan through it. If the staff confirms that the transaction can be justified enough to be true suspicious, then the bank is obliged to report the same by filing a SMR with the regulatory [4], [5]. The decision of concluding a transaction is suspicious is very important decision, if it goes incorrect the bank may end up reporting a good customer to regulatory for further investigation which may result into a criminal investigation by authorities and not identifying bad customers may result into continuing the money laundering activities by leveraging the banking systems and more finance crime.

Considering the limitations of rule-based systems, researchers have started leveraging the machine learning technologies to automatically identify the suspicious transaction patterns using a variety of solution categories such as AML typologies, link analysis, behavioral modelling, risk scoring, anomaly detection, and geographic capability [13].

## A. MACHINE LEARNING

There are several comprehensive and systematic review papers published over the decade that describes data mining and machine learning methods applied in AML domain. This paper will not describe those methods again here, instead list the most recent review papers in TABLE 3:

**TABLE 3.** Machine learning methods used in AML domain.

| No. | Literature reviews of AML | References |
|---|---|---|
| 1 | Review of machine learning methods | [3], [13], [21], [24] |
| 2 | Review of data mining methods | [20] |
| 3 | Application of statistical methods | [29] |
| 4 | Application of technological solutions | [26] |

### 1) REVIEW OF MACHINE LEARNING METHODS USED FOR MONEY LAUNDERING DETECTION

A literature review of money laundering and its related area was conducted by [3], with the aim of identifying the gaps and directing attention towards addressing them. The key findings are categorized into six groups as–(i) AML framework and effectiveness, (ii) impact of money laundering on economy, (iii) money laundering ecosystem and motivation, (iv) magnitude of money laundered, (v) avenues for money laundering, and (vi) detection methods of money laundering. As per the findings by [3], most studies of detecting money laundering have focused on transactions in banks, real-estate and trade based companies; however, the literature on detection of shell companies used for money laundering is meagre. Shell companies established in UK alone, were found to be linked with laundering £80bn between 2010 and 2014. The paper [3] has highlighted this gap in the literature and proposed a need for developing strategies to identify the shell companies involved in illicit activities.

A comprehensive survey conducted by [13] presents machine learning algorithms and methods applied to detect suspicious transactions. The results are organized in 6 solutions categories–AML typologies, anomaly detection, behaviors modelling, link analysis, geographic capability and risk scoring. Various methods are Analysed and compared. Authors have identified the key capabilities of the AML system as–efficient data preparation, data transformation and data analytics techniques. The key findings from the review is – inadequate focus on data quality assurance in the published research. Future research direction is to employ reinforcement learning to train the model considering the agility of financial operations.

A review conducted by [21] has brought out the machine learning algorithms used for identifying the money laundering patterns, detect unusual behavior, identify money laundering groups, and detecting money laundering groups. The identified ML algorithms/techniques are–Rule Based Methods, Decision Trees, Artificial Neural Networks (ANN), Support vector Machines (SVM), Random Forest, Outlier Detection Methods, Social Network Analysis (SNA), Naive Bayes, K-Nearest Neighbor (KNN), Deep Learning, Graph Mining, K-Means Clustering and One Class SVM. These identified methods have been thoroughly studied and compared to present how they behave for large and highly imbalanced datasets. The key findings of these papers are-each method has some strength and weakness hence the method needs to be leveraged as per the circumstances, though supervised and semi-supervised ML showed decent results and considered as out-of-the box solutions however they cannot find new ML patterns and have a high rate of false positives, therefore author feels unsupervised ML is the way forward to detect new money laundering patterns.

A literature review conducted by [24] focuses on the papers published between 2015 to 2020 to understand the state-of-the-art in AML systems, presents the results using the following categories–supervised learning, unsupervised learning, data sources, evaluation methods, implementation tools, sampling techniques and regions of study. The key findings by [24] are–Decision Tree, Radom Forest and SVM are most frequently used algorithms in AML system from supervised category, neural networks is mostly used in unsupervised category; Accuracy, Area Under the Curve (AUC) and precision are used for model evaluation; most of the data used for research was customer and transaction data from banks however there are many other methods for laundering the money such as restaurants, hotels and law offices, which are not researched enough.

#### 2) A REVIEW OF DATA MINING TECHNIQUES IN FINANCIAL FRAUD DETECTION

A comprehensive literature review was conducted by [20] on application and classification of data mining techniques for financial fraud detection by critically reviewing 49 journal articles published between 1997 and 2008. The financial fraud is classified into four categories as–bank fraud, insurance fraud, securities, and commodities fraud, and other relevant financial frauds. The data mining techniques are classified into six categories–(i) classification, (ii) regression, (iii) prediction, (iv) outlier detection, (v) visualization, and (vi) clustering. The key findings are–data mining techniques are largely applied in detection of insurance frauds, followed by corporate and credit card fraud, and identified a need of applying these techniques from money laundering, mortgage fraud and securities fraud. Only one technique 'network analysis' is found for detecting of money laundering. Otherwise, largely Logistic Models, Neural Network, Bayesian Neural Network, and Decision Trees are found to be used for detection of overall frauds.

#### 3) A SURVEY OF STATISTICAL METHODS FOR DETECTION OF MONEY LAUNDERING

Sudjianto *et al.* [29] provided a survey of statistical methods, data mining and machine learning techniques used for detection of money laundering and retail banking frauds. The authors identified the key challenges as–data volume and complexity, class imbalance, frequent evolving patterns, class overlap and, class mislabeling. The reviewed methods are classified in two categories as–supervised learning containing profiling, classification (SVM, BBN, HMM, neural network, classification Tree and classification rules) and link analysis; and unsupervised learning containing clustering, low-dimension representation and scoring, and anomaly detection. The key finding is, some methods are used effectively, however it is also emphasized to put more focus on preventing the fraud, example–employee training and awareness, defining policies and procedures.

#### 4) A REVIEW OF TECHNOLOGICAL SOLUTIONS FOR AML

A systematic literature review conducted by [26], on application of technological solutions to combat money laundering by reviewing 71 papers published between 1997 and 2019. The results are presented using the following categories–domains of application approaches and classification of support systems. Application domains are defined as-suspicious transaction detection, pattern detection/groups/money laundering anomalies, risk assessment/analysis, security, control, structuring and/or governance applications and visual analysis/applications of visual techniques. Support mechanism categories are defined as–systems/software/tools/programming languages, hardware, patterns/theories/frameworks, algorithms/mathematical application (data mining and machine learning). The key findings by [26] are, among the application domains, detection of suspicious transaction attracted more attention of researchers, from support systems adoption point of view, data mining techniques were used seldom for money laundering detection. A key gap identified from the papers was a need for data analysis description and evidence to support the benefits presented.

Apart from the reviews listed in the above 4 categories, [25] presents the review of anomaly detection methods for fraud detection using graph structures, [27] presents the analysis of anomaly detection, machine learning and neural networks, and [28] presents the measures for fraud detection.

It is evident from the literature described above that statistical methods and several machine learning techniques have been used for detection of money laundering. However, elaboration of DL technique usage is very limited. The following section describes the DL techniques used for money laundering as per the literature.

### B. DEEP LEARNING

Deep learning techniques have been used in various fields for predictions and found to be giving highly accurate results [34]–[36]. There were some challenges with DL such as a need for heavy computing, and more data, however, in today's world these challenges are no longer a big issue. This section describes the existing literature focused on usage of DL methods for detecting money laundering.

#### 1) SCALABLE GRAPH CONVOLUTIONAL NEURAL NETWORK

Weber *et al.* [22] used scalable graph convolutional neural network for forensic analysis for financial data which is massive, dense and dynamic in nature. The outcome of the analysis in visual form is presented as one of the effective decision support for the AML analysts who are involved in a review of large amount of alerts raised by rule-based AML systems. The method was developed and evaluated using the synthetic graph (1M nodes and 9 M edges) generated using the AMLSim data simulator tool. The vertex represents the account with attributes such as account number, account type, owner name and account creation date. The edge represents the transaction with attributes such as transaction ID, amount, timestamp. Using escalated alerts and SMRs as a label data, a semi-supervised learning model predicts the suspiciousness of a given node and potential bad actors in the transaction network based on the direct or indirect connections with the node. Author ran the experiment on a workstation with two deep graph model. First using the graph model GCN developed by [37], which took 611 seconds to converge in 32 epochs. Second experiment using the improved graph model FastGCN [38], which took 386 seconds to converge on the same number of epochs. FastGCN is twice as fast as GCN. Considering the huge amount of financial data that goes as millions of transactions per second, the training speed is important to timely identify the suspicious activities. The key findings of this study [22] are - graph deep learning has also been emerging as an important tool for AML, due to nature of the domain where relationships can be easily established using account data as node and transaction data as edges, and the model is able to handle the large volume of data however author recommends further improvements to reduce the training time.

### 2) MULTI-CHANNEL CONVOLUTIONAL NEURAL NETWORK

Han *et al.* [39] developed a novel distributed and scalable framework using DL driven natural language processing (NLP) technology to augment AML monitoring and investigation. The proposed framework performs different level of sentiment analysis, entity identification, relationship extraction, and link analysis on different data sources such as news, tweets, social media, etc. Each NLP module uses a specific data source to perform the analysis and bring the recommendations. The proposed framework is based on micro-service oriented distributed architecture and AMQP based integration platform, database as Cassandra, Neo4j and MySQL along with twitter and news engine. Two types of data are considered – financial data that includes KYC, Customer, Account, Transactions; and open data that includes financial news articles, financial reports, fraud open databases and social media contents. The system starts with identifying the suspicious transactions, then the key attributes are extracted from the alerted transactions such as name, location, account details which are used by next NLP modules. Finally, the suspicious transaction confidence score (in a range of 0.00 to 1.00) is calculated and presented by using the evidences produced by the following modules–TM, name screening, fraud knowledge base, sentiment analysis trend and entity disambiguation module. The sentiment analysis is used to identify the polarity of the sentiment–either positive or negative. Author used multi-channel convolutional neural network based sentiment classifier to process financial news and CNN based sentiment classifier for social media data. Relation extraction is used to predict the relation between pairs of entities in the sentence. Document level SA classifier, trained on auto labelled 12,467 financial news articles, achieved 76.96 % accuracy. Author used a pipeline based method for relationship extraction tasks. Name Entity Recognition (NER) is performed using a combination of two methods – Stanford NER recognizer and neural NRE based on LSTM-CRF framework. The NER model was evaluated on SemEval 1010 task 8 data and reported 80.62% micro-f1 measure. For handling multi-instance problem author has developed an RNN with word-level and sentence-level attention for relation prediction. The RNN model reported 88% accuracy using P@100 measure post evaluation on New York Times dataset. Overall experiment is performed on synthetic and real world dataset. The results are verified by AML experts who mentioned that approximately 30% cost can be saved over the existing manual approach of AML investigation. To give a perspective of the manual efforts, authors have given one example of bank, where 10,000 analysts globally investigated over 400,000 alerts of suspicious transactions per week. As a manual investigating process, the analysts are required to investigate several sources of data that include news search, name screening, querying fraud databases, crime records, fraud offenses or any existing suspicious activities. Author has identified the improvement areas that can be considered for future research as–consider domain specific data and fine-tune the parameters, scale and deploy system on cloud for processing large data in real time, tailor the solution and evaluate it in other domains.

### 3) AutoEncoder

Paula *et al.* [23] proposed the unsupervised deep learning model to classify Brazilian exporters to find out the possibility of committing the frauds in exports. The model uses the AutoEncoder classifier to detect anomalies considering the regular transaction patterns in the data. Brazilian exports are reaching to ∼200 countries with the help of 50,000 legal entities involved in shipping the goods. Author uses the database of foreign trade of the secretariat of federal revenue of Brazil for applying the DL model and finding out the export organizations whose explanatory variables of their export operations show signs of divergence compared to regular pattern. The paper has followed the CRISP-DM methodology for implementation, considering the flexibility of the model. Two methods are evaluated–AutoEncoder and PCA using 819,990 records and, H2O software and H2O R package. From data preparation perspective, 80 attributes were confirmed by the SMEs as adequate to prove a fraudulent exports. These 80 attributes went through the changes–using Gradient Boosting Machine (GBM) author identified 18 attributes to explain 80% variability, and 18 attributes were relativized to create 18 indices. These 18 indices reflect the participation of the attribute in which anomalies are sought. To detect anomalies, two methods are evaluated: AutoEncoder and PCA. AutoEncoder is found to be 20 times faster than PCA, AutoEncoder finds the subtle anomalies which PCA fails to detect and can detect the anomalies even with higher latent dimensions that linear PCA cannot. PCA requires more computation than AutoEncoder. Mean Square Error method is used to measure how distant the predictions were from the real data. Author has acknowledged the difficulty in evaluating the results against the business objectives to be achieved. This work has identified the suspected cases of fraudulent exports using unsupervised DL that looks promising, however, it needs further thorough assessment by experts. Depending on the assessment results by experts, the model may need to adjust the number of hidden layers and neurons to have better results.

### 4) GRAPH CONVOLUTIONAL NEURAL NETWORK

Alarab *et al.* [40] presented a novel approach based on graph convolutional neural network to predict illicit transactions in the bitcoin transaction graph. The proposed method has used GCN along with multi-layer perceptron, which has given better results than only GCN as used in the original research paper. The features derived from GCN and the latent representation of a linear layer boosts the performance of the model. The proposed approach is evaluated using elliptic data, a publicly available dataset that belongs to real Bitcoins transactions, which is represented as a directed graph network of transactions that are nodes, the directed edges between the transactions represent the payment flow from source to destination. The dataset is labelled as licit and illicit. The graph network containing 203,769 node transactions and 234,355 edges representing the payments flow between nodes. 2% of the data set are labelled as illicit, while 21% are labelled as licit transactions. Accuracy of this model is 0.974 while the accuracy of previous models compared is 0.961. Real time of the transaction is not used as a feature in the proposed model, which is identified as an additional feature for the model to try out in the future.

### 5) MULTI-LAYER PERCEPTRON

Weber *et al.* [41] has proposed a multi-classification method for detecting suspicious behavior and categorizing the money laundering related crime using SVM, Liner Regression (LR) and Multi-Layer Perceptron. Two models are produced. Model 1 trained using SVM, LR and MLP (with ReLU activation function) methods by giving inputs as financial transactions and profile data, that gives the suspicious transaction dataset as output, and Model 2 is trained using the same methods, by giving the input dataset as fraudulent transactions and suspicious transactions to determine the suspicious transactions along with the crime category. Author used the synthetic data for training and testing. The model precision rates are–88.13, 87.53 and 90.42 for SVM, LR and MLP respectively.

## *C. EXPLAINABLE AI*

Advancement in computing and storage infrastructure, continuous generation of large volume of data and a need to utilize this data to derive actionable insights has escalated the research in machine learning methodology over the last decade. The accurate prediction has remained the primary goal during the model development and ended up having many complex models or black box models, such as DL models with high accuracy. These complex models are opaque, whose actions are difficult to understand for humans. The lack of transparency, interpretability and explainability of the DL/ML models is making the adoption difficult for the domains (medical, banking, crime, law) where the predictions or recommendations made by black boxes are expected to be used to make critical decisions that involves human life. Not every domain requires the explainability, for example: weather forecast does not need explanation if the black box can give highly accurate results. Similarly, ads displayed on social media based on the browsing habit do not need the explanation of how the ads are chosen.

Explainable AI has become a prerequisite for building the trust, and to drive adoption of AI systems in high stake domains such as finance crime, credit risks, healthcare which requires reliability, safety and fairness [42], [43] [18]. The regulations like General Data Protection Regulation (GDPR) [44] particularly 'Records of Processing Activities', and 'Right to be informed'; and California Consumer Private Act (CCPA) [45] have also imposed the interpretability and explainability mandates for most of the AI/ML solutions in regulatory compliance domain.

For detecting the money laundering patterns, suspicious transactions, anomalies; or for performing the investigative tasks using link analysis or graph mining, many machine learning methods are found in the literature, with reasonable accuracy. For AML domain, where the suspicious transactions are required to be reported to regulatory by preparing the SMRs, it is critical to include adequate evidences that justifies the suspiciousness. Since most of the machine learning models that give high accuracy are black box in nature, it fails to create the trust in using AI/ML enabled system.

To assess the interpretability of the ML models recommended for AML domain, we conducted a study of 77 research articles (identified in a ''Methods in AML'' category as per TABLE 2) that presented a unique model for detection of money laundering.

The TABLE 4 provides the outcome of this study. We choose 43 papers that described the ML methods, and excluded the papers that described approach, system architecture or papers from other domains. The methods are classified using supervised, semi-supervised, unsupervised and reinforcement learning category. The *problem* column indicates the key problem addressed by *methods* using *data* in the paper mentioned in *Ref* column. The meaning of *interpretability* in column 'Is Method Interpretable' is, the ability of the method to present indicators that can help humans to understand the functioning of the method to know how decisions are made by the method.

FIGURE 2 shows the analysis based on the 43 papers filtered that provides the solutions using machine learning models for money laundering pattern detection, suspicious transaction detection, money launderers group detection and help investigation using link analysis. FIGURE 2.a shows that the highest number of papers are published in year 2020 in AML domain, that indicates the escalation in attention the subject is getting to leverage machine learning technology to help solve one of the highly complex problem of industry. FIGURE 2.b shows that 51% researchers have used non-interpretable methods.FIGURE 2.c shows 65% methods are based on supervised learning while only 2% have used reinforcement learning models. FIGURE 2.d shows 58% methods

**TABLE 4.** Interpretability of methods used for AML.

| No. | Category | Problem | Method | Is Method Interpretable | Data | Year | Ref |
|---|---|---|---|---|---|---|---|
| 1 | Supervised learning | Watch-list filtering automation to prevent false positives | SVM, Naïve Bayes, Decision Tree - individually | Yes | Synthetic | 2021 | [46] |
| 2 | | Identification of illicit Bitcoin transactions | Ensemble Method using RF, Extra Trees, and Bagging Classifier. | No | Elliptic | 2020 | [47] |
| 3 | | Predict illicit transactions in bitcoin transaction graph | Graph Convolutional Network and Multi-Layer Perceptron together. | No | Elliptic | 2020 | [47] |
| 4 | | Detecting potentially illicit behavior | Logistic Regression, *Extreme gradient boosting trees Catboost methods* | No* | Real | 2020 | [48] |
| 5 | | Detect illicit accounts involved in money laundering over ethereum blockchain | Extreme Gradient Boosting (XGBoost) | No | Public Dataset | 2020 | [49] |
| 6 | | Examine AI methodologies against money laundering crimes | Logistic regression, decision tree, *Random Forest, XGBoost, and AutoEncoder, DNN* | No* | Real | 2020 | [50] |
| 7 | | Detect suspicious money laundering transactions | XGBoost algorithm | No | Real | 2020 | [32] |
| 8 | | Detect suspicious money laundering transactions | Naïve Bayes Classifier | Yes | Synthetic | 2020 | [51] |
| 9 | | Identification of suspicious transactions and categorizing the type of finance crime | SVM, Liner Regression, *Multi-layer Perceptron* | No* | Synthetic | 2019 | [41] |
| 10 | | Suspicious money laundering transaction detection | Bayes Logistic Regression, Decision Tree, Random Forest, SVM, and *ANN* | No* | Real | 2019 | [52] |
| 11 | | Suspicious money laundering transaction detection | Random Forest; MinMaxScaler method | Yes | Synthetic | 2018 | [53] |
| 12 | | Proposes a technique for generating variants of typologies | Graph Learning, BigData | No | Unclear | 2018 | [54] |
| 13 | | Detect money laundering criminals – actual court case | Logistic Regression, Decision Tree, Random Forest and *Neural Networks* | No* | Real | 2018 | [55] |
| 14 | | Detect money launders laundering groups | Support Vector Machine and *Random Forests* | No* | Real | 2017 | [56] |
| 15 | | Improve the suspicious transaction signaling process by client profiling | PART algorithm that implements Decision tree, best leaf technique | Yes | Real | 2016 | [57] |
| 16 | | Suspicious money laundering transaction detection | Affiliation Mapping Calculation and Sequential Mining (AMC-SM) | Unclear | Unclear | 2016 | [58] |
| 17 | | Identification of suspicious money laundering accounts | Probabilistic Relational Model using the Audit Sequential Pattern (PRM-ASP) Mining | Unclear | Real | 2015 | [59] |
| 18 | | Detection of fraud chains in Mobile Money Transfer systems. | Predictive Security Analysis at Runtime (PSA@R) | Unclear | Synthetic | 2014 | [60] |
| 19 | | Identification of suspicious money laundering transaction | DBSCAN Clustering algorithm, Link analysis | Yes | Real | 2014 | [61] |
| 20 | | Identification of suspicious financial transactions | Clustering, Dynamic Bayesian Networks, Anomaly Detection | Yes | Real | 2011 | [62] |
| 21 | | Suspicious money laundering transaction detection | Graph learning method | No | Synthetic | 2011 | [63] |
| 22 | | Identify suspicious money laundering activities | Decision Tree (BIRCH and k-means) | Yes | Unclear | 2011 | [64] |
| 23 | | Suspicious money laundering transaction detection | Clustering (K-means), *Neural Network (back-propagation)* | No* | Real | 2010 | [65] |
| 24 | | Identify the most critical classifiers for decision tree used in investigation of money laundering | Decision Tree | Yes | Real | 2010 | [66] |
| 25 | | Identify money laundering cases within investment activities | Clustering, *Neural Network*, Genetics Algorithm | No* | Real | 2010 | [67] |
| 26 | | Identification of suspicious money laundering transaction | Decision Tree | Yes | Real | 2008 | [68] |

are either trained or evaluated on a small set of real data older than 2 years. 21% researches are done based on synthetic data. It is observed that the real data is obtained from following organizations–financial institutions, financial intelligence units, police department, and organizations involved in exports.

**TABLE 4.** ***(Continued)*** **Interpretability of methods used for AML.**

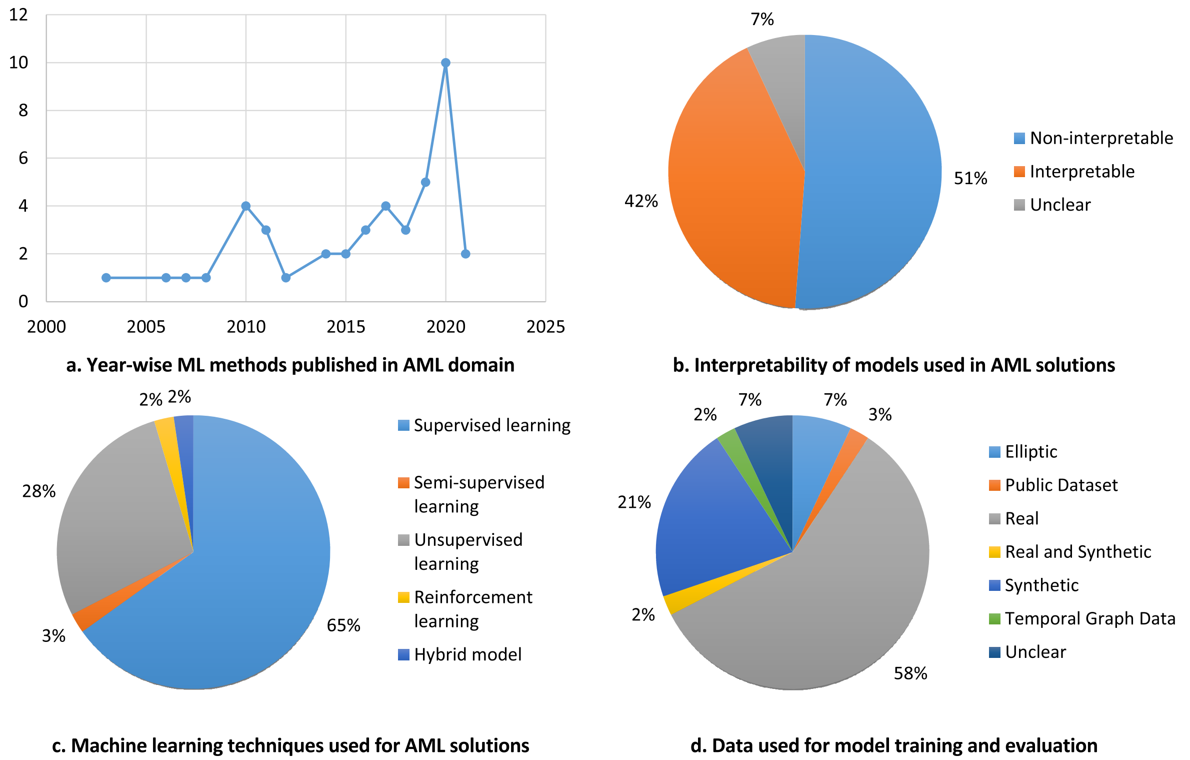
| No. | Category | Problem | Method | Is Method Interpretable | Data | Year | Ref |
|---|---|---|---|---|---|---|---|
| 27 | | Detection of hidden money laundering behavior | *Multi-agent Neural Network*, *Text Mining*, Genetic Algorithms, Velocity Analysis and Case-based reasoning | No* | Real | 2007 | [69] |
| 28 | | Facilitate investigation of money laundering crime | Link discovery based on correlation analysis | Yes | Real | 2003 | [70] |
| 29 | Unsupervised learning | Suspicious money laundering transaction detection | Core Decision Tree and Clustering Algorithm | No* | Real | 2021 | [71] |
| 30 | | Identify fraudulent financial transactions | Outlier Detection Methods, Visual Analytics Method | Yes | Real | 2020 | [72] |
| 31 | | Identify anomalies in a set of transactions of a non-banking correspondent | Isolation Forest, One Class SVM | Yes | Real | 2020 | [73] |
| 32 | | Detect hidden networks of money launderers | Isolation Forest – One Class SVM | Yes | Synthetic | 2020 | [74] |
| 33 | | Identify suspicious transaction in crypto currency | Expectancy Maximization (for clustering datasets), Random Forest (for anomaly detection) | No | Elliptic | 2019 | [75] |
| 34 | | Detect anomalies considering the regular transaction patterns | AutoEncoder and PCA examined separately | No | Real | 2017 | [76] |
| 35 | | Identify suspicious money laundering transactions | *Ensemble* of algorithms (Isolation Forests, One Class SVM, *Gaussian Mixture Models*, EM) | No* | Real and Synthetic | 2017 | [77] |
| 36 | | Detection of money launderers gangs | Community detection using temporal-directed Louvain algorithm | No | Real | 2017 | [78] |
| 37 | | Detection of money laundering transactions. Visualization and analysis system for Police Analysts. | Apriori, PrefixSpan, FP-growth and Eclat algorithms | Yes | Real | 2016 | [79] |
| 38 | | Suspicious money laundering transaction detection | Clustering CLOPE algorithm | Yes | Real | 2012 | [80] |
| 39 | | Identify suspicious sequences of transaction level for financial institutions | Scan Statistics | Yes | Real | 2010 | [81] |
| 40 | | Detect suspicious money laundering transactions | Semantic Core Tree | Yes | Synthetic | 2006 | [82] |
| 41 | Semi-supervised learning | Investigation Support System for AML | Multi-channel Convolutional Network based on NLP | No | Synthetic | 2015 | [83] |
| 42 | Reinforcement learning | Incremental graph pattern matching algorithm to deal with time-evolving graph data for detecting money laundering | Incremental graph pattern matching (IGPM) algorithm and partial execution manager (PEM) to re-compute the updated subgraphs | No | Temporal graph data | 2019 | [84] |
| 43 | Supervised and unsupervised learning | Detect trade-based money laundering | Supervised – Bayesian network, Cost sensitive learning<br>Unsupervised – clustering, regression | Yes | Real | 2019 | [85] |

* It indicates that the methods used by authors of respective paper includes interpretable and non-interpretable methods.

Given the steps involved in anti-money laundering, efforts involved by multiple organizations together, it becomes more critical to identify the suspicious money laundering transactions, patterns, groups as accurately as possible along with adequate explanation for the decisions made by the ML models. As the model accuracy increases the interpretability goes down, and in order to know how models are making decisions it needs to be interpretable. So far, the research focus has been more on increasing the model accuracy and rather than ensuring the model interpretability. This has triggered another research area that is Explainable AI.

XAI is a class of system that provides visibility into how an AI system makes the decisions, predictions and executes its actions [86]. Inter-disciplinary research area, XAI has attracted great attention from the researchers around the world. XAI techniques are applied in other related domains such as, in bitcoin domain [87] presented a study of applying XAI techniques to visualize and understand the results obtained from unsupervised learning, [88] presented an explainable anomaly detection technique for procurement fraud detections; however no research found in the literature that describes the application of XAI techniques for money laundering domain. This is a clear gap and potential for future research.

The study conducted by [89] enforces the need to understand the operational environment of stakeholders who are going to use the explanations generated by XAI methods, to support their decision-making process. Author proposes a scenario-based requirement elicitations method for developing user-centric explanations using XAI methods for fraud detections. Knowing the lack of interpretability and explainability of the black box models, researchers have already made exponential progress on coming up with different post-hoc approaches over last 5 years. There are several



**a. Year-wise ML methods published in AML domain**

**b. Interpretability of models used in AML solutions**

**c. Machine learning techniques used for AML solutions**

**d. Data used for model training and evaluation**

**FIGURE 2. Interpretability analysis of ML methods used in AML.**

review papers published on XAI techniques that describes concepts, taxonomy, methods, and challenges; the most recent comprehensive review papers on XAI subject are listed in TABLE 5.

There are several reasons why the explanation is required for the decisions made by black box models based on the subject of research domain, for example–regulatory application domain wants the explanation to *justify* the decisions, security application domain wants the explanation to *control* the underlying data and IP that may be uncovered, some domains would need the explanation to *improve* the decisions, other domains would need the explanation to discover the knowledge [90]. Further authors discussed the topic using 5 W's and How (What, Who, When, Why, Where, and How) to bring out the existing literature.

The survey, conducted by [91], is emphasizing the literature based on the importance of the trust in the system and a genuine need of explainability, Transparency and Interpretability for the AI applications in judiciary, governmental, finance and autonomous transport.

Explainable AI work is categorized into two groups [92]–(i) *transparency design* that focuses on the internal functioning of the model from developer's point of view and (ii) *post-hoc design,* which explains why a result is inferred from the user's point of view.

The study conducted by [16] has explained the underlying concepts of model Explainability, XAI taxonomies, opportunities, challenges and way forward to Responsible AI. XAI purpose and concepts are discussed using *what*, *why*, *what for*, and *how* aspects. The review of XAI is presented using two categories–(i) *potentially interpretable models*-the ML models having some level of transparency to make it interpretable (such as linear/logistic regression, decision tree, K-nearest neighbors, rule based learning, general additive models and Bayesian models) and (ii) *post-hoc techniques* (model agnostics, post-hoc techniques for shallow models, Explainability in DL, and alternate taxonomy for post-hoc techniques for DL models) that helps to make the ML models interpretable; resulting into a global taxonomy. Further, author leads the discussion towards *Responsible AI*, by defining the AI principles (fairness, transparency, and privacy) to follow when implementing AI models. It is noted that implementing XAI has some implications, especially on compromising the privacy involved by the data and business rules which are confidential in nature. Author's view is, the model interpretability should be addressed together with requirements and constraints of data privacy, model confidentiality, fairness and accountability.

Researchers from neural-symbolic integration (NSI) have tried to extract the relational knowledge from neural networks by proposing several methods but have remained a challenge to extract distinct and salient features from the input and hidden layers. Further the methods of identifying the relationship between the features have emerged. Townsend *et al.* [93] presented a review of the old and new methods of extraction without relational explanation. The review presents

**TABLE 5.** Explainable AI–review papers.

| No. | Explainable AI review paper title | Ref |
|---|---|---|
| 1 | Peeking Inside the Black-Box: A Survey on XAI | [90] |
| 2 | XAI: A survey from trust and genuine need of explainability perspective | [91] |
| 3 | XAI: History, Research Areas, Approaches and Challenges | [92] |
| 4 | XAI: Concepts, taxonomies, opportunities and challenges toward responsible AI | [16] |
| 5 | Extracting Relational Explanations from Deep Neural Networks: A Survey from a Neural-Symbolic Perspective | [93] |
| 6 | Explaining the black-box model: A survey of local interpretation methods for deep neural networks | [94] |
| 7 | A Survey of Data-driven and Knowledge-aware XAI | [95] |
| 8 | A Survey of Contrastive and Counterfactual Explanation Generation Methods for Explainable Artificial Intelligence | [96] |
| 9 | XAI: A review of machine learning interpretability methods | [97] |
| 10 | Explainable Reinforcement Learning: A Survey | [98] |

29 knowledge extraction methods by grouping them into 3 categories–(i) work that extracts quantized features only, (ii) work that extracts quantized feature along with relationship and (iii) embedding methods with associated extraction methods.

Due to the surge in performance of deep neural network models but lagging on explainability, has driven many researchers to come up with different machine learning interpretable methods. Significant efforts have gone into producing different interpretable methods, out of which the local interpretable methods are standing out from clear expression of feature and low on computation complexity point of view [94]. The local interpretable methods for DNN published between 2012 and 2020 are categorized into two groups [94]as (i) model-driven– describes 20 methods and (ii) data-driven–describes 27 methods.

Li *et al.* [95] reviewed a literature of XAI published over the last decade and presented using three phases of XAI lifecycle– methodology, evaluation and application. The methodology is presented using two categories–(i) *knowledge driven XAI* which requires external knowledge to produce the explanation, and (ii) *data driven XAI* methods which are reviewed from global, local and instance-specific methods point of view. The XAI evaluation metrics are classified into two categories – computational metrics (usually standardized and automated by AI experts) and cognitive metrics (usually collected by user-study). Further author has reviewed the XAI application for self-driving and finance AI.

There are multiple ways to look at the explanation required for the decisions made by black-box models. One approach is *evidence-based explanation* that describes the details of parameters that contributed to make the decision. Another approach is *Contrastive and Counterfactual (C&C) explanations* that justify why the output of the algorithms is not any different from what it is and how it could be changed, respectively. [96] examined the theoretical foundation for C&C explanations and reported the state-of-the-art computation frameworks for generating the C&C explanations and identified the shortcomings which can be a topic of future research.

Linardatos *et al.* [97] presented a comprehensive review of machine learning interpretability methods using 4 categories–(i) Methods for explaining black box models (17 methods focused on DL method interpretations, 16 methods that can explain any black-box model), (ii) methods for creating white-box models (5 methods), (iii) methods that promote fairness and restrict discrimination, (iv) methods that analyses the sensitivity of model predictions (28 methods). Most interpretability methods are focused on DL, largely ruled by neural networks, and are experimented with image classification explanation. Local Interpretable Model-Agnostic Explanations (LIME) [99] and SHapley Additive exPlanations (SHAP) [100] are the highly referred and experimented methods for producing explanations on black box models that use any type of data, followed by Partial Dependence Plots (PDPs).

Puiutta and Veith *et al.* [98] conducted a XAI literature review by keeping the reinforcement learning at center, because most of the XAI literature reviews are around supervised learning. In reinforcement learning, the models autonomously learn and make the decisions, which is equally important to know the reasons or explanations behind the decisions.

Knowing the need and importance of having the answers for following questions to AI models–why did you do that, why not something else, when do you succeed, when do you fail, when can I trust you, how do correct an error; USA Defense Advanced Research Project Agency [101] initiated a 4 year long XAI program to work on the same.

While there is mammoth progress on XAI method, [102] argues that the development in XAI is a patchwork to existing ML models and major effort of research community is going in the wrong direction. Author firmly recommends to stop using the black box machine learning models along with XAI techniques for high stake decisions, instead use the interpretable models. Author believes that the research effort should be directed towards developing new interpretable models that can give the required accuracy.

## V. DISCUSSION

Money laundering detection solutions are categorized in two groups. First category is to *identify the suspicious transactions*, example - [23], [40] has presented the AutoEncoder and Graph CNN deep learning methods respectively to identify suspicious transactions; and second category is to help investigate the identified suspicious transactions or alerts identified by rule-based systems, which is commonly called as *decision support systems*, example - [22], [39] has presented a multi-channel CNN using NLP and scalable GCN method as a decision support system for investigating the alerts, respectively.

Presently many financial institutions use rule based systems for detecting the transactions (beyond certain threshold values, international fund transfers and suspicious transaction of any nature) that are required to be reported to regulatory to be compliant with AML/CTF policies. While rule-based-system is crucial, but it generates many false positive alerts for suspicious transaction which requires huge manual effort to triage the same (example - in a global bank approximately 10,000 analysts investigates over 400,000 alerts per week [22]). Few technology savvy financial institutions have started leveraging AI/ML technology to automate such activities to improve the accuracy of detection of suspicious activities [15] but it remains a long way for adoption by many because of lack of explainability of the decisions made by AI/ML models.

Over last decades several papers have been published with different machine learning techniques summarized in many comprehensive literature review papers such as [3], [21], [24], [25], however by looking at the penalties issued by authorities for financial institutions in single year 2019 [11], it is evident that the published methods are either not useful or not used.

Despite the technological advancements from statistical methods, machine learning to DL, severity of 'suspicious money laundering transactions detection' issue has remained more or less constant since last two decades (example Tang and Yin [103] presented a SVM based method in 2005, [32] presented machine learning based technique in year 2020). Many research articles are published presenting the application of these methods to detect suspicious transactions and claimed the improvements in double digits, however rare evidences on practical use of these methods by relevant entities such as financial institutions and the actual performance in terms of false positive alerts reduction or operational cost reduction.

Graph Neural Networks is observed as one of the most commonly used method for detection of suspicious transaction and money laundering networks. Along with the potential of using graph neural networks, there are several challenges [104] such as complexities due to high-speed transaction systems, real-time systems, multi-channel updates, data size, data speed, data variety, and several business applications involved; which makes the practical implementation harder. Hence it is essential to consider the right infrastructure, appropriate tools and considerations for these challenges to improve the performance of future graph-based solutions.

### A. KEY CHALLENGES FOR DETECTION OF MONEY LAUNDERING

- *Changing canvas*–While the technological advancements has made the banking easy for customers, but also presented new avenues for fraudsters. The increase in volume and frequency of transactions, multiple customer channels, real-time transaction settlement, digital banking and changing fraud patterns has kept the canvas changing. Continuously changing regulatory landscape has also been a challenge for industry.
- *Multi-step classification*–The inherent nature of 'suspicious money laundering transaction detection' is a multi-step classification problem, where the decision of suspiciousness is taken at transaction level, alert level, case level, SMR level and finally by the law & enforcement agency level. Few decisions are taken by software and few requires human intervention for investigation. Only a degree at which the transaction is suspicious can be improved in a system, because whether the transaction is indeed money laundering or legitimate is always decided by a well-established and responsible government agency at the end.
- *Slow adoption of AI technology*–Though many complex models such as deep neural networks have given promising results in terms of accuracy and performance in other domains, but lacks on the transparency and interpretability of models which creates a barrier for AI adoption in AML domain.
- *AML domain being confidential in nature*–Many researched methodologies for detecting suspicious money laundering transactions are patented and hence they are not published for obvious reasons [105]. This also creates a gap/disconnect between what is indeed applied in practice vs what techniques/methods available, to solve the problem.

### B. CONSTRAINTS FOR RESEARCHERS FROM DATA PERSPECTIVE

- *Real data*–Banks and financial institutions are the custodians of the customer's data that includes customer's personally identifiable information, the products and transactions data. The customer data cannot be shared with anybody other than the customer, which is limited to his/her own data. From research of "suspicious transaction detection" point of view, customer, products and transactions are the key source of data. The researches where real data is used, mostly it is older than two years and a fraction of the data that any financial institution possesses.
- *Training data*–The suspicious transactions data and suspicious transaction alerts data is considered as highly sensitive data, since this is used by banks to prepare SMR for submission to regulatory. Based on the investigation outcome of the SMR by regulatory, it results in either SMR close or criminal investigation against the account holder. Banks are obliged to keep the SMRs confidential from even the customer who owns the data. From a research point of view, suspicious transaction data and suspicious transaction alerts data are key label data to train the supervised ML model to detect suspicious money laundering transaction.
- *Authenticity of training data*–The transactions involved in actual money laundering is rarely known to the financial institutions, because it remains confidential information with law enforcement department and regulatory.

This is an accurate label data to train the supervised ML models to detect suspicious money laundering transaction, but is not easily available.

- *Real data speed and volume*–Every day, the bank generates millions of transactions of different types through various banking systems and multiple channels. This is a large volume of data, generated at large velocity and of large variety. Many banks are struggling to catch up with the speed at which the data is getting created and consolidating the same together to get a view for analysing it to gain the insights or apply the advanced analytics techniques to identify the money laundering and financial frauds.
    - *Class imbalance, overlap and mislabelling*–The suspicious transactions are way too less than the legitimate transactions that creates a data imbalance while training the ML models, transactions used for money laundering are made similar to legitimate transaction that creates the overlap, and unavailability of the true money laundering case data leads to relying on existing suspicious transaction data that results in mislabelling of the data used by ML models [29]. A study conducted by [48] has presented a two-layered approach to address the class-imbalance and scalability issue for machine learning.

### C. BARRIERS FOR ADOPTION OF AI/ML IN FINANCE CRIME DOMAIN

Financial institutions believe in the potential of AI technology can help in several business cases [43]. Some organizations have already started taking baby steps by developing small prototypes using AI/ML [15]. However, the overall adoption of AI is slow primarily due to following reasons:

- *Explainability*–the models that give high prediction accuracy are usually non-interpretable in nature that makes it difficult to understand the reasoning behind the decisions made [42].
- *Trust*–humans trust the system if they know exactly how it functions. The black-box models which gives high accuracy but lacks on interpretability of the model, and that does not inspire the confidence and trust in the system [18].
- *Privacy*–the data used by ML algorithms includes the customer, accounts and transaction data, there are concerns around the usage of this information or revealing the confidential information while bringing out the explanations of the decisions [106].
- *AI ethics*–there are concerns regarding the AI agents making the biased decisions or discriminations while interpreting and making decisions [106].
- *Law and enforcement*–the courts across many developed countries are struggling to develop convincing and clear-enough guidelines for directing legislative and administration considerations for adoption of AI [107].

### D. THE WAY FORWARD

Machine learning and deep learning technology is used by select few AML software product vendors (such as SAS, Actimize, Oracle, LexisNexis, Fiserv.) for suspicious transaction detection. Most financial institutions heavily depend on third-party products for detecting suspicious activities. Different statistical methods, data mining and machine learning techniques are used by the products. Most AML products are trained on synthetic data and once the product is live in financial institutions, it is fine-tuned based on the real data. The third-party products are commonly IP protected but on top of it, even the decisions made by these products are not transparent and explainable to AML analysts to inspire the trust and confidence in system. Hence the research on AML domain using machine learning or deep learning should be driven by Responsible AI principles to ensure the technology is applied in a transparent way, yet safeguarding the interest of each player involved in the financial ecosystem.

### E. FUTURE RESEARCH DIRECTIONS FOR AML DOMAIN

While there has been a continuous research on finding out the best possible solution to detect and report the money laundering transactions, by researchers, commercial product companies and financial institutions; below are the directions for research identified after studying the literature:

- *Data pre-processing*–AML domain uses the data generated by internal banking systems, data from authorised third party such as World-Check, PEP screening, Sanctions screening, and social network data. Most of the published researches have used a limited set of data (limited to transactions) and ignored the data pre-processing part [13] and [19]. It is important to get the complete domain context, data sources, data types, and leverage the same to detect money laundering.
- *Evaluating the model against large data*–Most of the methods found in literature have been evaluated using a small set of data on limited computing, compared to the data that gets generated practically on day-to-day basis in financial institutions. Hence it is important to consider the large data scenarios to evaluate the models.
- *Graph mining and Social network analysis*–These techniques are an apt solution for finding the patterns, groups and perform the link analysis, which is helpful for detection of money laundering, launderer gangs and identify the relationships to find more leads in the money laundering networks. Though there are challenges in graph mining from large data processing point of view [104], but this is one of the potential area where research should be continued.
- *Applying Explainable AI techniques*–It is a need of AML domain to have an Explanation of the decisions made by non-interpretable models [42], [106]. There are several explainable AI techniques researched so far, for example

few of them - [86, 99-101], however to the best of our knowledge none of it is applied in AML domain yet. Hence application of XAI techniques can be further researched on the non-interpretable models that gives good accuracy of detection.

- *Ensemble learning*–Considering the number of financial systems, type of available data, data sources, volume of data; one specific model cannot be a solution instead ensemble learning must be considered to leverage the available data to bring out more confidence in suspiciousness of transaction along with evidences. It could include statistical methods, data mining, machine learning and deep learning all together. Example - [77] has applied the ensemble learning to find the suspicious transactions in distributed ledger payments.
- *Unsupervised learning*–Research efforts can be better utilised by focusing on unsupervised learning or reinforcement learning [13], considering the fact that AML data is highly imbalanced and true labelled data unavailability [108].
- *Academician and industry gap*–Many researchers attempted to solve the suspicious transaction detection issue, have used a synthetic data or a very small sample of real data compared to the actual data reporting-entity generates on a day-to-day basis. Hence the results shown by research papers can be far away from the reality if the methods are applied in practice. Part of the reason being, customer account and transaction data is highly sensitive and not always available in a required quantity. It is recommended to explore wherever possible to conduct a joint research with the organisations from finance industry to benefit from each other's expertise and controlled access to real data for research.
- *Data sharing between reporting entities*–Each financial institution has the accumulated intelligence/knowledge gained about the suspicious customers, suspicious transaction patterns, and fraud patterns. If the accumulated knowledge is available to all entities with adequate legal protection to prevent misuse of the same; combating money laundering can be improved further. A study conducted by 109] presents a secure framework for AML using ML and secret sharing between Banks, which is one step in this direction. Another study conducted in Japan proposes a global knowledge management of suspicious money laundering transactions from financial institutions (local) to FIU national) to FATF/Egmont Group (international) [110].

## VI. CONCLUSION

Money laundering problem exists since last five decades and the challenge of identifying suspicious money laundering transactions remains the same today as well, primarily due to following reasons - continuously changing canvas of fraud, technology and regulatory; being a multi-step classification problem, the challenges around the data for research and barriers for adoption of AI by industry. After having gone through the literature, it is evident that there are several machine learning methods recommended for suspicious transaction detection by researchers. However, hardly any evidence of application of the same in the industry. The possible identified reasons are–most researches are based on either sample of a very old real data or synthetic data, lack of training data (alerts, suspicious transactions) and lack of actual money laundering transaction data, lack of current real-data containing possible latest fraud patterns, and data being highly sensitive and confidential in nature. Limited research is seen on applying DL methods and absolutely no research in the area of applying XAI techniques for suspicious money laundering detection domain to the best of our knowledge. From the list of DL techniques identified from literature, out of 5 articles 3 articles have chosen CNN variant–graph based CNN, scalable CNN and multi-channel CNN based on NLP; 4th article has chosen AutoEncoder and 5th chose MLP. Our study also found that 51% of the machine learning models used in AML solutions are non-interpretable methods. Hence, along with accuracy and performance, it is important to consider model transparency, interpretability, explainability, privacy issues and define how the proposed model is going to fit into the overall AML solutions stack to put it into practice. This review paper has identified the key challenges for AML, barriers for adoption of AI/ML, constraints for researchers and future research directions. In a summary apart from focusing on DL and XAI technology for AML domain, possible research directions for better outcome is a joint research programs between academicians and financial institutions focusing on identification of suspicious transactions; between academicians and Financial Intelligence Units (FIUs) focusing on investigation and decision support systems.

## AUTHOR CONTRIBUTIONS

Conceptualization, D.K., B.P.,; Overall supervision and concept: B.P., methodology and formal analysis, D.K.; data curation, D.K.; writing—original draft preparation, D.K.; writing—review and editing, B.P., N.S.; supervision, B.P., N.S.; funding–B.P., A.A., All authors have read and agreed to the published version of the manuscript.

## CONFLICT OF INTEREST

The authors declare no conflict of interest.

## REFERENCES

[1] F. A. T. Force. (2020). *International Standards On Combating Money Laundering and The Financing Of Terrorism & Proliferation—FATF Recommendations, F.A.T. Force, Editor. 2020, Financial Action Task Force*. [Online]. Available: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html

[2] *Global Money Laundering*, Crime, U.N.O.o.D.a., Vienna, Austria, Feb. 2021.

[3] M. Tiwari, A. Gepp, and K. Kumar, "A review of money laundering literature: The state of research in key areas," *Pacific Accounting Rev.*, vol. 32, no. 2, pp. 271–303, 2020.

[4] Office of Parliamentary Counsel Australia. (2019). *Anti-Money Laundering and Counter-Terrorism Financing Act 2006, AUSTRAC, Editor*. [Online]. Available: https://www.legislation.gov.au/Details/C2019C00011

[5] *Bank Secrecy Act (BSA) Statute*, F.C.E. Netw., Vienna, Austria, Feb. 2021.

[6] Department of Justice. (Feb. 2021). *O.o.P.A. Credit Suisse Group of Switzerland Was Fined $536 Million. 2009* [Online]. Available: https://www.justice.gov/opa/pr/credit-suisse-agrees-forfeit-536-million-connection-violations-international-emergency

[7] J. Quinn and K. G. Lloyds. Banking Group of UK was fined $350 million (2009). *The Telegraph. The Telegraph*. [Online]. Available: https://www.telegraph.co.uk/finance/4213151/Lloyds-TSB-agrees-to-pay-fine-of-350m-for-sanctions-help.html

[8] CBS News. (2012). *HSBC to Pay $1.9B to Settle Money-Laundering Case. www.cbc.ca* [Online]. Available: https://www.cbc.ca/news/business/hsbc-to-pay-1-9b-to-settle-money-laundering-case-1.1226871

[9] The Wall Street Journal. (2012). *ING Fined a Record Amount, Penalty of $619 Million Tied to Cuba, Iran for Violating U.S. Economic Sanctions*. [Online]. Available: https://www.wsj.com/articles/SB10001424052702303901504577462512713336378

[10] Centre, A.T.R.a.A. (2018). *AUSTRAC and CBA Agree $700m Penalty*. [Online]. Available: https://www.austrac.gov.au/austrac-and-cba-agree-700m-penalty

[11] B. Monroe. (Feb. 2021). *Fincrime Briefing: AML Fines in 2019 Breach $8 Billion, Treasury Official Pleads Guilty to Leaking, 2020 Crypto Compliance Outlook*. [Online]. Available: https://www.acfcs.org/fincrime-briefing-aml-fines-in-2019-breach-8-billion-treasury-official-pleads-guilty-to-leaking-2020-crypto-compliance-outlook-and-more/#:~:text=Key%20observations%3A,25%20penalties%20totaling%20%242.29bn

[12] Centre. (2020). *A.T.R.a.A. AUSTRAC and Westpac Agree to Proposed $1.3bn Penalty*. [Online]. Available: https://www.austrac.gov.au/news-and-media/media-release/austrac-and-westpac-agree-penalty

[13] Z. Chen, "Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review," *Knowl. Inf. Syst.*, vol. 57, no. 2, pp. 245–285, 2018.

[14] Media Company. (2019). *Risk Transforming Approaches to AML and Financial Crime*. Accessed: Feb. 26, 2021. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Transforming%20approaches%20to%20AML%20and%20financial%20crime/Transforming-approaches-to-AML-and-financial%20crime-vF.pdf

[15] Institute of International Finance. (2018). *Machine Learning in Anti-Money Laundering—Summary Report*. [Online]. Available: www.iif.com

[16] B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. Garcia, S. Gil-Lopez, D. Molina, R. Benjamins, R. Chatila, and F. Herrera, "Explainable explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Inf. Fusion*, vol. 58, pp. 82–115, Jun. 2020.

[17] R. Al-Shabandar, G. Lightbody, F. Browne, J. Liu, H. Wang, and H. Zheng, "The application of artificial intelligence in financial compliance management," in *Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM)*, 2019, pp. 1–6.

[18] PricewaterhouseCoopers. (Feb. 2021). *Explainable AI Driving Business Value Through Greater Understanding. 2017*. [Online]. Available: https://www.pwc.co.uk/services/risk-assurance/insights/explainable-ai.html

[19] M. E. Lokanan, "Data mining for statistical analysis of money laundering transactions," *J. Money Laundering Control*, vol. 22, no. 4, pp. 753–763, Oct. 2019.

[20] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Syst.*, vol. 50, no. 3, pp. 559–569, 2011.

[21] N. M. Labib, M. A. Rizka, and A. E. M. Shokry, *Survey of Machine Learning Approaches of Anti-Money Laundering Techniques to Counter Terrorism Finance* (Lecture Notes in Networks and Systems). Singapore: Springer, 2020, pp. 73–87.

[22] M. Weber, J. Chen, T. Suzumura, A. Pareja, T. Ma, H. Kanezashi, T. Kaler, C. E. Leiserson, and T. B. Schardl, "Scalable graph learning for anti-money laundering: A first look," 2018, *arXiv:1812.00076*. [Online]. Available: https://arxiv.org/abs/1812.00076

[23] E. L. Paula, "Deep learning anomaly detection as support fraud investigation in Brazilian exports and anti-money laundering," Inst. Elect. Electron. Engineers Inc., CA, USA, Tech. Rep. 7838276, 2017.

[24] A. A. S. Alsuwailem and A. K. J. Saudagar, "Anti-money laundering systems: A systematic literature review," *J. Money Laundering Control*, vol. 23, no. 4, pp. 833–848, May 2020.

[25] P. Irofti, A. Pătraşcu, and A. Băltoiu, "Fraud detection in networks," in *Studies in Computational Intelligence*. Cham, Switzerland: Springer, 2021, pp. 517–536.

[26] G. S. Leite, A. B. Albuquerque, and P. R. Pinheiro, "Application of technological solutions in the fight against money laundering—A systematic literature review," *Appl. Sci.*, vol. 9, no. 22, p. 4800, 2019.

[27] A. Semenov, "Survey of common design approaches in AML software development," in *Proc. CEUR-WS*, 2017, pp. 1–9.

[28] B. Shaju and N. Valliammal, "Measures for financial fraud detection using data analytics and machine learning," *Int. J. Adv. Sci. Technol.*, vol. 28, no. 17, pp. 270–280, 2019.

[29] A. Sudjianto, "Statistical methods for fighting financial crimes," *Technometrics*, vol. 52, no. 1, pp. 5–19, 2010.

[30] F. A. T. Force. (2021). *What is Money Laundering*. Accessed: Feb. 26, 2021. [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

[31] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," in *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Keele, U.K., 2007.

[32] M. Jullum, A. Løland, R. B. Huseby, G. Ånonsen, and J. Lorentzen, "Detecting money laundering transactions with machine learning," *J. Money Laundering Control*, vol. 23, no. 1, pp. 173–186, Jan. 2020.

[33] T. Davenport. (2020). The Future Of Work Now: AI-Driven Transaction Surveillance At DBS Bank. Forbes [Online]. Available: https://www.forbes.com/sites/tomdavenport/2020/10/23/the-future-of-work-now-ai-driven-transaction-surveillance-at-dbs-bank/?sh=4772a6383f7f

[34] S. Jaiswal and M. Valstar, "Deep learning the dynamic appearance and shape of facial action units," IEEE, Lake Placid, NY, USA, Tech. Rep. 7477625, 2016, doi: 10.1109/WACV.2016.7477625.

[35] Y. Liang, "State of the art control of Atari games using shallow reinforcement learning," in *Proc. Int. Found. Auton. Agents Multiagent Syst. (IFAAMAS)*, 2016, pp. 485–493.

[36] C. Szegedy, "Going deeper with convolutions," *IEEE Comput. Soc.*, to be published.

[37] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2017, pp. 1–14.

[38] J. Chen and T. C. M. Xiao, "FastGCN: Fast learning with graph convolutional networks via importance sampling," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2018, pp. 1–15.

[39] J. Han, "NextGen AML: Distributed deep learning based language technologies to augment anti money laundering investigation," in *Proc. Assoc. Comput. Linguistics (ACL)*, 2015, pp. 37–42.

[40] I. Alarab, S. Prakoonwit, and M. I. Nacer, "Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain," in *Proc. Assoc. Comput. Machinery*, 202, pp. 23–27.

[41] Y. Feng, C. Li, Y. Wang, J. Wang, G. Zhang, C. Xing, Z. Li, and Z. Lian, "Anti-money laundering (AML) research: A system for identification and multi-classification," in *Proc. 16th Web Inf. Syst. Appl. Conf. (WISA)*, W. Ni, Ed. Cham, Switzerland: Springer, 2019, pp. 169–175.

[42] A. Mashrur, "Machine learning for financial risk management: A survey," *IEEE Access*, vol. 8, pp. 203203–203223, 2020.

[43] F. Königstorfer and S. Thalmann, "Applications of artificial intelligence in commercial banks—A research agenda for behavioral finance," *J. Behav. Exp. Finance*, vol. 27, Sep. 2020, Art. no. 100352.

[44] European Union, "General data protection regulation (GDPR)," *Official J. Eur. Union*, p. 43 and 50–51, Apr. 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[45] *TITLE 1.81.5. California Consumer Privacy Act of 2018*, California Legislative Body, CA, USA, 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5#:~:text=and%20to%20Whom-,(a)%20A%20consumer%20shall%20have%20the%20right%20to%20request%20that,business%20collected%20about%20the%20consumer

[46] M. Alkhalili and M. H. F. Q. Almasalha, "Investigation of applying machine learning for watch-list filtering in anti-money laundering," *IEEE Access*, vol. 9, pp. 18481–18496, 2021.

[47] I. Alarab, S. Prakoonwit, and M. Nacer, "Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain," in *Proc. 5th Int. Conf. Mach. Learn. Technol. (ICMLT)*, 2020, pp. 23–27.

[48] P. Tertychnyi, "Scalable and imbalance-resistant machine learning models for anti-money laundering: A two-layered approach," in *Proc. 10th Int. Workshop Enterprise Appl., Markets Services Finance Ind. (FinanceCom)*, B. Clapham and J. Koch, Eds. Cham, Switzerland: Springer, 2020, pp. 43–58.

[49] S. Farrugia and J. G. E. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," *Expert Syst. Appl.*, vol. 150, p. 2 and 15, Jul. 2020, Art. no. 113318, doi: 10.1016/j.eswa.2020.113318.

[50] O. Garcia-Bedoya, O. Granados, and J. C. Burgos, "AI against money laundering networks: The colombian case," *J. Money Laundering Control*, vol. 24, no. 1, pp. 49–62, May 2021.

[51] A. Kumar, S. Das, and V. Tyagi, "Anti money laundering detection using Naïve Bayes classifier," in *Proc. IEEE Int. Conf. Comput., Power Commun. Technol. (GUCON)*, 2020, pp. 568–572.

[52] Y. Zhang and P. Trubey, "Machine learning and sampling scheme: An empirical study of money laundering detection," *Comput. Econ.*, vol. 54, no. 3, pp. 1043–1063, 2019.

[53] S. Magomedov, S. Pavelyev, I. Ivanova, A. Dobrotvorsky, M. Khrestina, and T. Yusubaliev, "Anomaly detection with machine learning and graph databases in fraud management," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 33–38, 2018.

[54] K. Plaksiy, A. Nikiforov, and N. Miloslavskaya, "Applying big data technologies to detect cases of money laundering and counter financing of terrorism," in *Proc. 6th IEEE Int. Conf. Future Internet Things Cloud Workshops (W-FiCloud)*, 2018, pp. 70–77.

[55] E. Badal-Valero, J. A. Alvarez-Jareño, and J. M. Pavía, "Combining Benford's law and machine learning to detect money laundering. An actual spanish court case," *Forensic Sci. Int.*, vol. 282, pp. 24–34, Jan. 2018.

[56] D. Savage, "Detection of money laundering groups: Supervised learning on small networks," in *Proc. 31st AAAI Conf. Artif. Intell. (AAAI)*, 2017, pp. 24–34.

[57] C. Alexandre and J. Balsa, "Integrating client profiling in an anti-money laundering multi-agent based system," in *Proc. World Conf. Inf. Syst. Technol. (WorldCIST)*, M. M. Teixeira, Ed. Cham, Switzerland: Springer-Verlag, 2016, pp. 931–941.

[58] V. Jayasree and R. V. S. Balan, "Anti money laundering in financial institutions using affiliation mapping calculation and sequential mining," *J. Eng. Appl. Sci.*, vol. 11, no. 1, pp. 51–56, 2016.

[59] V. Jayasree and R. V. S. Balan, "Money laundering identification on banking data using probabilistic relational audit sequential pattern," *Asian J. Appl. Sci.*, vol. 8, no. 3, pp. 173–184, Jun. 2015.

[60] M. Zhdanova, J. Repp, R. Rieke, C. Gaber, and B. Hemery, "No smurfs: Revealing fraud chains in mobile money transfers," in *Proc. 9th Int. Conf. Availability, Rel. Secur.*, Sep. 2014, pp. 11–20.

[61] Y. Yang, B. Lian, L. Li, C. Chen, and P. Li, "DBSCAN clustering algorithm applied to identify suspicious financial transactions," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2014.

[62] S. Raza and S. Haider, "Suspicious activity reporting using dynamic Bayesian networks," in *Proc. 1st World Conf. Inf. Technol. (WCIT)*, Istanbul, Turkey, 2010, pp. 987–991.

[63] K. Michalak and J. Korczak, "Graph mining approach to suspicious transaction detection," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Szczecin, Poland, 2011, pp. 69–75.

[64] R. Liu, X.-L. Qian, S. Mao, and S.-Z. Zhu, "Research on anti-money laundering based on core decision tree algorithm," in *Proc. Chin. Control Decis. Conf. (CCDC)*, May 2011, pp. 4322–4325.

[65] N.-A. Le-Khac, S. Markos, and M.-T. Kechadi, "Towards a new data mining-based approach for anti-money laundering in an international investment bank," in *Proc. 1st Int. Conf. Digit. Forensics Cyber Crime (ICDF2C)*, Albany, NY, USA, 2010, pp. 77–84.

[66] I. George and M. Kavakli, "Data mining in the investigation of money laundering and terrorist financing," in *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection*. Hershey, PA, USA: IGI Global, 2010, pp. 228–241.

[67] N. A. Le Khac and M.-T. Kechadi, "Application of data mining for anti-money laundering detection: A case study," in *Proc. IEEE Int. Conf. Data Mining Workshops*, Sydney, NSW, Australia, Dec. 2010, pp. 577–584.

[68] C. H. Zhang and X. H. Zhao, "Research on money laundering recognition based on decision thee algorithm," *Wuhan Ligong Daxue Xuebao/J. Wuhan Univ. Technol.*, vol. 30, no. 2, pp. 154–156, 2008.

[69] Q. Yang, B. Feng, and P. Song, "Study on anti-money laundering service system of online payment based on union-bank mode," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Shanghai, China, Sep. 2007, pp. 4991–4994.

[70] Z. Zhang, J. J. Salerno, and P. S. Yu, "Applying data mining in investigating money laundering crimes," in *Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2003, pp. 747–752.

[71] 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, Art. no. 114470.

[72] R. A. L. Torres and M. Ladeira, "A proposal for online analysis and identification of fraudulent financial transactions," in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2020, pp. 240–245.

[73] J. Guevara, O. Garcia-Bedoya, and O. Granados, "Machine learning methodologies against money laundering in non-banking correspondents," in *Proc. 3rd Int. Conf. Appl. Inform. (ICAI)*, H. Florez and S. Misra, Eds. Cham, Switzerland: Springer, 2020, pp. 72–88.

[74] A. E. M. Shokry, M. A. Rizka, and N. M. Labib, "Counter terrorism finance by detecting money laundering hidden networks using unsupervised machine learning algorithm," in *Proc. 13th IADIS Int. Conf. (ICT), Soc. Hum. Beings (ICT), 6th IADIS Int. Conf. Connected Smart Cities (CSC), 17th IADIS Int. Conf. Web Based Communities Social Media (WBC), 14th Multi Conf. Comput. Sci. Inf. Syst. (MCCSIS), 13th IADIS Int. Conf. ICT, Soc. Hum. Beings (ICT), 6th IADIS Int. Conf. Connected Smart Cities (CSC), 17th IADIS Int. Conf. Web Based Communities Social Media (WBC), 14th Multi Conf. Comput. Sci. Inf. Syst. (MCCSIS IADIS)*, 2020, pp. 89–97. [Online]. Available: https://www.elearning-conf.org/wp-content/uploads/2020/07/02_202008L012_F050.pdf

[75] H. Baek, J. Oh, C. Y. Kim, and K. Lee, "A model for detecting cryptocurrency transactions with discernible purpose," in *Proc. 11th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2019, pp. 713–717.

[76] E. L. Paula, "Deep learning anomaly detection as suppor fraud investigation in Brazilian exports and anti-money laundering," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, 2017, pp. 954–960.

[77] R. D. Camino, R. State, L. Montero, and P. Valtchev, "Finding suspicious activities in financial transactions and distributed ledgers," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2017, pp. 787–796.

[78] X. Li, X. Cao, X. Qiu, J. Zhao, and J. Zheng, "Intelligent anti-money laundering solution based upon novel community detection in massive transaction networks on spark," in *Proc. 5th Int. Conf. Adv. Cloud Big Data (CBD)*, Aug. 2017, pp. 176–181.

[79] R. Drezewski, G. Dziuban, Ł. Hernik, and M. Paczek, "Comparison of data mining techniques for money laundering detection system," in *Proc. Int. Conf. Sci. Inf. Technol. (ICSITech)*, Oct. 2015, pp. 5–10.

[80] D. K. Cao and P. Do, "Applying data mining in money laundering detection for the Vietnamese banking industry," in *Proc. 4th Asian Conf. Intell. Inf. Database Syst. (ACIIDS)*, Kaohsiung, Taiwan, 2012, pp. 207–216.

[81] X. Liu and P. Zhang, "A scan statistics based suspicious transactions detection model for anti-money laundering (AML) in financial institutions," in *Proc. Int. Conf. Multimedia Commun. (Mediacom)*, 2010. Hong Kong, 2010, pp. 210–213.

[82] C. Yunkai, L. Zhengding, L. Ruixuan, L. Yuhua, and S. Xiaolin, "The research of an incremental conceptive clustering algorithm and its application in detecting money laundering," *Wuhan Univ. J. Natural Sci.*, vol. 11, no. 5, pp. 1076–1080, Sep. 2006.

[83] J. Han, U. Barman, J. Hayes, J. Du, E. Burgin, and D. Wan, "NextGen AML: Distributed deep learning based language technologies to augment anti money laundering investigation," in *Proc. ACL Syst. Demonstrations*, 2018, pp. 37–42.

[84] H. Kanezashi, T. Suzumura, D. Garcia-Gasulla, M.-H. Oh, and S. Matsuoka, "Adaptive pattern matching with reinforcement learning for dynamic graphs," in *Proc. IEEE 25th Int. Conf. High Perform. Comput. (HiPC)*, Dec. 2018, pp. 92–101.

[85] X. Chao, "Behavior monitoring methods for trade-based money laundering integrating macro and micro prudential regulation: A case from China," *Technol. Economic Develop. Economy*, vol. 25, no. 6, pp. 1081–1096, 2019.

[86] A. Rai, "Explainable AI: From black box to glass box," *J. Acad. Marketing Sci.*, vol. 48, no. 1, pp. 137–141, Jan. 2020.

[87] R. S. Shah, A. Bhatia, A. Gandhi, and S. Mathur, "Bitcoin data analytics: Scalable techniques for transaction clustering and embedding generation," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021.

[88] A. Westerski, "Explainable anomaly detection for procurement fraud identification—Lessons from practical deployments," *Int. Trans. Oper. Res.*, pp. 1–2, Mar. 2021, doi: 10.1111/itor.12968.

[89] D. Cirqueira, "Scenario-based requirements elicitation for user-centric explainable AI," in *Proc. Int. Cross-Domain Conf. Mach. Learn. Knowl. Extraction (CD-MAKE)*, vol. 4, A. Holzinger, Ed. Cham, Switzerland: Springer, 2020, pp. 321–341.

[90] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018.

[91] F. K. Dosilovic and M. N. B. Hlupic, "Explainable artificial intelligence: A survey," Inst. Elect. Electron. Eng., Opatija, Croatia, Tech. Rep. 17880343, 2018, doi: 10.23919/MIPRO.2018.8400040.

[92] F. Xu, *Explainable AI: A Brief Survey on History, Research Areas, Approaches and Challenges*, J. Tang, Ed. Cham, Switzerland: Springer, 2019, pp. 563–574.

[93] J. Townsend, T. Chaton, and J. M. Monteiro, "Extracting relational explanations from deep neural networks: A survey from a neural-symbolic perspective," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 9, pp. 3456–3470, Sep. 2020.

[94] Y. Liang, "Explaining the black-box model: A survey of local interpretation methods for deep neural networks," *Neurocomputing*, vol. 419, pp. 168–182, Jan. 2021.

[95] X.-H. Li, C. C. Cao, Y. Shi, W. Bai, H. Gao, L. Qiu, C. Wang, Y. Gao, S. Zhang, X. Xue, and L. Chen, "A survey of data-driven and knowledge-aware eXplainable AI," *IEEE Trans. Knowl. Data Eng.*, to be published.

[96] I. Stepin, J. M. Alonso, A. Catala, and M. Pereira-Farina, "A survey of contrastive and counterfactual explanation generation methods for explainable artificial intelligence," *IEEE Access*, vol. 9, pp. 11974–12001, 2021.

[97] P. Linardatos, V. S. Papastefanopoulos, and S. Kotsiantis, "Explainable AI: A review of machine learning interpretability methods," *Entropy*, vol. 23, no. 1, pp. 1–45, 2021.

[98] E. Puiutta *Explainable Reinforcement Learning: A Survey*, A. Holzinger, Ed. Cham, Switzerland: Springer, 2020, pp. 77–95.

[99] M. T. Ribeiro and S. C. Singh Guestrin, "'Why should i trust you?': Explaining the predictions of any classifier," in *Proc. ACM SIGKDD*, 2016, pp. 1135–1144.

[100] S. M. Lundberg and S. I. Lee, "A unified approach to interpreting model predictions," in *Proc. Neural Inf. Process. Syst. Found.*, 2017, pp. 4766–4775.

[101] D. Gunning and D. W. Aha, "DARPA's explainable artificial intelligence program," *AI Mag.*, vol. 40, no. 2, pp. 44–58, 2019.

[102] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," *Nature Mach. Intell.*, vol. 1, no. 5, pp. 206–215, 2019.

[103] J. Tang and J. Yin, "Developing an intelligent data discriminating system of anti-money laundering based on SVM," in *Proc. Int. Conf. Mach. Learn. Cybern.*, 2005, pp. 3453–3457.

[104] E. Kurshan, H. Shen, and H. Yu, "Financial crime & fraud detection using graph computing: Application considerations & outlook," in *Proc. 2nd Int. Conf. Transdisciplinary AI (TransAI)*, Sep. 2020, pp. 125–130.

[105] A. Korauš, "Using quantitative methods to identify security and unusual business operations," *Entrepreneurship Sustainability Issues*, vol. 6, no. 3, pp. 1101–1112, 2019.

[106] F. S. Board, *Artificial Intelligence and Machine Learning in Financial Services 2017*. Basel, Switzerland: Financial Stability Board.

[107] T. Rademacher, "Artificial intelligence and law enforcement," in *Regulating Artificial Intelligence*. Cham, Switzerland: Springer, 2019, pp. 225–254.

[108] A. I. Canhoto, "Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective," *J. Bus. Res.*, vol. 131, pp. 441–452, Jul. 2021.

[109] A. Zand, J. Orwell, and E. Pfluegel, "A secure framework for anti-money-laundering using machine learning and secret sharing," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Secur.)*, Jun. 2020, pp. 1–7.

[110] N. Yasaka, "Global knowledge management of suspicious transaction reporting system in Japan," *J. Money Laundering Control*, vol. 23, no. 1, pp. 55–63, Jan. 2020.

**DATTATRAY VISHNU KUTE** received the B.Engg. degree in computer science and engineering from Dr. BAM University, India. He is currently pursuing the M.Res. degree with the Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT, University of Technology Sydney (UTS). His research interests include the application of machine learning, deep learning, and explainable AI techniques in banking and finance domain. He has over two decades of work experience in information technology in providing solutions to large customers from various industries, including banking and finance, hi-tech, supply chain, mining, manufacturing, automotive, defense, government, and consumer electronics. His area of work include enterprise architecture, solution architecture, and consulting. He received the Senior Management Certificate in general business management from the Indian Institute of Calcutta, India.

**BISWAJEET PRADHAN** (Senior Member, IEEE) received the Habilitation degree in remote sensing from the Dresden University of Technology, Germany, in 2011. He is currently the Director of the Centre for Advanced Modelling and Geospatial Information Systems (CAMGIS), Faculty of Engineering and IT. He is the Distinguished Professor with the University of Technology Sydney. He is an internationally established scientist in the fields of geospatial information systems (GIS), remote sensing and image processing, complex modeling/geo-computing, machine learning and soft-computing applications, natural hazards, and environmental modeling. From 2015 to 2021, he served as the Ambassador Scientist for the Alexander Humboldt Foundation, Germany. Out of his more than 650 articles, more than 500 have been published in science citation index (SCI/SCIE) technical journals. He has authored eight books and 13 book chapters. He was a recipient of the Alexander von Humboldt Fellowship from Germany. He has been receiving 55 awards in recognition of his excellence in teaching, service, and research, since 2006. He was a recipient of the Alexander von Humboldt Research Fellowship from Germany. From 2016 to 2020, he was listed as the World's Most Highly Cited Researcher by Clarivate Analytics Report as one of the world's most influential mind. From 2018 to 2020, he was awarded as the World Class Professor by the Ministry of Research, Technology and Higher Education, Indonesia. He is an associate editor and an editorial member of more than eight ISI journals. He has widely travelled abroad, visiting more than 52 countries to present his research findings.

**NAGESH SHUKLA** is currently a Senior Lecturer in business analytics with the University of Technology Sydney, Ultimo, NSW, Australia. He is working in the area of business data analytics, simulation modeling, and optimization (applied to healthcare and supply chain/logistics management). He has contributed to more than 50 research publications in journals, conferences, patents, book chapters, and research reports. His research interests include development of models that deal with making complex business processes efficient and effective, analytical models for system-level optimization and decision making, and data-driven algorithms for decision making. He is a member of the editorial boards in a number of leading journals.

**ABDULLAH ALAMRI** received the B.S. degree in geology from King Saud University, in 1981, the M.Sc. degree in applied geophysics from the University of South Florida, Tampa, in 1985, and the Ph.D. degree in earthquake seismology from the University of Minnesota, USA, in 1990. He is currently a Professor of earthquake seismology. He is the Director of the Seismic Studies Center, King Saud University (KSU). His research interests include crustal structures and seismic micro zoning of the Arabian peninsula. His recent projects involve applications of EM and MT in deep groundwater exploration of Empty Quarter and geothermal prospecting of volcanic Harrats in the Arabian shield. He has published more than 150 research articles, achieved more than 45 research projects, authored several books, and technical reports. He is a Principal and a Co-Investigator in several national and international projects, including KSU, KACST, NPST, IRIS, CTBTO, U.S. Air Force, NSF, UCSD, LLNL, OSU, PSU, and Max Planck. He is the President of the Saudi Society of Geosciences. He has chaired and co-chaired several SSG, GSF, and RELEMR workshops and forums in the Middle East. He is a member of the Seismological Society of America, the American Geophysical Union, the European Association for Environmental and Engineering Geophysics, the Earthquakes Mitigation in the Eastern Mediterranean Region, the National Communication for Assessment and Mitigation of Earthquake Hazards in Saudi Arabia, and the Mitigation of Natural Hazards Com at Civil Defense. He obtained several worldwide prizes and awards for his scientific excellence and innovation. He is the Editor-in-Chief of the *Arabian Journal of Geosciences (AJGS)*.