applied sciences

MDPI

Review

Application of Technological Solutions in the Fight Against Money Laundering—A Systematic Literature Review

Gleidson Sobreira Leite *, Adriano Bessa Albuquerque and Plácido Rogerio Pinheiro

Department of Computer Science, UNIFOR, University of Fortaleza, Fortaleza 60811-905, Ceará, Brazil; adrianoba@unifor.br (A.B.A.); placido@unifor.br (P.R.P.)
* Correspondence: gleidson.sleite@gmail.com

Received: 10 October 2019; Accepted: 7 November 2019; Published: 10 November 2019

Abstract: With the growing interest in technological solutions aimed at combating money laundering, several studies involving the application of technology have been carried out. However, there were no records of studies aimed at identifying, selecting, rigorously analyzing and synthesizing the literature on solutions that adopt technology to combat money laundering. This paper presents a systematic review of the literature on the application of technological solutions in the fight against money laundering. Seventy-one papers were selected from the 795 studies initially retrieved for data extraction, analysis and synthesis based on predefined inclusion and exclusion criteria. The results obtained with the data analysis made it possible to identify a general categorization of the domains of application of the approaches, as well as a mapping and classification of the support mechanisms adopted. The findings of this review showed that, among the application domain categories identified, the detection of suspicious transactions attracted greater attention from researchers. Regarding the support mechanisms adopted, the application of data mining techniques was used more extensively to detect money laundering. Topics for further research and refinement were also identified, such as the need for a better description of data analysis to provide more convincing evidence to support the benefits presented.

Keywords: data mining; information technology; money laundering; literature review

1. Introduction

Since the mid-1980s, money laundering has been increasingly recognized as a significant global problem with serious economic and social ramifications [1]. In recent years, it has been increasingly present in headlines and various media, as well as the indignation of society that has also been growing through public manifestations or in online media.

Known as the process that transforms crime proceeds into legitimate and consumed assets, money laundering (ML) is systematically used to describe ways in which criminals process illegal or "dirty" money derived from proceeds of any illegal activity by succession of transfers and trades until an illegally acquired source of funds is obscured and money takes over a display of legitimate funds or assets [2].

Money laundering usually involves 3 steps: placing illicit proceeds into the financial system in such a way as to avoid detection by financial institutions and government authorities; layering or the separation of the criminal proceeds from their origin and obscure the audit trail; and integration or the use of apparently legitimate transactions to disguise the illicit proceeds [3].

The United Nations Office on Drugs and Crime (UNODC) estimates that between 2 and 5 percent of gross domestic product (GDP), somewhere between $800 billion and $2 trillion in US dollars, is laundered everywhere. Although the margin between these numbers is huge, even the lowest estimate underscores the seriousness of the problem [4].

Figure 1 presents a geographical map identifying the risk scores of money laundering and terrorist financing (ML / TF) from a study of Reference [5] which covered 125 countries.

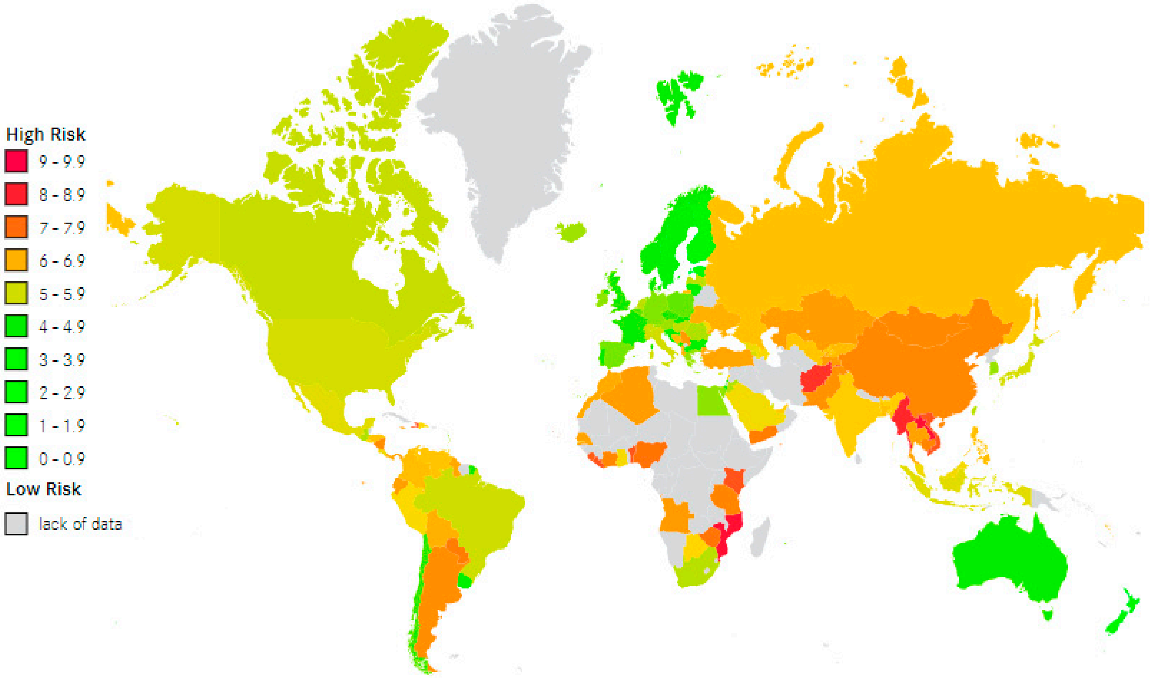

Figure 1. Money Laundering/Terrorist Financing risk scores distribution.

Reference [5] provided risk scores based on data from 15 publicly available sources such as the Financial Action Task Force (FATF), Transparency International, the World Bank and the World Economic Forum. It aggregated the scores into one overall risk score using an expert weighting system also presenting a ranking of the participant countries from highest to lowest level of risk.

Among the obtained results, Reference [5] pointed out that 60% of countries in 2019 (74 of 125) have a risk score of 5.0 or above and can be loosely classified as having a significant risk of ML/TF.

These and several other studies point to concerns about the economic and social expansion and impact of money laundering, where, due to the volume and diversity of existing ML practices, actions to combat them becomes essential in order to minimize the damage caused to society.

Being an emerging topic of great importance, especially due to the negative economic and social impacts caused by occurrences of this crime, money laundering has attracted much attention and concern from institutions and researchers considering the growing need to combat this type of crime.

Despite the existence of several publications by researchers that present different approaches to the use of technology to combat money laundering, however, there were no records of works aimed at identifying, selecting, rigorously analyzing and synthesizing this literature.

Also the large volume of articles and the fact that they are published in dozens of different conferences and journals makes it difficult to discover these works.

To help current and future researchers in the discovery these studies, as well as to identify, select, rigorously analyze and synthesize this literature, a systematic literature review (SLR) was performed.

This work also aims to assist in the understanding of what has been done and discover new directions, as well as have a better understanding of the approaches available, their main objectives, support mechanisms adopted, level of evidence reported, gaps that need further research and to organize the knowledge to support the technological transition.

This paper reports on the design, execution and findings of SLR aimed at systematically identifying, selecting and summarizing a comprehensive set of approaches that adopt information systems or technology to combat money laundering. For this review, 71 relevant papers were identified and rigorously reviewed, summarizing the extracted data in order to answer a set of research questions that motivated this review.

The findings of this review showed that, in the selected studies, the approaches of the technological solutions adopted can be classified into 5 general categories of application domains.

Of the identified categories, the detection of suspicious transactions attracted greater attention from researchers, followed by the pattern/group/anomaly money laundering detection category, which shows in which direction there is a greater tendency for anti-money laundering solutions using information technology.

Regarding the support mechanisms adopted, four main categories were identified, where the application of algorithms or mathematical applications as, for example, the use of data mining or machine learning, were more adopted by researchers.

From the analysis of the research questions adopted in the systematic review, it was found that most of the selected studies did not examine the potential bias of researchers and influence of results. There was also a lack of discussions about the limitations of techniques and tools reported in the reviewed studies.

The two significant contributions of this study to the body of knowledge regarding the use of information technology to combat money laundering are:

- The paper reports on the design, execution and results of a review that systematically identifies a comprehensive set of relevant studies on information technology applications in the fight against money laundering. The study was based on predefined selection criteria, rigorously analyzing and synthesizing the approaches, associated support mechanisms and reported evidence in an easily accessible format.
- The paper structures and classifies the approaches and support mechanisms adopted, as well as the available evidence, using different formats that are expected to be useful to practitioners and researchers concerned. Findings can be used as an evidence-based guide to select appropriate techniques, solutions, approaches or support mechanisms based on the different activities and needs. The findings also identify issues relevant to interested researchers.

Background and Related Work

Information technology plays an important role in combating money laundering and has attracted a lot of attention and concern from researchers and practitioners.

Anti-money laundering solutions may involve applying different approaches such as focusing on suspicious transaction detection, pattern or anomaly detection, visual analysis or even security and control applications (see Section 3.3.1).

Historically many support mechanisms have been proposed, developed and studied, including in the fight against other financial crimes such as fraud detection, as pointed out in Reference [6], which conducted a systematic review of the literature on the application of data mining techniques in detecting financial fraud. In this paper the authors analyzed 49 articles published between 1997 and 2008 classifying them into four categories of financial fraud (bank fraud, insurance fraud, securities and commodities fraud and other related financial fraud) and six classes of data mining techniques (classification, regression, clustering, prediction, outlier detection and visualization).

Among the selected publications, the work showed that the main data mining techniques used to detect financial fraud are logistic models, neural networks, the Bayesian belief network and decision trees. All of which provide primary solutions to the problems inherent in detection and classification of fraudulent data.

Also focused on detecting financial fraud, Reference [7] conducted a survey that categorized, compared and summarized several published technical and review articles on automated fraud detection by applying data mining techniques. The article also formalizes the main types and subtypes of known frauds and presents the nature of evidence from data collected in the affected industries.

Application of statistical methods to combat financial crime was discussed by Reference [8] in their work which aimed to conduct a survey of broad classes of methodologies accompanied by selected illustrative examples, while Reference [9] also conducted a survey of common design approaches in the development of anti-money laundering software by conducting a detailed analysis of anomaly detection, machine learning and neural network techniques.

A survey of the machine learning algorithms and methods applied to detect suspicious transactions focusing on machine learning was conducted by Reference [10], where solutions like anti-money laundering typologies, link analysis, behavior modeling, risk score, anomaly detection and geographical capability were identified and analyzed.

So, over the years, a number of reviews and surveys articles focused on solutions for the combat of financial crimes have appeared in conference or journal publications. However, there were no records of works aimed at systematic reviewing the literature on the application of technical solutions in approaches focused on the fight against money laundering.

Through this systematic literature review, we are interested in finding out what approaches and support mechanisms are available and how they can contribute to the combat of money laundering. The paper is structured as follows—Section 2 describes the systematic literature review method used in this paper and defines the review protocol. Section 3 presents demographic information, quality assessment of included studies and research questions by analyzing selected studies with further discussion of results. Threats to the validity, implications and limitations of research are discussed in Section 4 and, finally, conclusions are presented in Section 5.

2. Research Method

As stated earlier, a Systematic Literature Review (SLR) was performed, which is one of the most widely used research methods in Evidence Based Software Engineering (EBSE). The SLR research method provides a well-defined process for identifying, evaluating and interpreting all available evidence relevant to a specific research question or topic [11].

An SLR evaluates existing studies on a specific phenomenon in a fair and credible manner. For this review, we follow the guidelines of Reference [11] which involve three main phases: defining a review protocol, conducting the review and reporting the review. The review protocol adopted consists of the following elements—(i) research questions, (ii) search strategy, (iii) inclusion and exclusion criteria, (iv) study selection, (v) evaluation of study quality and (vi) data extraction and synthesis. These steps are discussed later in the following subsections.

2.1. Research Questions

This SLR was intended to summarize and provide an overview of current research on "which approaches that adopted information systems or technology to the combat of money laundering were reported in the peer-reviewed literature?" To achieve this goal, a set of research questions (RQs) were formulated to be answered through this SLR. Table 1 presents the research questions and the motivations for their constitution.

The answers to these research questions can provide a systematic insight, being beneficial for researchers to identify missing gaps in this area, as well as for the use of approaches and support mechanisms synthesized in SLR by practitioners. The questions may be directly linked to the objectives of this SLR—an understanding of approaches that adopt information systems and/or technology to combat money laundering (RQ1), identification of application domains of identified approaches (RQ2), identification of support mechanisms adopted (RQ3), level of evidence reported for each of the studies (RQ4) and applied contexts (RQ5).

Table 1. Research questions of the systematic literature review (SLR).

Research Question	Motivation
RQ1: What approaches have been suggested or used to combat money laundering that adopt information systems and/or information technology solutions?	The purpose of this question is to identify which anti-money laundering approaches are present in the literature and which use information systems and/or information technology solutions.
RQ2: What are the different application domains of the identified approaches?	This question seeks to identify the application domains or purposes of the approaches, as well as the frequency of application. This information can help practitioners and researchers identify the application domains that have gained the most interest in combating money laundering.
RQ3: What types of support mechanisms are part and/or have been suggested or applied?	What tools, techniques, systems, standards, among other mechanisms have been proposed or used to support or achieve the objectives of the approaches? This information can assist researchers and practitioners in identifying trends in the use of money laundering solutions, techniques, tools and other mechanisms.
RQ4: How much evidence is available to support the adoption of anti-money laundering approaches?	The purpose of this question is to gain knowledge of the maturity of the proposed approaches. This research question is of interest to practitioners and researchers when they want to further adopt or evaluate existing approaches. Maturity is measured based on the level of evidence as described in Section 2.4.
RQ5: What are the contexts addressed?	The intent of this question is to identify in what context the study was applied, that is, if it was an experiment in the academy or if the validation or evaluation was performed in any organization/institution or with actual data from it. If the work describes validations in both contexts, the industrial context will be considered for the purpose of work evaluation.

2.2. Search Strategy

The search strategy is essential to allow relevant studies to be included in search results to help researchers get as many as possible [11]. In this SLR we sought to conduct the research using various combinations of derivative terms related to the subject of the study. The search strategy used was composed by the following elements: search method, search items and data sources.

2.2.1. Search Method

The search strategy adopted automatic searches on electronic database engines or digital libraries listed in Table 2 using the search terms mentioned in Section 2.2.2.

Table 2. Electronic databases for the automatic search included in the SLR.

Electronic Database	Search Terms are Matched With	Web Address	Publications Found
IEEE Xplore Digital Library	Paper title, keywords, abstract	http://ieeexplore.ieee.org	76
ACM Digital Library	Paper title, keywords	http://dl.acm.org	77
El Compendex	Paper title, keywords, abstract	www.engineeringvillage.com	194
Elsevier Scopus	Paper title, keywords, abstract	http://www.scopus.com	448

2.2.2. Search Terms

Search terms are used to match paper titles, keywords and abstracts in electronic data sources during automatic search. The exceptional case is ACM, where search terms are matched only to titles and paper keywords, as these databases return an excessively large number of articles by including abstracts. According to the guidelines provided in Reference [11], the following strategies were used to form the most relevant search terms for automatic search:

- Derive key terms from research questions and study topics;
- Identify synonyms, plurals and related terms;
- Use the logical operator "OR" to incorporate synonyms;
- Use the logical operator "AND" to concatenate the parameters;
- Check terms in article titles, abstracts and keywords;

The resulting search terms are composed of the synonyms and terms related to "money laundering" AND "technology" AND "approach." The following terms were used—

> (money laundry OR money laundering OR anti money laundering OR fight money laundering OR fight against money laundering OR combating money laundering OR money laundering prevention) AND (technology OR information technology OR information system OR system) AND (approach OR process OR model OR method OR framework).

It should be added that the terms "system," "process," "model" and "method" were also added since the results of the inclusion of these terms are also of interest to the research.

2.2.3. Data Sources

The electronic databases selected for the research are presented in Table 2 and sorted by consulted order including publications found in each database. They were selected considering the ease of access, possibility of retrieving the full text of the articles, to be used for indexing journals and conference proceedings, as well as being cited by References [11,12] as relevant sources.

Table A1 presents the mapping of the selected studies identifying in which of the selected databases the publications were retrieved after the search strings were executed.

In order to allow a broader scope of the research, there was no limitation for the period of publication of the papers and English was selected as the language considered being standard of most international journals and international.

In addition, the GOOGLE SCHOLAR data source has not been included because of the high possibility of inaccurate results return generating many irrelevant results and because of the considerable overlap with ACM Digital Library and IEEE Xplore Digital Library in the software engineering literature [12].

2.3. Inclusion and Exclusion Criteria

In order to enable only studies that met the objectives of the systematic review to be analyzed, inclusion and exclusion criteria were adopted in all studies returned from the database searches in order to select relevant primary studies to answer the research questions. Table 3 presents the inclusion and exclusion criteria adopted.

Table 3. Inclusion and exclusion criteria of the SLR.

	Inclusion Criteria
I1	Money laundering related work addressing the use of information technology and/or information systems.
	Exclusion Criteria
E1	Duplicate publications (even with different references).
E2	Standards, models, industry standards.
E3	Editorials, position papers, keynotes, reviews, summaries tutorials, books, courses or workshops, panel discussions.
E4	Non-scientific publications
E5	Publications that do not meet the inclusion criteria

2.4. Study Selection and Data Extraction

The selection process was divided into three stages. In the first one, the digital libraries were selected, the search expression was executed in each electronic database and all the returned works were compiled forming a set of 795 publications found. The number of studies selected at each stage is shown in Figure 2.

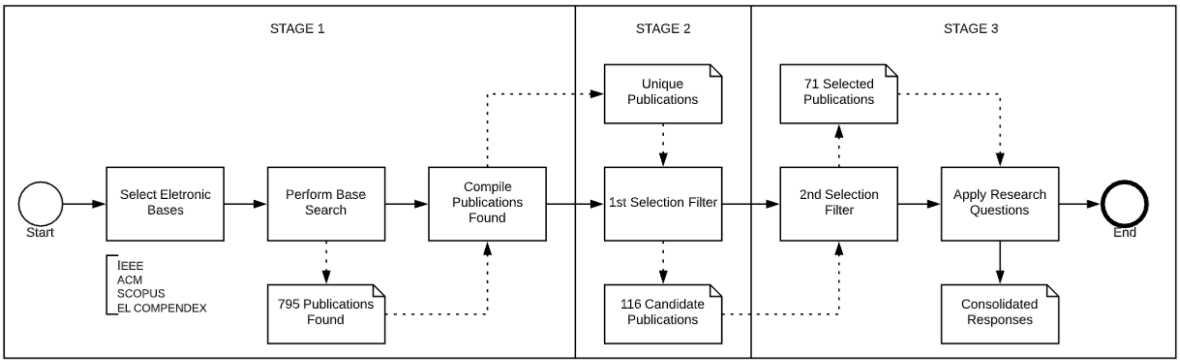

Figure 2. Stages of the search process and number of selected studies.

In the second stage, duplicate records and those that do not correspond to scientific publications were discarded. In addition, we also performed a filter reading of the title, keywords and abstract of each article in which an analysis was made according to the inclusion and exclusion criteria resulting in a list of 116 candidate publications.

Finally, in the third stage, after all the papers were downloaded, they were read in their entirety and analyzed again using inclusion and exclusion criteria, corresponding to the second selection filter that resulted in a final selection of 71 studies. At the end of this stage, the research questions were applied in each of the studies and finally, data were extracted based on the items presented in Table 4 recording the answers (see results and discussions in Section 3).

Table 4. Items extracted from each study, related research questions and quality criteria.

Objective	Data Item	Objective	Data Item
General data	Title Author(s) Year of publication Venue Paper Summary	RQ5 Q1 Q2 Q3 Q4	Context Study Objectives Context Description Research Project description Data analysis
RQ1	Approach Used	Q5	Presentation of conclusions
RQ2	Application domain	Q6	Critical analysis
RQ3	Support Mechanisms	Q7	Credibility and limitations
RQ4	Evidence level		

The search expression was executed in the digital libraries in June 2019. Publication selection filters (filter 1: title, abstract and keywords reading of each paper returned by the initial search; and filter 2: Full text reading of the candidate publications) were used by a researcher to record the reasons for the inclusion and exclusion decision of each study that were used in subsequent decision-making discussions.

The selected publications were presented to another two researchers, who agreed with the selection, where the papers were later classified (for cases of divergence of selections and classifications, discussions were held to ensure the inclusion of papers relevant to this study).

Table 4 contains descriptions of the items used in the study and were selected for the purpose of documenting the work, meeting the research questions and evaluating the quality of the studies. The referenced quality criteria are described in Section 3.2 and the levels of evidence, the results of which help researchers to evaluate the maturity of a technique, are listed in Table 5.

Table 5. Levels.

Level	Classification	Description
0	Without evidence	No evidence of validation or evaluation.
1	Demonstration or usage example	The authors describe an application and provide an example to aid in its description.
2	Expert Notes	Some textual, qualitative assessments or opinions are provided. For example, it compares and contrasts the advantages and disadvantages.
3	Laboratory experiment	The result is obtained from simulations with artificial data used in real experiments. Evidence is collected informally or formally.
4	Empirical Investigation	Investigate the behavior of the proposed approach within a real context.
5	Strict analysis	Use of a more formal methodology to evaluate and validate the study. For example, defining questions and variables to be analyzed while applying the approach.

Based on the work done by Reference [13], Table 5 lists ways in which a method can be validated or evaluated and different degrees of accuracy are assigned to each form. This classification was used to identify the evidence level of the solutions described in the selected publications.

3. Results and Discussions

In the following subsections, we present the results and discussions of the synthesis and analysis of data extracted from primary studies to answer the research questions. Most of the results presented in this section are based on the systematization of data collected directly from the reviewed studies. Interpretations of the results by the authors of this SLR have been limited to a minimum in order to primarily focus on what has been reported in the revised primary studies. However, some of the revised primary studies may not have provided sufficient information to solidly answer the RQs, so interpretations and inferences to some extent were unavoidable. In these situations, attempts have been made to examine other available resources on the revised studies (e.g., the authors' home page and other online available information on approaches) to make interpretations and inferences as reliable as possible in this type of effort.

3.1. Demografic Data

Before reporting the results of the synthesis and analysis of relevant data extracted from the studies included in this SLR, Section "Publication Venues and Citation Count" presents the demographic information on the included studies: places of publication and status of citations. All included studies are listed in Table A2 (Appendix A).

Publication Venues and Citation Count

Attempts to identify the types and places of publication of a specific topic/theme may be potentially useful for researchers who may be interested in conducting research on a relevant topic. That is why in one of the silent reporting elements of an SLR is demographic information about the documents included in the SLR. Table 6 shows how the 71 primary studies are distributed in 65 publication venues.

Table 6. Distribution of the selected studies on publication venues.

Publication Venue	#	%	Publication Venue	#	%	Publication Venue	#	%
ESWA	2	308	eCRS	1	154	IJCAA	1	154
FedCSIS	2	308	EIConRus	1	154	IJCNA	1	154
ICMLC	2	308	EIDWT	1	154	IJMCMC	1	154
IJET	2	308	EMCIS	1	154	IS	1	154
WCIT	2	308	ETCS	1	154	ISAT	1	154
WiCOM	2	308	FiCLOUDW	1	154	JATIT	1	154
ACIIDS	1	154	FSKD	1	154	JDM	1	154
AIP	1	154	GCCCE	1	154	JEAS	1	154
AJAS	1	154	GLOBECOM	1	154	JFC	1	154
AMACLSD	1	154	HICSS	1	154	JOMLC	1	154
APSCC	1	154	HST	1	154	MEDIACOM	1	154
APVIS	1	154	ICACC	1	154	RIDE	1	154
ARES	1	154	ICDMW	1	154	RISK	1	154
CBD	1	154	ICMLA	1	154	RISTI	1	154
CCDC	1	154	ICNSC	1	154	SIEDS	1	154
CICN	1	154	ICOS	1	154	SIN	1	154
CODS-COMAD	1	154	ICS	1	154	SSCC	1	154
CORE	1	154	ICSEMA	1	154	STIDS	1	154
CyberC	1	154	ICSESS	1	154	UEMCON	1	154
DI	1	154	ICWAPR	1	154	VAST	1	154
DSS	1	154	IEEE Access	1	154	VINCI	1	154
DTGS	1	154	IJCA	1	154			

Citation information may partially show the quality of the reported study and also the maturity of the techniques proposed. It can also show the impact of a study on the revised topic. Table 7 provides an overview of the citation count of the included studies, sorted by citation count in descending order. These numbers were obtained from Google Scholar on 4 September 2019.

Table 7. An overview of citation counts of the selected studies.

Studies ID	Citation Counts	Studies ID	Citation Counts	Studies ID	Citation Counts
[S71]	123	[S1]	11	S21	2
[S25]	72	[S12]	11	S43	2
[S32]	53	[S48]	10	S44	2
[S65]	50	[S23]	9	S46	2
[S5]	41	[S38]	9	S66	2
[S69]	40	[S27]	7	S15	1
[S9]	33	[S29]	7	S19	1
[S64]	31	[S36]	7	S30	1
[S11]	30	[S42]	6	[S31]	1
[S28]	30	[S2]	5	[S40]	1
[S61]	30	[S33]	5	[S54]	1
[S41]	25	[S37]	5	[S58]	1
[S13]	23	[S59]	5	[S6]	1
[S4]	23	[S60]	5	[S17]	0
[S56]	22	[S70]	5	[S18]	0
[S3]	20	[S16]	4	[S34]	0
[S63]	20	[S45]	4	[S35]	0
[S22]	18	[S26]	3	[S39]	0
[S10]	16	[S47]	3	[S50]	0
[S55]	16	[S49]	3	[S53]	0
[S52]	14	[S51]	3	[S57]	0
[S62]	13	[S68]	3	[S67]	0
[S20]	12	[S7]	3	[S8]	0
[S24]	12	[S14]	2		

From the ordered list presented in Table 7 it is possible to identify the studies that received the highest quantity of mentions by citations. Among the first 11 studies that got the most interest, analyzing the application domain categories table presented in Section 3.3.1., which presents the mapping of the studies by categories of application domain, it is possible to identify that 4 of the studies ([S32], [S9], [S64] and [S61]) adopted approaches, the technological solutions of which focused on suspicious transaction detection (CD1).

Regarding the studies that adopted approaches focusing on the detection of money laundering patterns/groups/anomalies (CD2), 2 studies ([S65] and [S28]) were identified among the first 11 studies that obtained the most interest.

With regard to risk analysis/assessment (CD3) and visual analysis or applications of visual techniques (CD5), 4 studies adopted approaches focusing on these categories where 2 studies ([S5] and [S69]) focused on CD3 and two other studies ([S71] and [S11]) on CD5. Study [S25] adopted the approach focusing on the application of security, control and governance techniques.

It should also be added that, analyzing the support mechanisms table presented in Section 3.3.2., which presents the mapping of the studies by categories of support mechanisms adopted, all 11 studies that were of greater interest adopted data mining techniques as a support mechanism.

Figure 3 presents the number of published studies selected per year, where it can be noted that, with the exception of 1997 there are studies published from 2005 in which 50.7% of the studies were published in the last 6 years, which means the subject has gained increasing interest and attention.

Table 8 presents the distribution of studies according to the country of the institution reference of the author and the domain application categories presented in Section 3.3.2 sorted by number of studies in descending order. China, India, Russia, Poland and the United States were the countries where the largest number of selected studies were concentrated, totaling 45 (63.38%) of the studies.

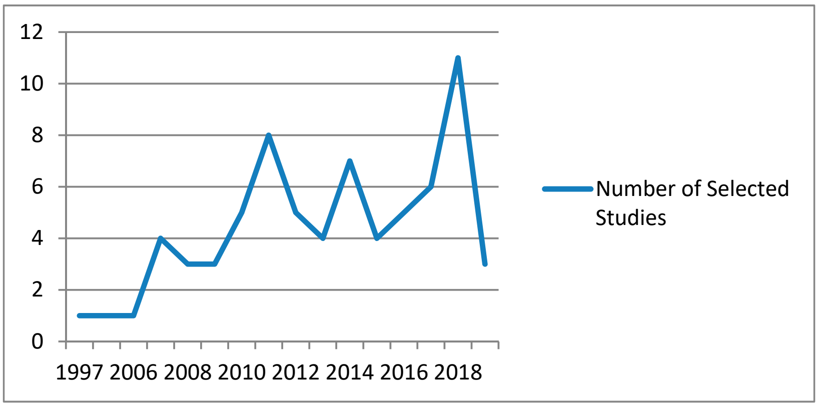

Figure 3. Number of selected studies published per year.

Table 8. Study distribution by countries and application domain categories.

Countries/Categories	CD1	CD2	CD3	CD4	CD5
China (20)	[S9], [S10], [S12], [S13], [S16], [S27], [S32], [S44], [S54], [S58], [S59], [S61], [S62]	[S23], [S33], [S36], [S43]	[S5], [S60]		[S57]
India (8)	[S14], [S31], [S34], [S48], [S50]	[S39], [S46], [S49]			
Russia (7)	[S17], [S18], [S19], [S30], [S53]	[S2]			[S45]
Poland (5)	[S41], [S47], [S64]	[S65]			[S70]
United States (5)		[S42], [S56]	[S68]	[S67]	[S71]
Pakistan (3)	[S1], [S22], [S63]				
United Kingdom (3)	[S24]			[S4], [S38]	
Egypt (3)	[S15], [S29]	[S26]			
Australia (2)				[S25], [S55]	
Italy (2)			[S69]		[S66]
Spain (1)				[S3]	
Portugal (1)	[S6]				
Canada (1)		[S7]			
Iran (1)			[S8]		
Italy (1)					[S11]
Vietnam (1)		[S20]			
Iraq (1)		[S21]			
Brazil (1)		[S28]			
Turkey (1)			[S35]		
Malaysia (1)	[S37]				
Luxembourg (1)	[S40]				
Ireland (1)	[S51]				
Germany (1)	[S52]				

3.2. Study Quality Assessment

The 71 primary studies were evaluated by the authors against a set of questions on quality assessment of the studies listed in Table 9 and adopted and adjusted from [14]. Unlike the study quality assessment described in Reference [11], these questions were not used for study selection but to validate the results of the selected studies. Each question can be answered according to a ratio scale: "Yes," "No" and "Partially" during the data extraction process (see Section 2.4). Responses for each study show the quality of the study selected and the credibility of the study results. The outcome of the quality assessment of the included studies may reveal the potential limitations of current research and guide future field research [11,14].

Table 9. Study quality assessment questions.

ID	Study Quality Assessment Question	Yes	Partially	No
Q1	Are the aims and objectives of the study clearly specified?	59 (83.1%)	12 (16.9%)	0 (0%)
Q2	Is the context of the study clearly stated?	7 (9.9%)	34 (47.9%)	30 (42.3%)
Q3	Does the research design support the aims of the study?	8 (11.3%)	36 (50.7%)	27 (38.0%)
Q4	Has the study an adequate description of the data analysis?	8 (11.3%)	23 (32.4%)	40 (56.3%)
Q5	Is there a clear statement of findings and was sufficient data provided to support them?	17 (23.9%)	36 (50.7%)	18 (24.4%)
Q6	Do the researchers critically examine their potential bias and influence to the study?	2 (2.8%)	9 (12.7%)	60 (84.5%)
Q7	Are the limitations of the study discussed explicitly?	3 (4.2%)	14 (19.7%)	54 (76.1%)

As shown in Table 9, all studies set the objectives of the research performed (Q1) and more than half of the papers had an adequate description of the context (Q2), for example, details about the nature of the organization, type of organization, software type and level of experience of the team, as well as providing the research design to achieve the objectives (Q3), presenting clear conclusions with enough data to support them (Q5). However, about data analysis (Q4), more than half of the analyzed studies did not provide an adequate description. For the analysis of potential bias and influence in the study (Q6), as well as discussions of limitations (Q7), a lack of most studies was noted.

3.3. *Question Analysis*

The following sections present the analysis and discussion of the research questions.

3.3.1. Approaches and Application Domains (RQ1 e RQ2)

For each selected work, the adopted approaches were identified, descriptions are presented in Table A2 and their respective purposes/domains of application grouped into 5 main categories. Table 10 presents the categories identified in the selected studies.

Table 10. Application domain categories.

Category	Studies
CD1: Suspicious transaction detection	[S1], [S6], [S9], [S10], [S12], [S13], [S14], [S15], [S16], [S17], [S18], [S19], [S22], [S24], [S27], [S29], [S30], [S31], [S32], [S34], [S37], [S40], [S41], [S44], [S47], [S48], [S50], [S51], [S52], [S53], [S54], [S58], [S59], [S61], [S62], [S63], [S64]
CD2: Pattern detection/groups/money laundering anomalies	[S2], [S7], [S20], [S21], [S23], [S26], [S28], [S33], [S36], [S39], [S42], [S43], [S46], [S49], [S56], [S65]
CD3: Risk Assessment/Analysis	[S5], [S8], [S35], [S60], [S68], [S69]
CD4: Security, control, structuring and/or governance applications	[S3], [S4], [S25], [S38], [S55], [S67]
CD5: Visual Analysis/Applications of Visual Techniques	[S11], [S45], [S57], [S66], [S70], [S71]

Below are the category descriptions:

- Suspicious Transaction Detection (CD1): Category that covers approaches that seek to identify suspicious transactions by applying different methodologies or techniques.
- Money Laundering Pattern/Group/Anomaly Detection (CD2): A category that covers approaches that act by detecting and/or classifying patterns or performing money laundering-focused clusters.
- Risk Assessment/Analysis (CD3): Covers approaches that apply money laundering risk rating techniques by conducting assessments or analyzes.

- Security, control, structuring and/or governance applications (CD4): Covers approaches that apply governance, security, structuring or control techniques focused on money laundering.
- Visual Analysis/Applications of Visual Techniques (CD5): Category of approaches involving applications of techniques, methodologies or visual systems focused on money laundering.

Of the selected works, we can highlight that 52.1% (37 publications) have as their main focus the detection of suspicious transactions through the application of different methodologies or techniques, such as machine learning techniques, classification, clustering and others. That is, it is clear that it is an application domain with higher trends of studies by researchers compared to other application domains.

16 of the papers focus on the detection of money laundering patterns/groups/anomalies, where they act by detecting and / or classifying patterns (e.g., behavioral patterns, anomalies) or grouping (e.g., grouping transactions with similar attributes or behaviors or based on social networks, grouping of individuals or participants by behavior or roles) focused on money laundering.

With regard to risk analysis and assessment, 6 of the papers have this application domain as their main focus, applying money laundering risk rating techniques, performing analyzes as risk classification systems (risk-score) and others.

About the CD4 category, 6 papers apply governance, security, structuring (e.g., systems and environment, fragmented data) or control (e.g., preventive controls) techniques focused on money laundering. Finally, 6 of the selected studies fell into the category of visual analysis or applications of visual techniques.

Figure 4 presents the number of studies published per year, quantifying by category, where it is possible to notice that there are studies of category CD1 from 2005 to 2019 which shows a tendency of studies that apply approaches that seek to identify suspicions transactions.

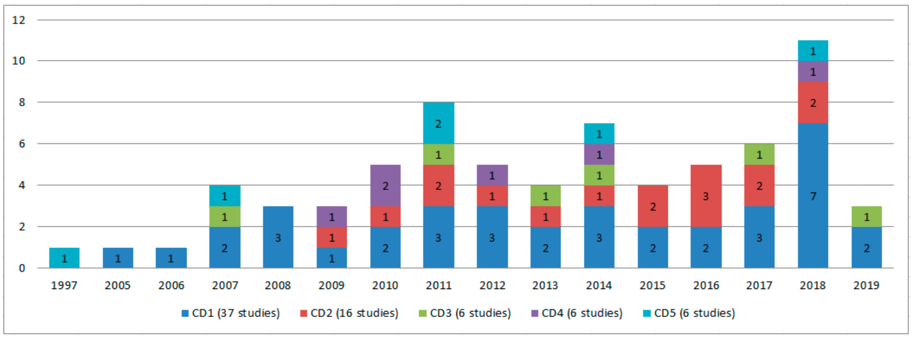

Figure 4. Quantitative distribution of studies by application domain category over time period.

It should be added that the approaches were classified into categories with greater prominence within the study but some works fell into more than one category, such as [S8] in which despite being in the CD3 category for presenting an intelligent method for money laundering risk estimation, also makes it possible to track and recognize suspicious transactions. [S69] is another example that, while adopting visual analysis and techniques, focuses on analyzing and assessing risks and is categorized on CD3 (other examples involve work that applies pattern or group detection but focuses on suspicious transaction detection).

3.3.2. Support Mechanisms (RQ3)

Once the main application domains of the approaches adopted in the selected studies were identified; another important step would be to identify and categorize the support mechanisms proposed or used to support or achieve the objectives of the approaches.

Table 11 presents the mapping of the support mechanisms identified in the selected studies, grouping them into categories and subcategories.

Table 11. Mechanisms.

Support Mechanism Categories	**Techniques/Mechanism**		**Studies**
C1: Systems/Software/ Tools/Programming Languages	Malware Analysis		[S3]
	Mainframe, SOA		[S16]
	Big Data		[S19]
	Forensic Practices		[S24]
	Semantic Web, Data models, Functional programming, Data processing, Formal languages		[S67]
	Others		[S5], [S6], [S7], [S8], [S14], [S15], [S21], [S25], [S28], [S42], [S43], [S45], [S47], [S50], [S51], [S53]
C2: Hardware's	Others		[S16], [S21], [S66]
C3: Patterns/Theories/Frameworks	COBIT-COSO		[S4]
	Decision making theory, Multi-agent, Cognitive Approach		[S44]
	Structural Coupling (System Theory)		[S38]
	Predictive Security Analysis		[S52]
	Semi-Markov Decision, Process (SMDP), Resource Allocation, Maximal Rewards		[S54]
	Simon's decision-making/problem-solving process theory, Cynefin sense-making framework, Multi-agent		[S55]
	Hierarchical Model Algorithms, Multi-attribute Evaluation, Entropy-weight Method		[S57]
	Risk Analysis, Link Analysis, Behavior Profiling		[S60]
C4: Algorithms/Mathematical Application (data mining and machine learning)	**Application Class**	**Technique**	**Studies**
	Classification	Decision Trees	[S5]
		Bayesian Network	[S1]
		Sequential Patter, Analysis, Affiliation Mapping	[S14]
		Machine Learning, SVM (support vector machine), Random Forest, Logical Regression	[S17], [S18]
		Neural Networks, Network Analysis	[S26], [S28], [S30], [S35]
		Behavioral Patter, Separation (BPS)	[S46]
		Natural Language Processing, Sentiment Analysis, Link Analysis, Fuzzy Logic, Neural Network	[S51]
		Privacy-Preserving, Decision tree	[S59]
		Euclidean distance sequence matching	[S61]
		Multi-agent, Neural Network, Genetic Algorithms, Velocity Analysis, Fuzzy Logic, Case-based Reasoning	[S62]
		Patter Recognition, Sequence Matching, Case-based Analysis, Network Analysis, Complex Event Processing	[S68]
	Regression	Logistic model	[S42]
	Outlier Detection/Approximation	Outlier Point Analysis, Statistic Pattern Recognition, Machine Learning	[S10], [S12], [S13]
		Rule-based Bayesian Classification algorithm	[S31]
		Support Vector Machine	[S32]
		RRS, FastVOA, LOF	[S39]
		Isolation Forest (IF), One Class SVM, Gaussian Mixture Models	[S40]
		Forensic Analysis, Rule based Dempster Shafer Theory of Evidence	[S50]
	Clustering	K-Means	[S6], [S22], [S23]
		Decision Tree, K-Means, BIRCH	[S56]
		Structural Similarity	[S7]
		Neural Networks, Fuzzy Logic	[S2], [S8], [S25], [S41]
		Affinity Propagation Clustering (APC)	[S9]
		Network/Link analysis, Visualization	[S15], [S21], [S29], [S36], [S53], [S69], [S71]
		CLOPE Algorithm	[S20]
		Network/Link analysis, DBSCAN	[S27]
		K-Cores, Network/Link analysis, Visualization	[S11]
		Hidden Model Markov, Genetic Algorithm	[S33]
		Hash-based algorithm, Link analysis	[S34]
		Expectation Maximization	[S37]
		Louvain algorithm	[S43]
		OntologyNetwork Analysis	[S47]
		Probabilistic Relational Model, Association Mapping, Audit Sequential Patter	[S49]
		K-Means, Frequent Pattern, Visualization, Sequence Miner, BI-Directional Extension checkin-BIDE	[S48]
		Distributed Association Rule Analysis	[S58]
		Bayesian Network	[S63]
		Frequent Pattern, Network Analysis, Visualization	[S64], [S65]
		Neural Patter Recognition, Visualization	[S66]
	Visualization	RadViz, Heat Map, Graphs	[S45]
		Heuristics Evolutionary Algorithm	[S70]

After analyzing the selected studies, 4 general categories were identified and were used to group the identified support mechanisms. For categories C1, C2 and C3 a set of techniques/mechanisms applied were identified. In the case of category C1 despite the use of systems, software, among others, a set of techniques or auxiliary mechanisms were also adopted. The exception is for those studies grouped into the "Others" subcategory that was used to identify studies that adopted a set of market or developed solutions to achieve the study objectives. The same nomenclature was used in category C2 to identify studies that adopted a set of hardware market solutions.

Solutions that adopted standards, theories and frameworks (C3) were grouped by the identified support mechanism (8 studies). The category C4 was the one that grouped the largest amount of work (58 of 71 studies), where it is possible to perceive a greater tendency to apply data mining techniques to combat money laundering. The techniques identified in the selected studies were grouped by class based on the classification framework proposed by Reference [7].

It should be added that some studies were included in more than one category because they adopted different support mechanisms in their approach. For example, studies with subcategory "Others" in categories C1 and C2 (with exception of the study [S16], which is presented only in categories C1 and C2) are also present in category C4.

Figure 5 presents the quantitative distribution of the selected studies by category of support mechanism where, for the case of category C4 the studies were distributed into subcategories that grouped the studies into the identified application classes. Of the 58 studies grouped in category C4, 32 used clustering techniques in their approaches, which show a greater tendency in their adoption compared to other studies.

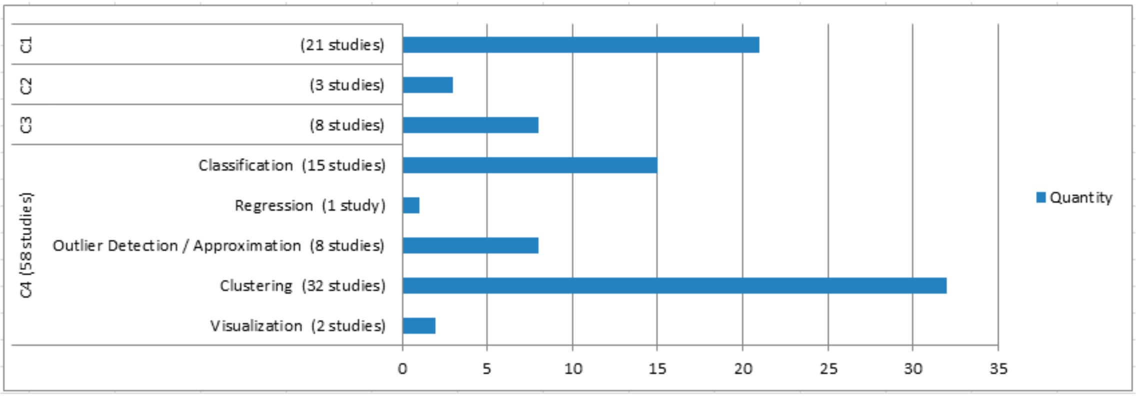

Figure 5. Quantitative distribution of studies by support mechanism category and application class.

3.3.3. Available Evidence and Context (RQ4 e RQ5)

Table 12 presents the distribution of studies according to the levels of evidence described in Table 5 also grouping by the context of application of the studies (academic or industrial). Data extraction was performed based on the items in the form presented in Table 4 to answer questions RQ4 and RQ5 in order to investigate the maturity of the selected studies.

Based on the distribution presented, it can be seen that most of the selected studies presented some evidence, except for only 10 studies. Among the selected papers, 12 works performed only demonstrations (application descriptions) or examples of use in which 11 were in the academic context and only 1 in the institutional context.

Considering experiments in laboratories, 28 studies used artificial data in real experiments, in which 23 were in academic context and 5 in institutional context. It should be added that there were no papers that provided expert observations such as textual, qualitative or opinion evaluations.

Table 12. Evidence and context.

Evidence Level	Context	
	Academic	Industrial
0: Without evidence	[S2], [S12], [S16], [S21], [S47], [S56], [S60], [S62], [S66], [S67]	X
1: Demonstration or usage example	[S4], [S8], [S17], [S18], [S19], [S24], [S29], [S30], [S51], [S53], [S55]	[S25]
2: Expert Notes	X	X
3: Laboratory experiment	[S3], [S5], [S7], [S9], [S11], [S34], [S35], [S39], [S41], [S42], [S43], [S44], [S45], [S46], [S48], [S49], [S52], [S54], [S57], [S58], [S59], [S64], [S65]	[S10], [S20], [S26], [S27], [S33]
4: Empirical Investigation	X	[S1], [S6], [S13], [S14], [S28], [S31], [S32], [S36], [S37], [S38], [S40], [S50], [S61], [S63], [S68], [S70], [S71]
5: Strict analysis	X	[S15], [S22], [S23], [S69]

For empirical investigations that act on the behavior of approaches within real contexts, 17 works were identified in which, because the context is real, were applied in institutional contexts only. Finally, four studies that performed more rigorous analysis/methodologies of evaluation or validation were identified, all in institutional context.

In general, we can see that there was a lower tendency for works to be explored in industrial contexts (only 27 studies), although in this study industrial context approaches were also considered, which used industrial data (with appropriate adaptations) and were not necessarily applied within an institution.

Possible reasons may be that it is difficult to find motivated industry participants to conduct experiments, as well as the fact that conducting controlled experiments requires an excessive amount of effort and resources mainly because much of the information used is classified.

4. Research Implications and Limitations

When performing automatic searches in digital libraries, one of the main objectives is to ensure the completeness of the selected studies. As mentioned earlier, a comprehensive search was performed using synonym terms related to the subject matter of the search. This helped to ensure that the data returned by the search expression had several relevant studies. However, the number of papers initially returned could be a problem but in the research development phase, the application of exclusion criteria at 2 different stages allowed studies that were not related to the research objectives to be removed.

This systematic literature review has two main threats to validity—possible bias in the selection of studies and possible bias in data extraction where, because they are considerably subjective, researcher's bias may affect the results of this review.

To enhance bias reduction in study selection, the review protocol was developed and validated as follows: initially the protocol was defined by a researcher and validated by another two researchers with extensive experience and practice in the field of software engineering and systematic literature review. After protocol completion it was strictly followed.

To minimize the effect of possible bias by researchers on study selection, the selection process was conducted in 3 phases (see Section 2.4) to reduce the chances of exclusion of relevant studies. One researcher performed the study selection process and the two other researchers examined all included and excluded studies (inclusion and exclusion reasons were recorded and disagreements were resolved through discussions).

Still in order to reduce bias in the selection of studies, only automatic searches using keywords in digital libraries were performed, where the search terms were iteratively improved based on evaluation searches and were carefully tested before executing the review.

To reduce the threat of data extraction inaccuracies, a data extraction form has been created (see Table 4) to consistently extract and analyze the data needed to answer the research questions of this systematic literature review.

To enable bias reduction, the data extraction process was conducted by two researchers who performed the extraction and verification of the selected works (all disagreements were resolved through discussions) and the results were validated by a third researcher.

In the data extraction process, both researchers performed the complete reading of the selected studies answering the research questions (RQ1–RQ5) and the quality criteria (Q1–Q7) according to Table 4. All extracted information was recorded and a comparative analysis of the information extracted from each study was performed. Similar observations and conclusions were unified with appropriate additions and, for disagreements, they were resolved through discussions.

At the end of the process, the third researcher validated the results by acting as the final decision-maker for discussions where no agreement decision was made.

Analyzing the quality of studies has also contributed to increased accuracy and precision of data extraction results, as it gives more credibility to the fact that the data extracted comes from reliable studies.

This study has two major limitations. First, the limited number of sources searched (only four sources were selected) and second, the fact that only automatic search was performed, in which the use of keywords does not encompass all studies that use information technology aimed at combating money laundering for the following reasons:

- The keywords searched may not all be explicit in the search places such as in the title, keywords or abstract.
- Relevant works may not be found because the String search may not contain the full set of keywords required because of their variety.

Finally, it should be added that, although the guidelines suggested by Reference [11] were used for this systematic review, there was a deviation from the suggested procedures. Instead of a group of researchers, only 3 researchers extracted the data in this research. Although the practice of analysis by only one researcher is adopted in some studies, it is possible that some collected data may have some description or classification questioned even with the triple validation in this study.

5. Conclusions

There has been a growing interest in technological approaches and solutions aimed at combating money laundering. Due to the importance of the theme and its social impact, it is equally important to systematically analyze and document the approaches, methodologies, methods and support mechanisms adopted to help understand its nature and potential application areas, as well as to identify the direction areas of future research.

This study was motivated to contribute to the aforementioned needs that were described as key research questions aiming to meet the objectives of this review.

This paper aimed to report the design, execution and results of a systematic literature review, in which a systematic selection and rigorous analysis of a comprehensive set of approaches was performed. The objective was to provide evidence-based knowledge of the current state of combat money laundering through the use of information technology and areas of potential research.

The paper presented a structure and classification of the approaches and support mechanisms adopted for the use of technology to combat money laundering, as well as the available evidence, using different formats that are expected to be useful to practitioners and researchers concerned. The findings may be used as an evidence-based guide to selecting appropriate techniques, solutions, approaches or support mechanisms based on the appropriateness needed for different stakeholder activities and needs. The findings also identified issues relevant to interested researchers.

The result of this study showed that the approaches presented in the selected studies can be classified into 5 general categories of application domains, in which, of the presented categories, the detection of suspicious transactions through the application of different methodologies or techniques attracted more attention from the researchers, followed by the pattern/group/anomaly/money laundering detection category, which shows in which direction there is a greater tendency for anti-money laundering solutions using information technology.

Regarding the support mechanisms adopted, it was found that there was a greater tendency to apply data mining techniques in relation to the other mechanisms.

From the analysis of the research questions used, it was found that most of the selected studies did not examine the potential bias of researchers and influence of results, as well as there was a lack of discussions about the limitations of techniques and tools reported in the reviewed studies.

While it cannot be said that the study is exhaustive, it is believed to be a useful resource for anyone interested in anti-money laundering research using information technology and will help stimulate new interests in the field.

Future work recommends expanding the scope of this review by including manual searches through snowball techniques in the references of the studies selected in this review, as well as in relevant journals and conferences.

Author Contributions: Conceptualization, G.S.L. and A.B.A.; methodology, G.S.L., A.B.A. and P.R.P.; formal analysis, G.S.L., A.B.A. and P.R.P.; investigation, G.S.L., A.B.A. and P.R.P.; writing—original draft preparation, G.S.L. and A.B.A.; writing—review and editing, G.S.L., A.B.A. and P.R.P.; visualization, G.S.L. and A.B.A.; supervision, A.B.A. and P.R.P.; project administration, G.S.L., A.B.A. and P.R.P.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

See Tables A1 and A2.

Table A1. Mapping of selected studies returned by selected databases.

ID	ACM	IEEE	Scopus	Compendex	ID	ACM	IEEE	Scopus	Compendex	ID	ACM	IEEE	Scopus	Compendex
S1			X	X	S25	X		X	X	S49			X	
S2	X		X	X	S26			X		S50			X	
S3		X		X	S27	X	X			S51			X	X
S4			X	X	S28			X		S52	X	X	X	X
S5		X	X	X	S29			X		S53			X	
S6			X	X	S30			X		S54			X	X
S7			X	X	S31			X	X	S55		X	X	X
S8		X			S32		X			S56		X	X	X
S9		X			S33	X	X	X	X	S57			X	X
S10	X	X	X	X	S34			X	X	S58		X	X	X
S11		X			S35				X	S59	X	X		
S12		X	X		S36	X				S60			X	
S13	X	X	X	X	S37		X			S61	X		X	X
S14			X		S38				X	S62		X		
S15			X		S39	X				S63			X	X
S16		X	X	X	S40		X	X	X	S64			X	X
S17			X		S41		X	X	X	S65	X		X	X
S18			X	X	S42		X			S66		X		
S19		X		X	S43		X	X	X	S67			X	X
S20	X			X	S44		X	X	X	S68		X	X	X
S21		X	X	X	S45	X		X	X	S69	X		X	X
S22			X	X	S46			X		S70		X		
S23		X	X	X	S47			X	X	S71	X	X	X	X
S24	X	X	X	X	S48		X	X	X					

Table A2. Studies.

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S1	[15]	A bayesian approach for suspicious financial activity reporting	Bayesian network (BN) based approach to detect suspicious behavior in financial transactions.	Nida S. Khan, Asma S. Larik, Quratulain Rajput and Sajjad Haider	International Journal of Computers and Applications	IJCAA	2013
S2	[16]	A clique-based method for mining fuzzy graph patterns in anti-money laundering systems	Click-based method for fuzzy graphic money-mining pattern mining	Bershtein L.S. and Tselykh A.A.	International Conference on Security of Information and Networks	SIN	2013
S3	[17]	A framework for financial botnet analysis	Framework for detecting, viewing and sharing information about financial botnets	Marco Riccardi, David Oro, Jesus Luna, Marco Cremonini and Marc Vilanova	eCrime Researchers Summit	eCRS	2010
S4	[18]	A framework for preventing money laundering in bank	A framework for bank money laundering prevention formed by mapping COBIT to COSO	Vandana Pramod, Jinghua Li and Ping Gao	Information Management & Computer Security (Renamed to: Information and Computer Security)	ICS	2012
S5	[19]	A Money Laundering Risk Evaluation Method Based on Decision Tree	Decision Tree for Creating Money Laundering Risk Determination Rules for Bank Customers	Su-Nan Wang and Jian-Gang Yang	International Conference on Machine Learning and Cybernetics	ICMLC	2007
S6	[20]	A multi-agent system in the combat against money laundering	Multiagent approach to combating money laundering by capturing suspicious transactions and assisting in analyzing suspicious behavior	Claudio Alexandre and João Balsa	Iberian Journal of Information Systems and Technologies	RISTI	2017
S7	[21]	A new algorithm for money laundering detection based on structural similarity	Framework for detecting money laundering transactions between large data volumes by reducing the input data set	Reza Soltani, Uyen Trang Nguyen, Yang Yang, Mohammad Faghani, AlaaYagoub and Aijun An	IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference	UEMCON	2016
S8	[22]	A Novel Multiobjective Approach for Detecting Money Laundering with a Neuro-Fuzzy Technique	Multi-objective approach based on Adaptive Neuro-Diffuse Inference System to recognize bank money laundering and currency exchange	Mohammad (Behdad) Jamshidi, Ali Lalbakhsh, MohammadrezaGorjiankhanzad and Saeed Roshani	IEEE International Conference on Networking, Sensing and Control	ICNSC	2019
S9	[23]	A RBF neural network model for anti-money laundering	Radial function neural network model based on clustering algorithm APC-III and smaller recursive square algorithm for combating money laundering	Lin-Tao LV, Na Ji and Jiu-Long Zhang	International Conference on Wavelet Analysis and Pattern Recognition	ICWAPR	2008
S10	[24]	A Scan Statistics Based Suspicious Transactions Detection Model for Anti-money Laundering (AML) in Financial Institutions	Suspicious transaction detection model based on statistical scanning and machine learning	Xuan Liu and Pengzhu Zhang	International Conference on Multimedia Communications	MEDIACOM	2010
S11	[25]	An advanced network visualization system for financial crime detection	System for visual analysis of financial activity networks through social network analysis and clustering	Walter Didimo, Giuseppe Liotta, Pietro Palladino and Fabrizio Montecchiani	IEEE Pacific Visualization Symposium	APVIS	2011
S12	[26]	An Agent Based Anti-Money Laundering System Architecture for Financial Supervision	Agent-based anti-money laundering architecture for financial oversight	LiuXuan and Zhang Pengzhu	International Conference on Wireless Communications, Networking and Mobile Computing	WiCOM	2007

Table A2. *Cont.*

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S13	[27]	An Outlier Detection Model Based on Cross Datasets Comparison for Financial Surveillance	Cross-outlier detection model based on distance definition incorporated with financial transaction data capabilities.	Zhu Tianqing	IEEE Asia-Pacific Conference on Services Computing	APSCC	2006
S14	[28]	Anti-money laundering in financial institutions using affiliation mapping calculation and sequential mining	Affiliation mapping calculation and sequential mining	VikasJayasree and R.V Siva Balan	Journal of Engineering and Applied Sciences	JEAS	2016
S15	[29]	Anti-money laundering using a two-phase system	Plan-based framework for anti-money laundering systems	Tamer HossamMoustafa, Mohamed ZakiAbd El-Megied and Tarek Salah Sobh and Khaled Mohamed Shafea	Journal of Money Laundering Control	JOMLC	2015
S16	[30]	Anti-money-laundering System Based on Mainframe and SOA	Mainframe-based money laundering warning system with SOA architectures	Mao Shu, Liu Rui, Li Dancheng and Zhu Shuaizhen	International Conference on Computational Intelligence and Communication Networks	CICN	2013
S17	[31]	Application of artificial intelligence technologies for the monitoring of transactions in AMLsystems using the example of the developed classification algorithm	Transaction classification algorithm using machine learning methods and graph-based approaches	S.G. Magomedov, A.S. Dobrotvorsky, M.P. Khrestina, S.A. Pavelyev and T.R. Yusubaliev	International Journal of Engineering & Technology	IJET	2018
S18	[32]	Application of machine analysis algorithms to automate implementation of tasks of combating criminal money laundering	Application of machine analysis algorithms to automate the implementation of anti-money laundering tasks	Dmitry Dorofeev, Marina Khrestina, TimurUsubaliev, Aleksey Dobrotvorskiy and SaveliyFilatov	International Conference on Digital Transformation and Global Society	DTGS	2018
S19	[33]	Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism	Methodology for automating the generation of new typology-based ML / FT schema variants using Big Data	Kirill Plaksiy, Andrey Nikiforov and Natalia Miloslavskaya	International Conference on Future Internet of Things and Cloud Workshops	FiCLOUDW	2018
S20	[34]	Applying data mining in money laundering detection for the vietnamese banking industry	Money Laundering Detection Techniques Using Banking Data Transfer Grouping Techniques	Dang Khoa Cao and Phuc Do	Asian Conference on Intelligent Information and Database Systems	ACIIDS	2012
S21	[35]	Breaking Through Opacity: A Context-Aware Data-Driven Conceptual Design for a Predictive Anti Money Laundering System	Context-driven, data-driven software / hardware approach to physical money tracking	Oussama H. Hamid	IEEE-GCC Conference and Exhibition	GCCCE	2017
S22	[36]	Clustering based anomalous transaction reporting	Approach to Reporting Cluster-Based Anomalous Financial Transactions	Asma S. Larik and SajjadHaider	World Conference on Information Technology	WCIT	2011
S23	[37]	CoDetect: Financial Fraud Detection With Anomaly Feature Detection	A framework for detecting financial fraud and resource patterns associated with fraud activity	Dongxu Huang, Dejun Mu, Libin Yang and Xioayan Cai	IEEE Access	IEEE Access	2018
S24	[38]	Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions	Anti-money laundering model combining digital forensic practices and database analysis methodologies	Denys A. Flores, Olga Angelopoulou, Richard J. Self	International Conference on Emerging Intelligent Data and Web Technologies	EIDWT	2012

Table A2. *Cont.*

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S25	[39]	Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering	Application of intelligent agents to assist preventive controls in anti-money laundering system	Shijia Gao, Dongming Xu,	Expert Systems with Applications	ESWA	2009
S26	[40]	Data Mining Techniques for Anti-Money Laundering	Use of anti-money laundering data mining techniques based on the evaluation of four types of neural networks	AssemKhalaf Ahmed Allam El-Din and Nashaat El Khamesy	International Journal of Computer Applications	IJCA	2016
S27	[41]	DBSCAN Clustering Algorithm Applied to Identify Suspicious Financial Transactions	Clustering algorithm application to identify suspicious financial transactions and anti-money laundering regulatory enforcement system	Y. Yang, B. Lian, L. Li, C. Chen and P. Li	International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery	CyberC	2014
S28	[42]	Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering	Unsupervised model for detecting suspected export fraud through deep learning	Ebberth L Paula, Marcelo Ladeira, Rommel N. Carvalho and Thiago Marzagão	IEEE International Conference on Machine Learning and Applications	ICMLA	2016
S29	[43]	Design of a Monitor for Detecting Money Laundering and Terrorist Financing	Monitoring framework for anti-money laundering systems based on rule base monitoring, behavior detection monitoring, cluster monitoring and link analysis based monitoring	Tamer Hossam Eldin Helmy, Mohamed zakiAbd-ElMegied, Tarek S. Sobh and Khaled Mahmoud Shafea Badran	International Journal of Computer Networks and Applications	IJCNA	2016
S30	[44]	Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type	Decentralized approach to detecting possible money laundering transactions based on blockchain technology	Artem A. Maksutov, Maxim S. Alexeev, Natalia O. Fedorova and Daniil A. Andreev	IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering	EIConRus	2019
S31	[45]	Detection of Suspicious Transactions with Database Forensics and Theory of Evidence	Forensic methodology for monitoring database transactions through audit logs and Bayesian classification algorithm	Harmeet Kaur Khanuja and Dattatraya Adane	International Symposium on Security in Computing and Communication	SSCC	2019
S32	[46]	Developing an intelligent data discriminating system of anti-money laundering based on SVM	Unusual client behavior detection method based on support vector machine	JunTang and Jian Yin	International Conference on Machine Learning and Cybernetics	ICMLC	2005
S33	[47]	Discovering Hidden Group in Financial Transaction Network Using Hidden Markov Model and Genetic Algorithm	Approach to Hidden Group Discovery in a Hidden Model Markov Financial Transaction Network	Yuhua Li, DongshengDuan, Guanghao Hu and Zhengding Lu	International Conference on Fuzzy Systems and Knowledge Discovery	FSKD	2009
S34	[48]	Dynamic Approach for Detection of Suspicious Transactions in Money Laundering	Dynamic approach to detecting suspicious behavior-based money laundering transactions through hash method	Anagha A Rao, Kanchana V.	International Journal of Engineering & Technology	IJET	2018
S35	[49]	Dynamic Risk Model of Money Laundering	Dynamic money laundering risk model based on static risk score	Murad Mehmet, Murat Günestas and Duminda Wijesekera	International Workshop on Risk Assessment and Risk-driven Testing	RISK	2014
S36	[50]	Event-based approach to money laundering data analysis and visualization	Event-based approach to money laundering data analysis and visualization	Tat-Man Cheong and Yain-Whar Si	International Symposium on Visual Information Communication	VINCI	2010

Table A2. *Cont.*

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S37	[51]	Exploration of the effectiveness of expectation maximization algorithm for suspicious transaction detection in anti-money laundering	Application of expectations maximization algorithms to detect suspicious transactions	Zhiyuan Chen, Le Dinh Van Khoa, Amril Nazir, Ee Na Teoh and Ettikan Kandasamy Karupiah	IEEE Conference on Open Systems	ICOS	2014
S38	[52]	Fighting money laundering with technology: A case study of Bank X in the UK	Application of the structural coupling concept to portray the dynamic relationship between computer profile and human profile	Dionysios S. Demetis	Decision Support Systems	DSS	2018
S39	[53]	Finding shell company accounts using anomaly detection	Application of anomaly detection algorithms to identify ghost companies	Devendra Kumar Luna, Manoj Apte, Girish Keshav Palshikar and Arnab Bhattacharya	ACM India Joint International Conference on Data Science and Management of Data	CODS-COMAD	2018
S40	[54]	Finding Suspicious Activities in Financial Transactions and Distributed Ledgers	Methodology for exploratory analysis of financial data and information using anomaly detection algorithms	R. D. Camino, R. State, L. Montero and P. Valtchev	IEEE International Conference on Data Mining Workshops	ICDMW	2017
S41	[55]	Graph mining approach to suspicious transaction detection	Graphic mining machine learning method for suspicious transaction detection	K. Michalak and J. Korczak	Federated Conference on Computer Science and Information Systems	FedCSIS	2011
S42	[56]	Identifying and tracking online financial services through web mining and latent semantic indexing	Tool application for monitoring and identifying online financial transactions using latent semantic indexing for text mining	Kristen Bernard, Andrew Cassidy, Monica Clark, Kevin Liu, Katrina Lobaton, Drew McNeill and Donald Brown	IEEE Systems and Information Engineering Design Symposium	SIEDS	2011
S43	[57]	Intelligent Anti-Money Laundering Solution Based upon Novel Community Detection in Massive Transaction Networks on Spark	Method to detect suspected money laundering Communities in massive transaction networks by proposing a Louvain algorithm	X. Li, X. Cao, X. Qiu, J. Zhao and J. Zheng	International Conference on Advanced Cloud and Big Data	CBD	2017
S44	[58]	Intelligent money laundering monitoring and detecting system	Intelligent agents application for money laundering monitoring and detection based on Simons decision-making theory	Shijia Gao, Dongming Xu, Huaiqing Wang and Yingfeng Wang	European and Mediterranean Conference on Information Systems	EMCIS	2008
S45	[59]	Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services	Application of visualization techniques to detect fraudulent activity in mobile money transfer services	Evgenia Novikova, Igor Kotenko and Evgenii Fedotov	International Journal of Mobile Computing and Multimedia Communications	IJMCMC	2014
S46	[60]	Money laundering analysis based on time variant behavioral transaction patterns using data mining	Time-variant approach using behavioral patterns to identify money laundering	Krishnapriya, G and Prabakaran, M	Journal of Theoretical and Applied Information Technology	JATIT	2014
S47	[61]	Money Laundering Analytics Based on Contextual Analysis. Application of Problem Solving Ontologies in Financial Fraud Identification and Recognition	Application of problem solving ontologies in identifying and recognizing financial fraud	Chmielewski M. and Stąpor P.	International Conference on Information Systems Architecture and Technology	ISAT	2017
S48	[62]	Money laundering detection using TFA system	Application of mining and clustering algorithms for transaction flow analysis	P. Umadevi and E. Divya	International Conference on Software Engineering and Mobile Application Modelling and Development	ICSEMA	2012

Table A2. *Cont.*

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S49	[63]	Money Laundering Identification on Banking Data Using Probabilistic Relational Audit Sequential Pattern	Application of sequential probabilistic relational audit standard for identification of money laundering in bank data	Vikas Jayasree and R.V. Siva Balan	Asian Journal of Applied Sciences	AJAS	2015
S50	[64]	Monitor and Detect Suspicious Transactions With Database Forensic Analysis	Database forensic analysis methodology to monitor and detect suspicious transactions	Kaur Khanuja, Harmeet and Adane, Dattatraya	Journal of Database Management	JDM	2018
S51	[65]	NextGen AML: Distributed Deep Learning based Language Technologies to Augment Anti Money Laundering Investigation	Application of natural language processing techniques for deep learning in money laundering research	Jingguang Han, Utsab Barman, Jer Hayes, Jinhua Du, Edward Burgin and Dadong Wan	Annual Meeting of the Association for Computational Linguistics-System Demonstrations	AMACLSD	2018
S52	[66]	No Smurfs: Revealing Fraud Chains in Mobile Money Transfers	Application of the model-based approach to PSA@R event-driven process safety analysis	M. Zhdanova, J. Repp, R. Rieke, C. Gaber and B. Hemery	International Conference on Availability, Reliability and Security	ARES	2014
S53	[67]	On the use of data mining methods for money laundering detection based on financial transactions information	Use of data mining methods in financial transactions for money laundering detection	Ayshan Gasanova, Alexander N. Medvedev, Evgeny I. Komotskiy, Kamen B. Spasov and Igor N. Sachkov	AIP Conference Proceedings	AIP	2018
S54	[68]	Peer to Peer Anti-Money Laundering Resource Allocation Based on Semi-Markov Decision Process	Anti-money laundering resource allocation based on semi-Markov decision process	Xintao Hong, Hongbin Liang, Lin X. Cai, Zengan Gao and Limin Sun	IEEE Global Communications Conference	GLOBECOM	2015
S55	[69]	Real-Time Exception Management Decision Model (RTEMDM): Applications in Intelligent Agent-Assisted Decision Support in Logistics and Anti-Money Laundering Domains	Real-time decision support approach in multi-agent based exception management	S. Gao and D. Xu	Hawaii International Conference on System Sciences	HICSS	2010
S56	[70]	Research on anti-money laundering based on core decision tree algorithm	Central decision tree algorithm to identify money laundering activities by combining BIRCH and K-means	R. Liu, X. Qian, S. Mao and S. Zhu	Chinese Control and Decision Conference	CCDC	2011
S57	[71]	Research on Anti-Money Laundering Hierarchical Model	Hierarchical model of capital flow based on suspicious data to combat money laundering and use of the peso-entopine method	Y. Jin and Z. Qu	IEEE International Conference on Software Engineering and Service Science	ICSESS	2018
S58	[72]	Research on application of distributed data mining in anti-money laundering monitoring system	Application of data mining techniques to analyze custom transaction behavior	Cheng-wei Zhang and Yu-bo Wang	International Conference on Advanced Computer Control	ICACC	2010
S59	[73]	Research on Suspicious Financial Transactions Recognition Based on Privacy-Preserving of Classification Algorithm	Application of the privacy preservation rating algorithm to identify suspicious financial transactions	C. Ju and L. Zheng	International Workshop on Education Technology and Computer Science	ETCS	2009
S60	[74]	Risk-based approach for designing enterprise-wide AML information system solution	Risk-based approach to designing AML information system solution	Ai, Lishan and Tang, Jun	Journal of Financial Crime	JFC	2011

Table A2. *Cont.*

ID	References	Title	Approach	Author(s)	Venue	Acronym	Year
S61	[75]	Sequence Matching for Suspicious Activity Detection in Anti-Money Laundering	Computational approach to identifying suspicious transactions through sequence matching	Liu X., Zhang P. and Zeng D	International Conference on Intelligence and Security Informatics	CORE	2008
S62	[76]	Study on Anti-Money Laundering Service System of Online Payment Based on Union-Bank Mode	Dynamic monitoring and analysis of online payment transactions for money laundering identification	Q. Yang, B. Feng and P. Song	International Conference on Wireless Communications, Networking and Mobile Computing	WiCOM	2007
S63	[77]	Suspicious activity reporting using Dynamic Bayesian Networks	Approach employing a combination of clustering and dynamic Bayesian network (DBN) to identify transaction sequence anomalies	Raza, Saleha and Haider, Sajjad	Procedia Computer Science (World Conference on Information Technology)	WCIT	2011
S64	[78]	System supporting money laundering detection	Using a Money Laundering Detection Support System Using Clustering and Frequent Patters	Rafat Drezewski, Jan Sepielak and Wojciech Filipkowski	Digital Investigation	DI	2012
S65	[79]	The application of social network analysis algorithms in a system supporting money laundering detection	Social network analytics application in money laundering detection	Rafal Dreżewski, Jan Sepielak and Wojciech Filipkowski	Information Sciences	IS	2015
S66	[80]	The DBInspector project	Using High Performance Computing Technology to Implement a Software Environment for Anti-Money Laundering Activities	P. Stofella	International Workshop on Research Issues in Data Engineering	RIDE	1997
S67	[81]	Toward the discovery and extraction of money laundering evidence from arbitrary data formats using combinatory reductions	Using Comminatory Reductions to Discover and Extract Money Laundering Evidence	Alonza Mumford and Duminda Wijesekera	International Conference on Semantic Technologies for Intelligence, Defense and Security	STIDS	2014
S68	[82]	Using dynamic risk estimation & social network analysis to detect money laundering evolution	Using dynamic risk estimation and social network analysis to detect the evolution of money laundering	M. Mehmet and D. Wijesekera	IEEE International Conference on Technologies for Homeland Security	HST	2013
S69	[83]	Using social network analysis to prevent money laundering.	Approach to classifying and mapping relational data and presenting predictive models - based on network metrics - to assess customer risk profiles	Andrea Fronzetti Colladon and Elisa Remondi	Expert Systems With Applications	ESWA	2017
S70	[84]	Visual exploration of cash flow chains	Interactive visual exploration of financial transaction chains	J. Korczak and W. Łuszczyk	Federated Conference on Computer Science and Information Systems	FedCSIS	2011
S71	[85]	WireVis: Visualization of Categorical, Time-Varying Data From Financial Transactions	Multi view approach to assist in exploring large volume electronic transaction data	Remco Chang, Mohammad Ghoniem, Robert Kosara, William Ribarsky and Jing Yang	IEEE Symposium on Visual Analytics Science and Technology	VAST	2007

References

1. Camdessus, M. Money Laundering: The importance ofinternational countermeasures. In Proceedings of the IMF to the Plenary Meeting of the Financial Action TaskForce on Money Laundering, Paris, France, 10 February 1988; p. 2.
2. HM Treasury. Anti-Money Laundering Strategy, October 2004. Available online: http://wgfacml.asa.gov.eg/en/doc_interest/doc_sais/0%20UK%20Treasury%20AML%20strategy.pdf (accessed on 4 June 2019).
3. Federal Bureau of Investigation (FBI). Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform—Statement for the Record. Criminal Investigative Division, Department of Justice: United States, 2018. Available online: https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance (accessed on 2 June 2019).
4. United Nations Office on Drugs and Crime (UNODC). Money-Laundering and Globalization. Available online: https://www.unodc.org/unodc/en/money-laundering/globalization.html (accessed on 2 July 2019).
5. *Basel AML Index: A Country Ranking and Review of Money Laundering and Terrorist Financing Risks around the World*, 8th ed.; Basel Institute on Governance, University of Basel: Basel, Switzerland, 2019; Available online: https://www.baselgovernance.org/sites/default/files/2019-10/Basel%20AML%20Index%208%20edition.pdf (accessed on 29 October 2019).
6. Ngai, E.W.T.; Hu, Y.; Wong, Y.H.; Chen, Y.; Sun, X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decis. Support Syst.* **2011**, *50*, 559–569. [CrossRef]
7. Phua, C.; Lee, V.; Smith, K.; Gayler, R. A Comprehensive Survey of Data Miningbased Fraud Detection Research. *Comput. Hum. Behav.* **2012**, *28*, 1002–1013.
8. Sudjianto, A.; Nair, S.; Yuan, M.; Zhang, A.; Kern, D.; Cela Diaz, F. Statistical Methods for Fighting Financial Crimes. *Technometrics* **2010**, *52*, 5–19. [CrossRef]
9. Semenov, A.; Dorofeev, D.; Mazeev, A.; Yusubaliev, T. Survey of Common Design Approaches in AML Software Development. In Proceedings of the GraphHPC-2017 Conference, Moscow, Russia, 2 March 2017; Voevodin, V., Simonov, A., Eds.; Moscow State University: Moscow, Russia, 2017.
10. Chen, Z.; Dinh, L.; Khoa, V.; Nazir, A.; Teoh, E.N.; Karupiah, E.K.; Lam, K.S. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowl. Inf. Syst.* **2018**, *57*, 245–285. [CrossRef]
11. Kitchenham, B.A.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, EBSE Technical Report version 2.3, EBSE-2017-01; Software Engineering Group; Keele Univ.: Keele, UK; Univ of Durham: Durham, UK, 2007.
12. Chen, L.; Babar, M.A.; Zhang, H. Towards na evidence-based understanding of eletronic data souces. In Proceedings of the 14th International Conference on Evaluation and Assessment in Software Engineering (EASE), Swindon, UK, 12–13 April 2010; pp. 135–138.
13. Chen, L.; Babar, M.A.; Cawley, C. A Status Report on the Evaluation of Variability Management Approaches. In Proceedings of the 13th International Conference on Evaluation and Assessment in Software Engineering, EASE'09, Swindon, UK, 20–21 April 2009; pp. 118–127.
14. Dyba, T.; Dingsoyr, T. Empirical Studies of Agile Software Development: A Systematic Review. *Inf. Softw. Technol.* **2008**, *50*, 833–859. [CrossRef]
15. Khan, N.S.; Larik, A.S.; Rajput, Q.; Haider, S. A Bayesian Approach for Suspicious Financial Activity Reporting. *Int. J. Comput. Appl.* **2013**, *35*, 181–187. [CrossRef]
16. Bershtein, L.S.; Tselykh, A.A. A clique-based method for mining fuzzy graph patterns in anti-money laundering systems. In Proceedings of the 6th International Conference on Security of Information and Networks (SIN'13), New York, NY, USA, 26–28 November 2013; pp. 384–387. [CrossRef]
17. Riccardi, M.; Oro, D.; Luna, J.; Cremonini, M.; Vilanova, M. A Framework for Financial Botnet Analysis. In Proceedings of the 2010 eCrime Researchers Summit, Dallas, TX, USA, 18–20 October 2010; pp. 1–7. [CrossRef]
18. Vandana, P.; Jing, L.; Ping, G. A framework for preventing money laundering in banks. *Inf. Manag. Comput. Secur.* **2012**, *20*, 170–183. [CrossRef]

19. Wang, S.; Yang, J. A Money Laundering Risk Evaluation Method Based on Decision Tree. In Proceedings of the 2007 International Conference on Machine Learning and Cybernetics, Hong Kong, China, 19–22 August 2007; pp. 283–286. [CrossRef]
20. Alexandre, C.; Balsa, J. A Multi-Agent System in the Combat Against Money Laundering. *RISTI Porto* **2017**, *25*, 1–17. [CrossRef]
21. Soltani, R.; Nguyen, U.T.; Yang, Y.; Faghani, M.; Yagoub, A. A new algorithm for money laundering detection based on structural similarity. In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 20–22 October 2016; pp. 1–7. [CrossRef]
22. Jamshidi, M.B.; Gorjiankhanzad, M.; Lalbakhsh, A.; Roshani, S. A Novel Multiobjective Approach for Detecting Money Laundering with a Neuro-Fuzzy Technique. In Proceedings of the 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC), Banff, AB, Canada, 9–11 May 2019; pp. 454–458. [CrossRef]
23. Lin-Tao, L.; Na, J.; Jiu-Long, Z. A RBF neural network model for anti-money laundering. In Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition, Hong Kong, China, 30–31 August 2008; pp. 209–215. [CrossRef]
24. Liu, X.; Zhang, P. A Scan Statistics Based Suspicious Transactions Detection Model for Anti-money Laundering (AML) in Financial Institutions. In Proceedings of the 2010 International Conference on Multimedia Communications, Hong Kong, China, 7–8 August 2010; pp. 210–213. [CrossRef]
25. Didimo, W.; Liotta, G.; Montecchiani, F.; Palladino, P. An advanced network visualization system for financial crime detection. In Proceedings of the 2011 IEEE Pacific Visualization Symposium, Hong Kong, China, 1–4 March 2011; pp. 203–210. [CrossRef]
26. Liu, X.; Zhang, P. An Agent Based Anti-Money Laundering System Architecture for Financial Supervision. In Proceedings of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007; pp. 5472–5475. [CrossRef]
27. Zhu, T. An Outlier Detection Model Based on Cross Datasets Comparison for Financial Surveillance. In Proceedings of the 2006 IEEE Asia-Pacific Conference on Services Computing (APSCC'06), Guangzhou, China, 12–15 December 2006; pp. 601–604. [CrossRef]
28. Jayasree, V.; Siva, B.R.V. Anti-Money Laundering in Financial Institutions Using Affiliation Mapping Calculation and Sequential Mining. *J. Eng. Appl. Sci.* **2016**, *11*, 51–56. [CrossRef]
29. Tamer, H.M.; Mohamed, Z.A.E.; Tarek, S.S.; Khaled, M.S. Anti money laundering using a two-phase system. *J. Money Laund. Control* **2015**, *18*, 304–329. [CrossRef]
30. Shu, M.; Rui, L.; Dancheng, L.; Shuaizhen, Z. Anti-money-laundering System Based on Mainframe and SOA. In Proceedings of the 2013 5th International Conference and Computational Intelligence and Communication Networks, Mathura, India, 27–29 September 2013; pp. 613–616. [CrossRef]
31. Magomedov, G.S.; Dobrotvorsky, A.S.; Khrestina, M.P.; Pavelyev, S.A.; Yusubaliev, T.R. Application of Artificial Intelligence Technologies for the Monitoring of Transactions in AML-Systems Using the Example of the Developed Classification Algorithm. *Int. J. Eng. Technol.* **2018**, *7*, 76–79. [CrossRef]
32. Dorofeev, D.; Khrestina, M.; Usubaliev, T.; Dobrotvorskiy, A.; Filatov, S. Application of Machine Analysis Algorithms to Automate Implementation of Tasks of Combating Criminal Money Laundering. In *Digital Transformation and Global Society, DTGS 2018, Communications in Computer and Information Science*; Alexandrov, D., Boukhanovsky, A., Chugunov, A., Kabanov, Y., Koltsova, O., Eds.; Springer: Cham, Switzerland, 2018.
33. Plaksiy, K.; Nikiforov, A.; Miloslavskaya, N. Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 70–77. [CrossRef]
34. Cao, D.K.; Do, P. Applying Data Mining in Money Laundering Detection for the Vietnamese Banking Industry. In *Asian Conference on Intelligent Information and Database Systems*; Pan, J.S., Chen, S.M., Nguyen, N.T., Eds.; Springer: Berlin, Germany, 2012.
35. Hamid, O.H. Breaking Through Opacity: A Context-Aware Data-Driven Conceptual Design for a Predictive Anti Money Laundering System. In Proceedings of the 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), Manama, Bahrain, 8–11 May 2017; pp. 1–9. [CrossRef]

36. Asma, S.L.; Sajjad, H. Clustering based anomalous transaction reporting. *Procedia Comput. Sci.* **2011**, *3*, 606–610. [CrossRef]
37. Huang, D.; Mu, D.; Yang, L.; Cai, X. CoDetect: Financial Fraud Detection with Anomaly Feature Detection. *IEEE Access* **2018**, *6*, 19161–19174. [CrossRef]
38. Flores, D.A.; Angelopoulou, O.; Self, R.J. Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions. In Proceedings of the 2012 Third International Conference on Emerging Intelligent Data and Web Technologies, Bucharest, Romania, 19–21 September 2012; pp. 218–224. [CrossRef]
39. Shi, G.; Dong, X. Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering. *Expert Syst. Appl.* **2009**, *36*, 1493–1504. [CrossRef]
40. Khalaf, A.; El, N. Data Mining Techniques for Anti-Money Laundering. *Int. J. Comput. Appl.* **2016**, *146*, 28–33. [CrossRef]
41. Yang, Y.; Lian, B.; Li, L.; Chen, C.; Li, P. DBSCAN Clustering Algorithm Applied to Identify Suspicious Financial Transactions. In Proceedings of the 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, China, 13–15 October 2014; pp. 60–65. [CrossRef]
42. Paula, E.L.; Ladeira, M.; Carvalho, R.N.; Marzagão, T. Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 954–960. [CrossRef]
43. Tamer, H.E.H.; Mohamed, Z.A.E.; Tarek, S.S.; Khaled, M.S.B. Design of a Monitor for Detecting Money Laundering and Terrorist Financing. *J. Theor. Appl. Inf. Technol.* **2016**, *1*, 425–436.
44. Maksutov, A.A.; Alexeev, M.S.; Fedorova, N.O.; Andreev, D.A. Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type. In Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 28–31 January 2019; pp. 274–277. [CrossRef]
45. Khanuja, H.K.; Adane, D. Detection of Suspicious Transactions with Database Forensics and Theory of Evidence. In *International Symposium on Security in Computing and Communication*; Springer: Singapore, 2019.
46. Jun, T.; Jian, Y. Developing an intelligent data discriminating system of anti-money laundering based on SVM. In Proceedings of the 2005 International Conference on Machine Learning and Cybernetics, Guangzhou, China, 18–21 August 2005; pp. 3453–3457. [CrossRef]
47. Li, Y.; Duan, D.; Hu, G.; Lu, Z. Discovering Hidden Group in Financial Transaction Network Using Hidden Markov Model and Genetic Algorithm. In Proceedings of the 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery, Tianjin, China, 14–16 August 2009; pp. 253–258. [CrossRef]
48. Anagha, A.R.; Kanchana, V. Dynamic Approach for Detection of Suspicious Transactions in Money Laundering. *Int. J. Eng. Technol.* **2018**, *7*, 10–13. [CrossRef]
49. Mehmet, M.; Güneştaş, M.; Wijesekera, D. Dynamic Risk Model of Money Laundering. In *Risk Assessment and Risk-Driven Testing, RISK 2013, Lecture Notes in Computer Science*; Bauer, T., Großmann, J., Seehusen, F., Stølen, K., Wendland, M.F., Eds.; Springer: Cham, Switzerland, 2014; p. 8418. [CrossRef]
50. Tat-Man, C.; Yain-Whar, S. Event-based approach to money laundering data analysis and visualization. In Proceedings of the 3rd International Symposium on Visual Information Communication (VINCI'10), Beijing, China, 28–29 September 2010; ACM: New York, NY, USA, 2010.
51. Chen, Z.; Nazir, A.; Teoh, E.N.; Karupiah, E.K. Exploration of the effectiveness of expectation maximization algorithm for suspicious transaction detection in anti-money laundering. In Proceedings of the 2014 IEEE Conference on Open Systems (ICOS), Subang, Malaysia, 26–28 October 2014; pp. 145–149. [CrossRef]
52. Dionysios, S.D. Fighting money laundering with technology: A case study of Bank X in the UK. *Decis. Support Syst.* **2018**, *105*, 96–107. [CrossRef]
53. Devendra, K.L.; Manoj, A.; Girish, K.P.; Arnab, B. Finding Shell Company Accounts Using Anomaly Detection. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD '18), Goa, India, 11–13 January 2018; ACM: New York, NY, USA; pp. 167–174. [CrossRef]
54. Camino, R.D.; State, R.; Montero, L.; Valtchev, P. Finding Suspicious Activities in Financial Transactions and Distributed Ledgers. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 787–796. [CrossRef]

55. Michalak, K.; Korczak, J. Graph mining approach to suspicious transaction detection. In Proceedings of the 2011 Federated Conference on Computer Science and Information Systems (FedCSIS), Szczecin, Poland, 18–21 September 2011; pp. 69–75, ISBN 978-83-60810-39-2.
56. Bernard, K.; Cassidy, A.; Clark, M.; Liu, K.; Lobaton, K.; McNeill, D.; Brown, D. Identifying and tracking online financial services through web mining and latent semantic indexing. In Proceedings of the 2011 IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 29 April 2011; pp. 158–163. [CrossRef]
57. Li, X.; Cao, X.; Qiu, X.; Zhao, J.; Zheng, J. Intelligent Anti-Money Laundering Solution Based upon Novel Community Detection in Massive Transaction Networks on Spark. In Proceedings of the 2017 Fifth International Conference on Advanced Cloud and Big Data (CBD), Shanghai, China, 13–16 August 2017; pp. 176–181. [CrossRef]
58. Wang, Y.; Wang, H.; Gao, S.; Xu, D. Intelligent money laundering monitoring and detecting system. In Proceedings of the European and Mediterranean Conference on Information Systems, EMCIS, Al Bustan Rotana Hotel, Dubai, UAE, 25–26 May 2008. [CrossRef]
59. Novikova, E.; Kotenko, I.; Fedotov, E. Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services. *Int. J. Mob. Comput. Multimed. Commun.* **2014**, *6*, 73–97. [CrossRef]
60. Krishnapriya, G.; Prabakaran, M. Money laundering analysis based on time variant behavioral transaction patterns using data mining. *J. Theor. Appl. Inf. Technol.* **2014**, *67*, 12–17.
61. Chmielewski, M.; Stąpor, P. Money Laundering Analytics Based on Contextual Analysis. Application of Problem Solving Ontologies in Financial Fraud Identification and Recognition. Information Systems Architecture and Technology. In *ISAT 2016—Part I. Advances in Intelligent Systems and Computing, Proceedings of the 37th International Conference on Information Systems Architecture and Technology, Karpacz, Poland, 18–20 September 2016*; Borzemski, L., Grzech, A., Świątek, J., Wilimowska, Z., Eds.; Springer: Cham, Switzerland, 2017; p. 521. [CrossRef]
62. Umadevi, P.; Divya, E. Money laundering detection using TFA system. In Proceedings of the International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), Chennai, India, 19–21 December 2012; pp. 1–8. [CrossRef]
63. Jayasree, V.; Siva Balan, R.V. Money Laundering Identification on Banking Data Using Probabilistic Relational Audit Sequential Pattern. *Asian J. Appl. Sci.* **2015**, *8*, 173–184. [CrossRef]
64. Kaur, K.H.; Adane, D. Monitor and Detect Suspicious Transactions with Database Forensic Analysis. *J. Database Manag.* **2018**. [CrossRef]
65. Han, J.; Barman, U.; Hayes, J.; Du, J.; Burgin, E.; Wan, D. NextGen AML: Distributed Deep Learning based Language Technologies to Augment Anti Money Laundering Investigation. In Proceedings of the ACL 2018, System Demonstrations, Melbourne, Australia, 15–20 July 2018; Association for Computational Linguistics; pp. 37–42. [CrossRef]
66. Zhdanova, M.; Repp, J.; Rieke, R.; Gaber, C.; Hemery, B. No Smurfs: Revealing Fraud Chains in Mobile Money Transfers. In Proceedings of the 2014 Ninth International Conference on Availability, Reliability and Security, Fribourg, Switzerland, 8–12 September 2014; pp. 11–20. [CrossRef]
67. Gasanova, A.; Medvedev, A.N.; Komotskiy, E.I.; Spasov, K.B.; Sachkov, I.N. On the Use of Data Mining Methods for Money Laundering Detection Based on Financial Transactions Information. In Proceedings of the International Conference of Computational Methods in Sciences and Engineering 2018, ICCMSE 2018, Thessaloniki, Greece, 14–18 March 2018; Volume 2040. [CrossRef]
68. Hong, X.; Liang, H.; Cai, L.X.; Gao, Z.; Sun, L. Peer to Peer Anti-Money Laundering Resource Allocation Based on Semi-Markov Decision Process. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
69. Gao, S.; Xu, D. Real-Time Exception Management Decision Model (RTEMDM): Applications in Intelligent Agent-Assisted Decision Support in Logistics and Anti-Money Laundering Domains. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–10. [CrossRef]
70. Liu, R.; Qian, X.; Mao, S.; Zhu, S. Research on anti-money laundering based on core decision tree algorithm. In Proceedings of the 2011 Chinese Control and Decision Conference (CCDC), Mianyang, China, 23–25 May 2011; pp. 4322–4325. [CrossRef]

71. Jin, Y.; Qu, Z. Research on Anti-Money Laundering Hierarchical Model. In Proceedings of the 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23–25 November 2018; pp. 406–411. [CrossRef]
72. Zhang, C.; Wang, Y. Research on application of distributed data mining in anti-money laundering monitoring system. In Proceedings of the 2010 2nd International Conference on Advanced Computer Control, Shenyang, China, 27–29 March 2010; pp. 133–135. [CrossRef]
73. Ju, C.; Zheng, L. Research on Suspicious Financial Transactions Recognition Based on Privacy-Preserving of Classification Algorithm. In Proceedings of the 2009 First International Workshop on Education Technology and Computer Science, Wuhan, China, 7–8 March 2009; pp. 525–528. [CrossRef]
74. Lishan, A.; Tang, J. Risk-based approach for designing enterprise-wide AML information system solution. *J. Financ. Crime* **2011**, *18*. [CrossRef]
75. Liu, X.; Zhang, P.; Zeng, D. Sequence Matching for Suspicious Activity Detection in Anti-Money Laundering. In *Intelligence and Security Informatics, ISI 2008, Lecture Notes in Computer Science*; Yang, C.C., Ed.; Springer: Berlin, Germany, 2008; p. 5075. [CrossRef]
76. Yang, Q.; Feng, B.; Song, P. Study on Anti-Money Laundering Service System of Online Payment Based on Union-Bank Mode. In Proceedings of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007; pp. 4991–4994. [CrossRef]
77. Raza, S.; Haider, S. Suspicious activity reporting using Dynamic Bayesian Networks. *Procedia Comput. Sci.* **2011**, *3*, 987–991. [CrossRef]
78. Drezewski, R.; Sepielak, J.; Filipkowski, W. System supporting money laundering detection. *Digit. Investig.* **2012**, *9*, 8–21. [CrossRef]
79. Dreżewski, R.; Sepielak, J.; Filipkowski, W. The application of social network analysis algorithms in a system supporting money laundering detection. *Inf. Sci.* **2015**, *295*, 18–32. [CrossRef]
80. Stofella, P. The DBInspector Project. In *Proceedings Seventh International Workshop on Research Issues in Data Engineering*; High Performance Database Management for Large-Scale Applications: Birmingham, UK, 1997; pp. 73–75. [CrossRef]
81. Mumford, A.; Wijesekera, D. Toward the discovery and extraction of money laundering evidence from arbitrary data formats using combinatory reductions. In Proceedings of the International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA, USA, 18–21 November 2014; pp. 32–39.
82. Mehmet, M.; Wijesekera, D. Using dynamic risk estimation & social network analysis to detect money laundering evolution. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12–14 November 2013; pp. 310–315. [CrossRef]
83. Colladon, A.F.; Remondi, E. Using social network analysis to prevent money laundering. *Expert Syst. Appl.* **2017**, *67*, 49–58. [CrossRef]
84. Korczak, J.; Łuszczyk, W. Visual exploration of cash flow chains. In Proceedings of the 2011 Federated Conference on Computer Science and Information Systems (FedCSIS), Szczecin, Poland, 18–21 September 2011; pp. 41–46, ISBN 978-83-60810-39-2.
85. Chang, R.; Ghoniem, M.; Kosara, R.; Ribarsky, W.; Yang, J. Wirevis: Visualization of Categorical, Time-Varying Data from Financial Transactions. In Proceedings of the 2007 IEEE Symposium on Visual Analytics Science and Technology, Sacramento, CA, USA, 30 October–1 November 2007; pp. 155–162. [CrossRef]