computers

MDPI

Review

Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques: A Literature Review

Marco Sánchez-Aguayo [1,*,†], Luis Urquiza-Aguiar [2,†] and José Estrada-Jiménez [2,†]

[1] Departamento de Informática y Ciencias de la Computación, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito 170517, Ecuador
[2] Departamento de Electrónica, Telecomunicaciones y Redes de Información, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito 170517, Ecuador; luis.urquiza@epn.edu.ec (L.U.-A.); jose.estrada@epn.edu.ec (J.E.-J.)
* Correspondence: marco.sanchez01@epn.edu.ec
† These authors contributed equally to this work.

Abstract: Fraud entails deception in order to obtain illegal gains; thus, it is mainly evidenced within financial institutions and is a matter of general interest. The problem is particularly complex, since perpetrators of fraud could belong to any position, from top managers to payroll employees. Fraud detection has traditionally been performed by auditors, who mainly employ manual techniques. These could take too long to process fraud-related evidence. Data mining, machine learning, and, as of recently, deep learning strategies are being used to automate this type of processing. Many related techniques have been developed to analyze, detect, and prevent fraud-related behavior, with the fraud triangle associated with the classic auditing model being one of the most important of these. This work aims to review current work related to fraud detection that uses the fraud triangle in addition to machine learning and deep learning techniques. We used the Kitchenham methodology to analyze the research works related to fraud detection from the last decade. This review provides evidence that fraud is an area of active investigation. Several works related to fraud detection using machine learning techniques were identified without the evidence that they incorporated the fraud triangle as a method for more efficient analysis.

Keywords: fraud; machine learning; cybersecurity; human behavior

Citation: Sánchez-Aguayo, M.; Urquiza-Aguiar, L.; Estrada-Jiménez, J. Fraud Detection Using the Fraud Triangle Theory and Data Mining Techniques: A Literature Review. *Computers* **2021**, *10*, 121. https://doi.org/10.3390/computers10100121

Academic Editor: Francesca Fallucchi

Received: 16 June 2021
Accepted: 2 September 2021
Published: 30 September 2021

1. Introduction

Fraud has increased considerably in recent times, affecting the interests of both financial institutions and their customers. A study conducted by Price Waterhouse Coopers found that 30% of the companies that they surveyed had already been victims of fraud. Moreover, 80% of their fraud was committed within the companies' ranks, especially in administrative areas, such as accounting, operations, sales, and at the management level, without leaving aside the customer service dependencies [1]. Fraud-related activities, which are generally unknown within a company, determine a series of irregularities and illicit acts characterized by intentional deception committed by fraudsters. Most of the anomalies detected are due to the lack of internal control mechanisms, and in such situations, scammers commit fraud by exploiting the weaknesses [2].

Fraud is considered a subset of internal threats, such as corruption, misappropriation of assets, and fraudulent declarations, among others [3]. In a more formal definition, fraud is "the use of one's occupation for personal enrichment through the misuse or deliberate misapplication of the resources or assets of the employing organization", according to the Association of Certified Fraud Examiners (ACFE) [4]. The ability to commit this type of activity is based on the weakness of the control mechanisms that institutions and companies have. In such circumstances, fraudsters commit acts of fraud by taking advantage of these weaknesses.

Since it is committed by humans, fraud is tightly coupled with human behavior. Thus, understanding the motivations of perpetrators or their psychological and personality traits that drive them to cross ethical boundaries can provide a new perspective for fraud detection [5].

Currently, there are different solutions [6] for detecting fraud, which are focused on the use of different tools that perform statistical and parametric analyses based on data mining techniques, as well as analyses of behavior, but none of them solve the problem of timely fraud detection [7].

Given the complexity of analyzing human behavior to detect fraud, some approaches in this line have been proposed to tackle some of the issues involved in this task. For instance, some works aimed to improve the precision and increase the speed of data processing through a hybrid automatic learning system [8] or through incremental learning [9]. Another challenge for fraud detection is the lack of data from which detection systems learn, and [10] proposed a fraud-detection system that does not require previous fraudulent examples. However, even when the data are available, large and small datasets should be addressed differently [11]. In any case, as a human behavior, fraud detection is a multidimensional problem, and so are some of the fraud-detection mechanisms proposed in the literature [12,13].

There is a consensus that prevention should be a priority in order to minimize fraud through proper risk management. Avoiding fraud saves time and financial resources, since detecting it after it occurs has the consequence that the stolen assets are practically irrecoverable. To enhance fraud prevention, organizations should focus on the root of the problem by identifying the causes that lead people to commit fraud and to understand their behavior [14]. Many theories have attempted to answer this question, and the most frequently cited in this context are Cressey's Fraud Triangle Theory (FTT) and Wolf and Hermanson's Diamond Fraud Theory (FDT) [15]. Both approaches analyze how perpetrators go so far as to commit fraud, which is discussed below.

The study of fraud and its analysis is best explained with the help of the Fraud Triangle Theory (FTT), which was proposed by Donald R. Cressey, a leading expert in the sociology of crime. Cressey investigated why people committed fraud and determined their responses based on three elements: pressure, opportunity, and rationalization. This theory also mentions that these elements occur consecutively to provoke the desire to commit fraud. The first necessary element is perceived pressure, which is related to the motivation and drive behind the fraudulent actions of an individual. This motivation often occurs in people who are under some form of financial stress [16]. The second element, known as perceived opportunity, is nothing more than the action behind the crime and the ability to commit it. Finally, the third component, known as rationalization, has to do with the idea that the individual can rationalize their dishonest acts, making their illegal actions seem justified and acceptable [17].

The FDT, considered an extended version of the FTT, integrates a new vertex with the three that were already known—capacity [18]. Despite the cohesion among the three vertices of pressure, opportunity, and rationalization, it is unlikely that people will commit fraud unless they have the capacity (considered the fourth vertex). In other words, the potential perpetrator must have the skills and ability to commit fraud [19].

Various theories of fraud have been used to explain the motivation of this phenomenon. The FTT and FDT can be effectively used to detect the possibility of corporate fraud, where the measurement of all of the associated variables will depend to a great extent on the data used for the study, whether public or private [20].

Fraud analysis, when supported by data mining techniques, helps reduce the manual parts of the detection/verification process and makes the search for fraud more efficient. It is impossible to guarantee the proper moral and ethical behavior of people, especially in the workplace. Due to this reality, a valid option for identifying possible evidence of fraud from available data is to use automatic learning algorithms. Many works cover fraud detection and use data mining techniques as the primary focus [21–24]. Two criticisms of

data-mining-based fraud-detection research are frequently raised: the deficiency of the actual public data available in this domain for conducting experiments [25]—appropriate access to data for researching this area is extremely difficult due to privacy—and the lack of well-documented and published methods and techniques.

1.1. Related Work

Here, we describe some systematic reviews whose main objectives were the analysis and detection of fraud using automatic learning techniques and the application of fraud theories.

Phua et al. [25] carried out a survey in which they identified the limitations of fraud-detection methods and techniques and showed that this field can benefit from other related areas. Specifically, unsupervised approaches may benefit from existing monitoring systems and text extraction, semi-supervised, and game-theoretical approaches; spam and intrusion detection communities can contribute to future fraud-detection investigations. However, above all, the authors focused on the nature of the information and made an exciting reflection on the investigation of fraud detection based on data mining. They also referred to the scarcity of publicly available and real data for carrying out experiments, as well as to the lack of well-documented and published methods and techniques.

Zhou et al. [26] concluded that most fraud-detection systems employ at least one supervised learning method and that unsupervised and semi-supervised learning methods are also used. The study showed that these techniques can be used alone or in combination to build more robust classifiers and that, without losing generality, these approaches are relatively successful in detecting fraud and credit scoring. They mentioned that fraud detection and data-mining-based credit scoring are subject to the same classification-related issues, such as feature engineering, parameter selection, and hyperparameter tuning. The authors also observed that fraud-related data are not abundant enough for investigators to train and test their models and that complex financial scenarios are nearly impossible to represent. They explained that fraud detection must constantly evolve, and it must particularly depend on the industry in which it is applied.

The authors of [27] performed a meta-analysis to establish the effect of mapping data samples from fraudulent companies to non-fraudulent companies using classification methods by comparing the general classification precision found in the literature. The results indicated that fraudulent samples could be matched equally to non-fraudulent samples (1:1 data mapping) or could be unevenly mapped using a one-to-many ratio to proportionally increase the sample size. Based on this meta-analysis, compared to statistical techniques, machine learning approaches can achieve better classification precision, specifically when the availability of sample data is low. Furthermore, high classification precision can even be obtained with a dataset with 1:1 mapping by using machine learning classification approaches.

The results mentioned by the authors of [28] clearly show that data mining techniques have been applied more widely for fraud detection in other fields, such as insurance, corporate, and credit card fraud. In this line, we found a lack of research on mortgage fraud, money laundering, and security fraud.

The main data mining techniques used for detecting financial fraud are logistical models that provide immediate solutions to the problems inherent in detecting and classifying fraudulent data. The authors of [29] conducted a review of the literature to address the following research questions related to financial statement fraud (FSF): (1) Can FSF be detected, how likely is it, and how can it be done? (2) What characteristics of the data can be used to predict FSF? (3) What kind of algorithm can be used to detect FSF? (4) How can detection performance be measured? (5) How effective are these algorithms in terms of detecting fraud? This work presents a generic framework to guide this analysis.

The reviews mentioned above have something in common: They try to unveil the main techniques used for fraud detection, such as machine learning methods (supervised, unsupervised, and semi-supervised), and try to identify which of these are more effective.

This analysis was carried out in different scenarios, contrasting the results obtained and specifying the study area in which they are most accurate. We could not find studies linking fraud detection by means of machine learning techniques and the Fraud Triangle Theory.

Finally, we find it important to comment on some theories for the understanding of fraud detection. Studies such as [15] analyzed the convergence and divergence of two classic theories of fraud: the triangle theory and the diamond theory. There, the concept of fraud and the convergence of the two classical theories were examined. This work also discussed the differentiation between them. In doing so, the similarities and differences between these theories were highlighted and appreciated. A discussion of the two approaches contributes to the understanding of fraud, especially for fraud professionals and fraud examiners.

1.2. Contribution

This research aims to compile the literature related to fraud detection from two perspectives. On the one hand, we analyze works that consider human behavior as an inherent risk factor in this problem, especially by using the FTT and FDT. Beyond exploring these theories, on the other hand, our review analyzes different works where machine learning techniques have been used for fraud detection. Moreover, we look for works that integrate ML techniques with behavior-based theories of fraud, such as the FTT and FDT.

To do this, we used the well-known methodology of Barbara Kitchenham and formulated three research questions. As a result, we provide an up-to-date and comprehensive analysis of the subject. It will help in identifying, investigating, and evaluating the causes that lead to fraud and in detecting it. This study can guide further research on the topic in areas that the investigation has not considered.

The rest of this paper is organized as follows. Section 2 addresses the methodology used to perform this review. Then, Section 3 summarizes our findings. After that, we discuss the weaknesses and strengths of the techniques identified in Section 4. Finally, Section 5 draws conclusions and describes future work.

2. Materials and Methods

A systematic literature review (SLR) was carried out for this research work. According to [25], the purpose of an SLR is to provide a complete list of all studies related to specific subject areas. Meanwhile, traditional reviews attempt to summarize the results of several studies. An SLR uses an evidence-based approach to meticulously search for relevant studies within a context to answer predefined research questions and select, evaluate, and critically analyze the findings in order to answer those research questions; this is done by following the recommendations reported in [30]. Considering the guidelines and recommendations described by Barbara Kitchenham [31], a systematic literature review must follow the methodological process illustrated in Figure 1.

2.1. Research Questions

As we stated, this article aims to review and summarize the works related to fraud detection that is performed by using machine learning techniques or the Fraud Triangle Theory. We do not restrict our search to any specific knowledge. The SLR research questions (RQs) that we intend to answer in this paper are the following:

1. RQ1: How can fraud be detected by analyzing human behavior by applying fraud theories?
2. RQ2: What machine or deep learning techniques are used to detect fraud?
3. RQ3: Using machine learning techniques, how can fraud cases be detected by analyzing human behavior associated with the Fraud Triangle Theory?

2.2. Keywords

We looked for scientific publications related to fraud detection, its process of identification, and its application to answering our research questions. We specifically targeted

works focused on fraud that relied on machine learning techniques or the Fraud Triangle Theory. To this end, we created a base list of keywords that was built from the keywords found in related research, as shown in Table 1.

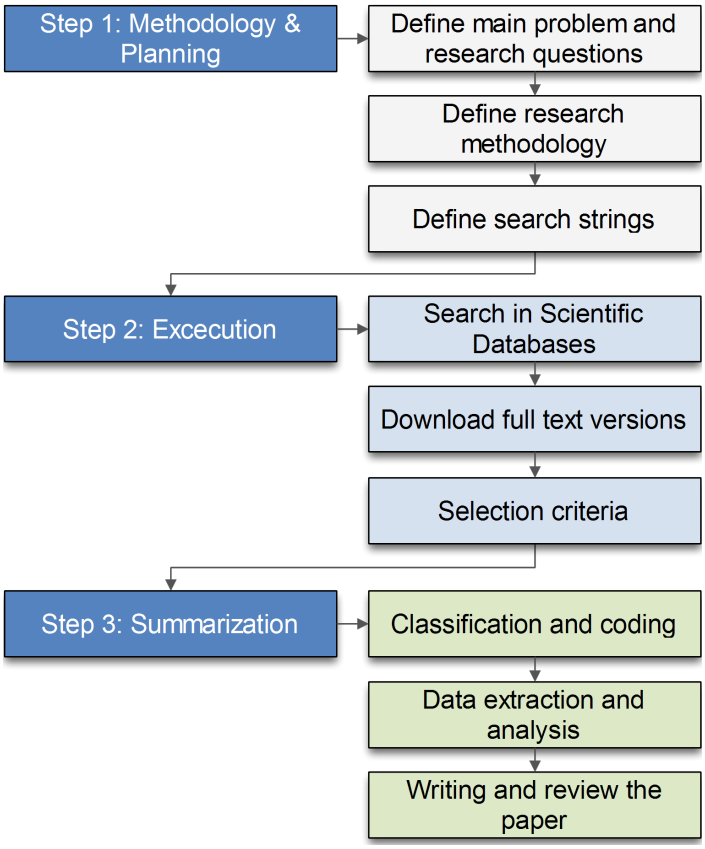

Figure 1. Methodology applied in the systematic literature review (SLR).

Table 1. Keywords.

Title 1	Title 2	Title 3
1	fraud	FR
2	fraud detection	FD
3	fraud triangle theory	FTT
4	fraud diamond theory	FDT
5	human behavior	HB
6	behavior patterns	BP
7	data mining	DT
8	machine learning	ML
9	deep learning	DL

2.3. Search Strategy

We employed the guidelines from [32,33] to define a search strategy in order to retrieve as many relevant documents as possible. Our search strategy is described below.

2.3.1. Search Method

To find the most relevant publications for the topic addressed in this work, we queried the following databases: IEEEXplore, ScienceDirect, ACM Digital Library, and Scopus. We chose these databases because they offer the most essential and high-impact full-text journals and conference proceedings that cover the ML and FD fields in general. We carried out the searches in the titles, keywords, and abstracts of articles using the combinations of terms introduced in the following section.

2.3.2. Search Terms

The search string was designed according to what was mentioned in [34]. Based on the research questions, we constructed the following relationships: ("Data mining" OR "Machine learning" OR "Deep Learning") AND ("Detection Fraud" OR "Internal Fraud" OR "Fraud Triangle" OR "Diamond Triangle" OR "Human Behavior"). All of these search terms were combined using "AND" operators to build the search string. The search terms in the string only matched the title, abstract, and keywords of the digital databases' articles. It is essential to find the correct search field or combination, be it the title, abstract, or full text, to apply in the search string and, thus, obtain effective results. In many cases, searching only by the "title" does not always provide the most relevant publications. Therefore, it can be necessary to include the "abstract" and, in other cases, "the complete document" of the related publications.

2.3.3. Selection of Papers

Since the searches in the articles' full text resulted in many irrelevant publications, we decided to apply the search criteria by incorporating the "abstracts" of the papers. This means that an article was selected as a potential candidate if its title or abstract contained the keywords defined in the search string. As a first filter, we evaluated each paper's title and abstract according to the inclusion and exclusion criteria (see Table 2). We selected the articles within the scope of the research questions. We thoroughly and entirely read the previously selected articles (which passed the first filter) as a second filter. Ultimately, the papers were included or excluded according to the inclusion and exclusion criteria. We will focus next on explaining the inclusion/exclusion criteria. Additionally, the search was limited to research written in English and published since 2010 [35].

Table 2. Inclusion/exclusion criteria.

No	Inclusion Criteria
IC1	Indexed publications not older than 10 years.
IC2	Scope of study: Computer Science
IC3	Primary studies (journal or articles).
IC4	Papers that discuss aspects regarding fraud detection.
IC5	The investigations considered have information relevant to the research questions.
No	**Exclusion Criteria**
EC1	Papers in which the language is different from English cannot be selected.
EC2	Papers that are not available for reading and data collection (papers that are only accessible by paying or are not provided by the search engine) cannot be selected.
EC3	Duplicated papers cannot be selected.
EC4	Publications that do not meet any of the inclusion criteria cannot be selected.
EC5	Publications that do not describe scientific methodology cannot be selected.

2.4. Study Selection

As shown in Figure 2, the selection of studies was performed through the following processes [36]:

1. Identification: The keywords were selected from the databases listed above according to the research questions mentioned in the search method section. The search string was applied only to the title and abstract, as a full-text search would produce many irrelevant results [37]. The search period went from 2010 to 2021.
2. Filter: All possible primary studies' titles, abstracts, and keywords were checked against the inclusion and exclusion criteria. If it was difficult to determine whether an article should be included or not, it was reserved for the next phase.
3. Eligibility: At this stage, a complete reading of the text was carried out to determine if the article should be included according to the inclusion and exclusion criteria.

4. Data extraction: After the filtering process, data were extracted from the selected studies to answer RQ1–RQ3.

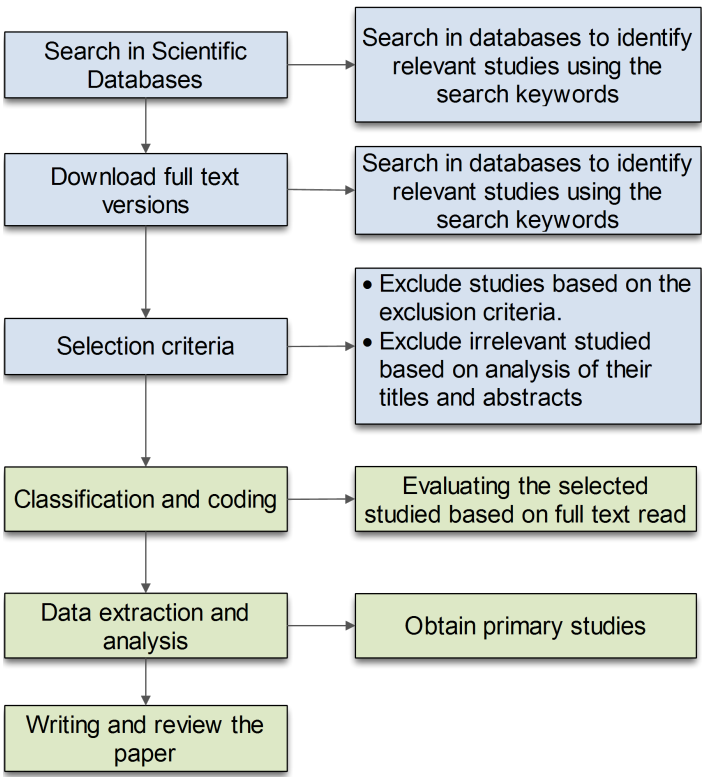

Figure 2. Process of the selection of studies.

2.5. Quality Assessment

Once we selected several primary studies based on the inclusion and exclusion criteria, we assessed their quality. Following the guidelines in [36], three quality assessment (QA) questions were defined to measure the research quality of each proposal and to provide a quantitative comparison between the research works considered. The criteria were based on three quality assessment (QA) questions:

1. Are the topics covered in the article relevant for fraud detection? Yes: It explicitly describes the topics related to fraud detection by applying ML techniques through the FTT. Partially: Only a few are mentioned. No: It neither describes nor mentions topics related to fraud detection using ML techniques through the FTT.
2. Were the limitations for the study of fraud detection detailed? Yes: It clearly explained the limitations related to fraud detection by applying ML techniques through the FTT. Partially: It mentioned the limitations but did not explain why. No: It did not mention the limitations.
3. Did the study address systematic research? Yes: The study was developed systematically and applied an adequate methodology to obtain reliable findings. Partially: The study was developed systematically and used a proper methodology but did not provide details. No: The study was not explained in a clear way and the authors did not apply an adequate methodology.

The scoring procedure was defined as follows: Y (Yes = 1), P (Partially = 0.5), N (No = 0), or Unknown (i.e., the information was not specified).

2.6. Data Extraction and Analysis

This section describes the data extraction process performed with the selected papers and the analysis of the data extracted in order to answer the research questions of this SLR. We extracted the required data from previously selected works that were accordingly

classified to answer the research questions, as shown in Table 3. The data extraction form used for all selected primary studies is indicated in order to carry out an in-depth analysis.

Table 3. Data extraction form.

No	Extracted Data	Description	Type
1	Identity of the study	Unique identity for the study	General
2	Bibliographic references	Authors, year of publication, title, and source of publication	General
3	Type of study	Book, journal paper, conference paper, workshop paper	General
4	The theories employed	Description of the detection of fraud by applying the FTT and HB	RQ1
5	The techniques considered	Description of the detection of fraud by applying ML/DM techniques	RQ2
6	Combination of techniques and theories used	Description of the analysis of theories and techniques used to detect fraud	RQ3
7	Findings and Contributions	Indication of the findings and contributions of the study	General

We extracted the most representative papers related to the research questions based on the search string and associated terms. The results of the analysis of the data obtained are presented in the next section.

2.7. Synthesis

Many papers could contain keywords that were used in the search string, but they could be irrelevant to our research questions. Therefore, a careful selection of documents should include only those containing helpful information with respect to the research approach and the answers to the different research questions. As shown in Figure 3, we first searched each data source separately in order to later join the results obtained from the various sources of information, resulting in a total of 1891 papers. We obtained the most articles from Scopus, representing around 50% of all documents.

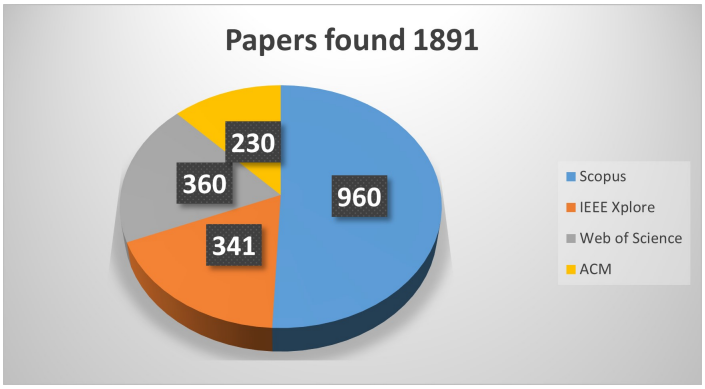

Figure 3. Studies retrieved through search engines.

Table 4 shows the number of articles found per source according to the search for keywords related to the search strings in the selected databases. The second column shows the results of the initial selection of papers found in each source. Below is the number of articles that were chosen after removing the exclusion criteria. The number of articles that were selected after eliminating duplicate articles is presented in the fourth column. Finally, the papers from each source that were selected after completing the inclusion process are presented.

It was necessary to refine the papers obtained by previously eliminating irrelevant studies to ensure that the works complied with the established selection criteria. Our search in the databases, the application of the search string to only the titles and abstracts of the articles, and the selection of articles that were published during the last eleven years yielded 1891 records. After using the exclusion criteria on these records, we obtained 254 studies. The analysis of the duplicity of such studies enabled us to find 106 papers that were relevant for a full-text review. Finally, after a full-text assessment, 32 studies [38–69] were identified as a result of the analysis through the SLR technique. Therefore, a total of

32 publications met all of the inclusion criteria. The selection of studies from the initial search identification phase and the final number of included studies are presented in Figure 4. As initially proposed and to ensure that the resulting reviews contained relevant information, we read the full text of the 32 studies to verify if they fit our adopted selection criteria. As a result, all of these publications represented our final set of primary studies.

Table 4. Number of papers found through the selection process.

Source	Papers Found	Abstract and Title	Duplicity	Selected
Scopus	960	77	48	16
IEEE	341	68	31	7
WoC	360	61	16	9
ACM	230	48	11	4
Total	1891	254	106	32

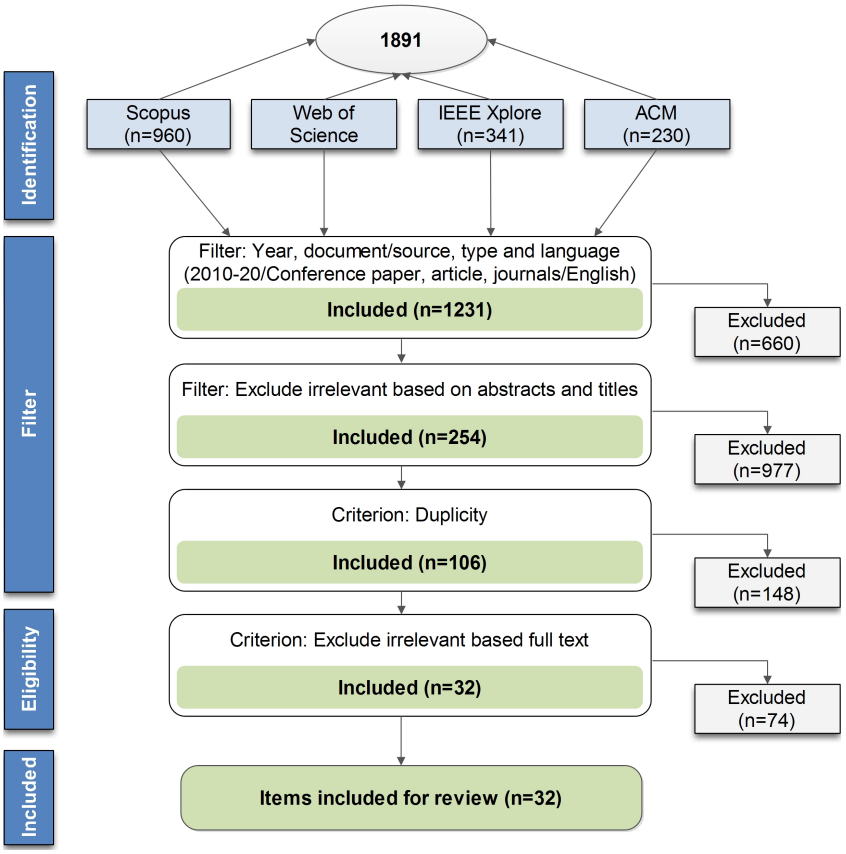

Figure 4. Steps followed to narrow the search results.

Regarding the types of publications where the selected papers were available, we found that 50% of them had been published in conferences and 50% in journals.

Table 5 shows the number of citations of the selected articles. The data presented (column cited) provide only an approximation of the citation rates and are not intended for comparisons among studies.

Regarding the period of publication of the selected articles, 32 studies were published between 2010 and 2021. Furthermore, as shown in Figure 5, 2010, 2015, 2016, and 2017 had the most significant numbers of articles, while 2011, 2012, 2019, and 2020 had the lowest numbers.

Table 5. Numbers of selected studies by type.

#	Cited	#	Cited	#	Cited	#	Cited
[38]	905	[48]	6	[58]	43	[68]	954
[39]	16	[49]	6	[59]	23	[55]	6
[40]	20	[50]	431	[60]	258		
[41]	3	[51]	9	[61]	5		
[42]	55	[52]	0	[62]	133		
[43]	18	[53]	16	[63]	90		
[70]	120	[54]	55	[64]	29		
[45]	11	[65]	7	[46]	22		
[56]	7	[66]	3	[47]	22		
[57]	209	[67]	4	[69]	6		

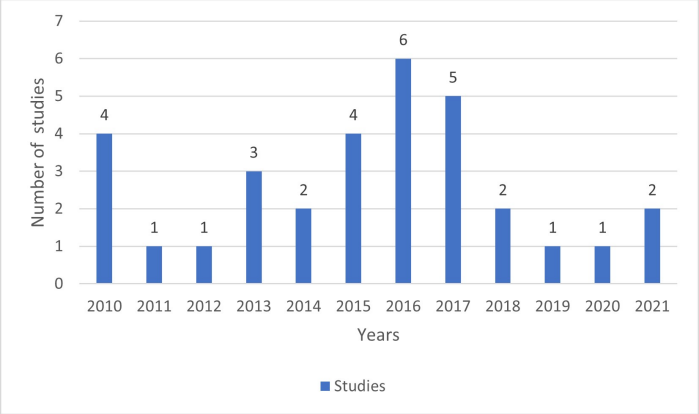

Figure 5. Number of articles by year of publication.

3. Results

As the result of our methodology, we found 32 documents that were published between 2010 and 2021 that covered the most representative work on the topic of this paper. We focused only on peer-reviewed papers from journals and conferences. All of them were obtained as a result of searching for fraud-related topics in four scientific libraries. Table 6 shows a matrix built using the topics most closely related to the research questions and with references to the corresponding articles. As can be seen, each column identifies a relevant topic associated with the research questions. We can see that seven works were found for RQ1(Fraud Detection + Human Behavior + Fraud theory). In contrast, for RQ2 (Fraud Detection + ML/DM techniques), 24 works were found, while for RQ3 (Fraud Detection + Human Behavior + ML/ DM + Fraud theory), only one study was found. So, it looks like there is room for improving fraud detection because RQ3 brings together most of the topics established in the other research questions.

Table 6. Data extraction form.

#	Ref	Fraud Detection	Human Behavior	ML/DM Techniques	Fraud Theory
1	[38]	RQ1	RQ1		RQ1
2	[39]	RQ1	RQ1		RQ1
3	[40]	RQ1	RQ1		RQ1
4	[41]	RQ1	RQ1		RQ1
5	[42]	RQ1	RQ1		RQ1
6	[43]	RQ1	RQ1		RQ1
7	[70]	RQ1	RQ1		RQ1
8	[45]	RQ2		RQ2	
9	[46]	RQ2		RQ2	

Table 6. *Cont.*

#	Ref	Fraud Detection	Human Behavior	ML/DM Techniques	Fraud Theory
10	[47]	RQ2		RQ2	
11	[48]	RQ2		RQ2	
12	[49]	RQ2		RQ2	
13	[50]	RQ2		RQ2	
14	[51]	RQ2		RQ2	
15	[52]	RQ2		RQ2	
16	[53]	RQ2		RQ2	
17	[54]	RQ2		RQ2	
18	[55]	RQ2		RQ2	
19	[56]	RQ2		RQ2	
20	[57]	RQ2		RQ2	
21	[58]	RQ2		RQ2	
22	[59]	RQ2		RQ2	
23	[60]	RQ2		RQ2	
24	[61]	RQ2		RQ2	
25	[62]	RQ2		RQ2	
26	[63]	RQ2		RQ2	
27	[64]	RQ2		RQ2	
28	[65]	RQ2		RQ2	
29	[66]	RQ2		RQ2	
30	[67]	RQ2		RQ2	
31	[68]	RQ2		RQ2	
32	[69]	RQ3	RQ3	RQ3	RQ3

Table 7 shows the frequencies of the works found vs. the research question. As can be seen, RQ2 is the most frequently investigated. It accounts for 88.46%. Only one paper was found for RQ1, accounting for 3.84%, and RQ3 accounts for 7.69%.

Table 7. Data extraction form.

RQ	Study Identifier	Frequency	Percentage
1	[38–43,70]	7	21.88
2	[45–68]	24	75
3	[69]	1	3.13

3.1. RQ1: How Can Fraud Be Detected by Analyzing Human Behavior by Applying Fraud Theories?

This section details the results obtained from the analysis of research papers that relate fraud detection with the point of view of human behavior by applying the Fraud Triangle Theory. The investigation is intended to answer RQ1. We answer this question through a statistical analysis of the number of documents linked to the research question. According to Table 6, seven works were found. Hoyer et al. [38] proposed a prototype in a generic architectural model that considers the factors of the fraud triangle. In this way, in addition to the analysis applied as part of a traditional fraud audit, human behavior is considered. By doing this, the transactions examined by an auditor can be better differentiated and prioritized. Behavioral patterns are found through the incorporation of the human factor. These patterns appear in multiple sources of information, especially in users' data, such as in e-mails, messages, network traffic, and system records from which evidence of fraud can be extracted.

Sanchez et al. [39] presented a framework that allows the identification of people who commit fraud and is supported by the Fraud Triangle Theory. This proposal is based on the use of a continuous audit that is installed on user devices, collects information from agents, and employs the collection of phrases. They are subsequently analyzed to identify fraud patterns through the analysis of human behavior and the treatment of the

results. In [40], based on primary data on the behavior of perpetrators who commit fraud, the authors showed the complementarity between an ex-post analysis and the existing literature on this topic. They suggested that the presence or absence of fraudulent intent can be assessed by scrutinizing human behavior. Mackevicius and Giriunas [41] analyzed the Fraud Triangle Theory and presented its associated elements: "motives, possibilities, pressure, rationalization, incentive, and others". They offered a theoretical analysis of the fraud scales and their elements: motives, conditions, possibilities, and performance. To this end, the authors analyzed 265 respondents—including accountants, stakeholders, public officials, and inspectors in Central Java, Indonesia—by using structural equation modeling (SEM) with the AMOS analysis tools. In [42], the authors assessed the Fraud Triangle Theory and human behavior in order to study the factors of opportunity, financial processes, and rationalization. The authors emphasized the importance of psychological and moral aspects. The International Auditing Standard AI240 focuses on the auditor's responsibility to assess fraud in an audit of financial statements. The authors of [43] explored if the standard has been used effectively in Indonesia based on the proposed fraud indicators through a fraud analysis. A questionnaire survey was conducted with three groups of auditors: external, internal, and government auditors. This study examined auditors' perceptions of the importance and existence of warning signs of financial fraud by using the fraud diamond. The findings indicate that the auditors were able to identify these red flags by giving them high scores. On the contrary, regarding the "level of use", the scores were low.

Mekonnen et al. [70] presented an insider threat prevention and prediction model based on the fraud diamond by combining various approaches, techniques, and IT tools, as well as criminology and psychology. The deployment of this model involved the collection of information about possible intentions by using privileged information within a context of preserving privacy, thus enabling high-risk insider threats to be identified while balancing privacy concerns.

3.2. RQ2: What Machine or Deep Learning Techniques Are Used to Detect Fraud?

This section reports the results of works that described the implementation of machine learning and data analysis for fraud detection. We aimed to identify the most commonly used machine or deep learning techniques in this realm. Table 7 shows that this research question had the highest number of related works. Table 8 presents the main focus of the articles and the ML/DL techniques used, as well as the dataset information. All of these articles are summarized below.

There are works that enhance traditional security approaches. In [60], the need to use the Process Information Systems (PAIS) software in organizations and the importance of fraud detection were investigated. They claimed that this tool is a must for organizations, as its flexibility raises fraud detection. The authors of [63] sought to design an artifact (hardware) for detecting communications from disgruntled employees through automated text mining techniques. The artifact that they developed extended the layered approach in order to combat internal security risks. They claimed that this phenomenon can be detected in e-mail repositories by using employee dissatisfaction as the primary indicator of fraud risk. Considering the methods of fraud detection based on simple comparisons, detection of associations, clustering, perdition, and outliers, an automated fraud-detection framework was proposed in [47]. The framework allowed fraud identification by using intelligent agents, data fusion techniques, and various data mining techniques. In [67], the authors proposed the detection of bank fraud through data extraction techniques, association, grouping, forecasting, and classification to analyze customer data to identify patterns leading to fraud. To conclude this group of papers, West et al. suggested that a higher level of verification/authentication can be added to banking processes by identifying patterns. To do this, the authors reviewed key performance metrics used to detect financial fraud, with a focus on credit card fraud. They compared the effectiveness of these metrics to detect if fraud was carried out. In addition, the performance of the application of various

computational intelligence techniques to this problem's domain was also investigated, and the efficacy of different binary classification methods was explored.

Table 8. Summary of works that used machine or deep learning techniques to detect fraud.

Ref.	Techniques [a]	Dataset	Main Focus
[45]	NN, DT, BN	N/A	Summarized and compared different datasets and algorithms for automated accounting fraud detection.
[46]	RF	Financial and non-financial data	Presented a hybrid detection model using machine learning and text mining methods for detecting financial fraud.
[47]	KDD	N/A	Automated fraud detection framework that allows fraud identification using intelligent agents, data fusion techniques, and data mining techniques.
[48]	KM	UCI Machine Learning Repository [71]	Modified k-means clustering algorithm for detecting outliers and removing them from the dataset to improve grouping precision.
[49]	C.45, KM, SVM, NB, CART	N/A	Categorized the different types of fraud and explained the best available data mining techniques.
[50]	NN	N/A	Used neural networks to correlate information from a variety of technologies and database sources to identify suspicious account activity.
[51]	KM Clustering and AdaBoost Classifier	Worldline and the Université Libre de Bruxelles	Presented a study on the use of clustering and classifier techniques and compared their precision for fraud detection.
[52]	SVM, ANN	Indonesian stock exchange (IDX)	Through the application of data mining algorithms, such SVM and ANN, the essential indicators for detecting financial fraud are profitability and efficiency.
[53]	MLR, SVM, and BN	N/A	Development of three multiple-class classifiers—MLR, SVM, and BN—as well as predictive tools for detecting and classifying misstatements according to the presence of intent of fraud.
[54]	MLFF, SVM, GP, GMDH, LR, PNN	N/A	Used data mining techniques that were tested on a dataset involving 202 Chinese companies and compared them with and without the selection of functions.
[55]	BLR, SVM, NN, ensemble techniques, and LDA	10-K financial reports of documents (EDGAR)	For fraud detection in financial reporting, various techniques of natural language processing, and supervised machine learning are applied.
[56]	ANN	[72]	Identified a person of interest from a published corpus of Enron email data for research.
[57]	LR, NN, SVM, BN, DT, AdaBoost, and LogitBoost	[71]	Method based on Grammatical Genetic Programming (GBGP) through multi-objective optimization and set learning. They compared the proposed method with LR, NN, SVM, BN, DT, AdaBoost, and LogitBoost on four FFD datasets.
[58]	LR, ANN, KNN, SVM, Decision Stem, M5P Tree, J48 Tree, RF, and Decision Table	N/A	Explored the use of data mining methods to detect electronic ledger fraud through financial statements.
[59]	DRL	N/A	Applied DRL theory through two applications in banking and discussed its implementation for fraud detection.
[60]	Petri-Net, Heuristic	N/A	Used the Process Information Systems (PAIS) software in organizations for fraud detection.
[61]	DT, NB	N/A	Credit card fraud detection using supervised learning algorithms.
[62]	Luhn's and Hunt's	N/A	System that detects fraud in the processing of credit card transactions.
[63]	NB	Email data	Designed an artifact (hardware) for detecting communications from disgruntled employees using automated text mining techniques.
[64]	MLCC	International financial service provider	Analyzed the use of a data mining approach in order to reduce the risk of internal fraud.
[65]	CNN, SLSTM, hybrid of CNN–LSTM.	Card transactions from an Indonesian bank	Explored three deep learning models for the recognition of fraudulent card transactions.
[66]	DT, RF, NB	Twitter and Facebook	Implementation of the document grouping algorithm as a set of classification algorithms along with appropriate industry use cases.
[67]	Association, clustering, forecasting, and classification	N/A	Detection of bank fraud through the use of data mining techniques.
[68]	GP, NN, SVM	UCSD-FICO	Key performance metrics used for Financial Fraud Detection (FFD) with a focus on credit card fraud.

[a] Neural Networks: NN; Decision Trees: DT; Bayesian Networks: BN; Random Forest: RF; K-means: KM; Support Vector Machine: SVM; Artificial Neural Network: ANN; Multinomial Logistic Regression: MLR; Multilayer Direct Feed Neural Network: MLFF; Genetic Programming: GP; Group Method of Data Management: GMDH; Logistic Regression: LR; Probabilistic NN: PNN; Binomial Logistic Regression: BLR; Latent Dirichlet Assignment: LDA; K-Nearest Neighbor: KNN; Deep Reinforcement Learning: DRL; Multivariate Latent Class Clustering: MLCC; Convolutional Neural Network: CNN; Stacked Long Short-Term Memory: SLSTM; Naive Bayes: NB.

In [45], the authors summarized and compared different datasets and algorithms for automated accounting fraud detection. The selected works addressed mining algorithms that included statistical tests, regression analysis, NN, DT, BN, stack variables, etc. Re-

gression analysis was widely used to hide data. Generally, the effect of detection and the precision of NN were higher than those of regression models. The overall conclusion was that pattern detection is better than detection by an unaided auditor. Due to the small size of the fraud samples, some publications reached decisions based on training samples and may have overestimated the effects of the models. In [46], S. Wang presented a hybrid detection model using machine learning and text mining methods for detecting financial fraud. This model used financial and non-financial data and employed two ways of selecting easy-to-explain characteristics. During the investigation, the author chose 120 fraudulent financial statements disclosed by the China Securities Regulatory Commission (CSRC) between 2007 and 2016. He compared the performance of five machine learning methods and found that the Random Forest method had the following advantages: (1) It is suitable for processing high-dimensional data; (2) it avoids overfitting to some extent; (3) it is robust and stable. Ravisankar et al. proposed the use of data mining techniques to identify companies that resort to financial statement fraud [54]. Specifically, the authors tested the MLFF, SVM, GP, GMDH, LR, and PNN techniques. The evaluation considered the role of feature selection and relied on a dataset involving 202 Chinese companies. Their results indicated that the PNN outperformed all of the methods without feature selection, and the GP and PNN outperformed others with feature selection and marginally equal precisions.

For other works that compared different ML methods, we found the following. In [53], the authors developed three multiple-class classifiers (MLR, SVM, and BN) to detect and classify misstatements according to the presence of fraud intent. Using the MetaCost tool, the authors conducted cost-sensitive learning and solved class imbalance and asymmetric misclassification costs. In [58], the use of data mining methods to detect fraud in electronic ledgers through financial statements was explored. The Linear Regression, ANN, KNN, SVM, Decision Stem, M5P Tree, J48 Tree, RF, and Decision Table techniques were used for training. The authors of [61] detected credit card fraud by using supervised learning algorithms, such as a DT and NB.

Focusing on the use or comparison of ANNs with other methods, Vimal Kumar et al. [49] analyzed the challenges of detecting and preventing fraud in the banking industry when having insider information. The authors reviewed some of the data analysis techniques for detecting insider trading scams. Their work lists the best data mining techniques available (NN, DT, and Bayesian Belief Networks), which have been proposed by many researchers and employed in different industries. They concluded that the banking industry's primary requirements are fraud detection and prevention and that data mining techniques can help reduce fraud cases. In addition, the work in [50] proposed the use of NN to correlate information from a variety of technological sources and databases in order to identify suspicious account activity. The work in [52] applied data mining algorithms, such as a SVM and ANNs, to detect financial fraud. The authors stated that the essential indicators of financial fraud are profitability and efficiency. The incorporation of these factors improved the accuracy of the SVM algorithm to 88.37%. The ANNs produced the highest precision, 90.97%, for data without feature selection. In [56], Mohanty et al. aimed to identify a person of interest from the corpus of Enron email data released for research. They tried to detect fraudulent activities by means of an ANN with the activation functions of the Adam optimizer and ReLU. Their work achieved high precision in terms of recall, accuracy, and F1 score.

Regarding unsupervised approaches, a proposal to detect outliers using a modified K-Means Clustering algorithm was presented in [48]. For this work, the detected outliers were removed from the dataset to improve the grouping precision. They also validated their approach against existing techniques and benchmark performance. The authors of [51] presented a study on the use of K-Means Clustering and the AdaBoost Classifier, comparing their accuracies and performances with an analysis of the past and present models used for fraud detection.

Regarding the use of more sophisticated techniques for the problem of fraud detection in financial reporting, the authors of [55] applied various natural language processing techniques and supervised machine learning, including BLR, SVM, NN, ensemble techniques, and LDA. They applied Latent Dirichlet Allocation (LDA) to a collection of 10-K financial reports of documents available in the EDGAR database of the United States Security and Exchange Commission to generate a frequency matrix of documents and topics. In addition, they applied evaluation metrics, such as the accuracy, receiver performance characteristic curve, and area under the curve, to evaluate the performance of each algorithm. For the resolution of problems for FFD, Li and Wong, [57] proposed a new method based on GBGP through multi-objective optimization and set learning. They compared the proposed method with LR, NN, SVM, BN, DT, AdaBoost, bagging, and LogitBoost in four FFD datasets. The results showed the efficacy of the new approach on the given FFD problems, including two real-life situations. The authors of [59] applied the theory of DRL through two applications in banking and discussed its implementation for fraud detection. Using a DT with a combination of the Luhn algorithm and the Hunt algorithm, Save et al. [62] proposed a system that detects fraud in the processing of credit card transactions. The validation of the card number is done through the Luhn algorithm. The authors of [64] focused on the detection of external fraud. The use of a data mining approach in order to reduce the risk of internal fraud was also discussed. Consequently, a descriptive data mining strategy was applied instead of the widely used prediction data mining techniques. The authors employed a multivariate latent class clustering algorithm for a case firm's procurement data. Their results suggested that their technique helps to assess the current risk of internal fraud.

Exploring a deep learning model to learn short- and long-term patterns from an unbalanced input dataset was an objective set by [65]. The data obtained were transactions of an Indonesian bank in 2016–2017 with binary labels (no fraud or fraud). They also explored the effects of sample ratios of non-fraud to fraud from 1 to 4 and three models: a convolutional neural network (CNN), short-term/long-term stacked memory (SLSTM), and a CNN–LSTM hybrid. Using the area under the ROC curve (AUC) as the model performance metric, the CNN achieved the highest AUC for R = 1, 2, 3, 4, followed by the SLSTM and CNN–LSTM. The authors of [66] proposed the implementation of both the document clustering algorithm and a set of classification algorithms (DT, RF, and NB), along with industry-appropriate use cases. In addition, the performance of three classification algorithms was compared by calculating the "Confusion Matrix", which, in turn, helped us calculate performance measures such as "accuracy", "precision", and "recovery".

3.3. RQ3: Using Machine Learning Techniques, How Can Fraud Cases Be Detected by Analyzing Human Behavior Associated with the Fraud Triangle Theory?

We found only one work related to this research question. This means that we obtained few results when we tried keywords related to the topics most relevant to the research questions (Fraud Detection + Human Behavior + Machine Learning Techniques + Fraud Triangle Theory). Therefore, the combination of ML techniques and theories related to fraud needs further investigation because it would integrate two knowledge fields (psychology and data science) in order to improve fraud detection. In [69], the authors examined the aspects of the fraud triangle using data mining techniques in order to evaluate attributes such as pressure/incentive, opportunity, and attitude/rationalization, and, through the use of expert questionnaires, they discussed whether their suggestion agreed with the results obtained with the adoption of those techniques. The data extraction methods used in this research included logistic regression, decision trees (CART), and artificial neural networks (ANNs). They also compared data mining techniques and expert judgments. The ANNs and CART achieved training samples of 91.2% (ANN) and 90.4% (CART), and they were tested with correct classification rates of 92.8% (ANN) and 90.3% (CART), which were more precise than those of logistic models, which only reached 83.7% and 88.5% of correct classification in the assessment of the presence of fraud.

3.4. Quality Assessment

Once the QA questions were defined, we evaluated the primary studies identified in the SLR. The score assigned to each study for each question is shown in Table 9.

Table 9. Quality assessment.

#	QA-1	QA-2	QA-3	Total Score	Max S
[38]	P	P	Y	2	66.67
[39]	P	P	Y	2	66.67
[40]	N	N	N	0	0
[41]	P	Y	Y	2	66.67
[42]	N	N	N	0	0
[43]	N	N	N	0	0
[70]	P	P	Y	2	66.67
[45]	P	Y	Y	2.5	83.33
[46]	P	Y	Y	2.5	83.33
[47]	N	N	N	0	0
[48]	P	P	Y	2	66.67
[49]	P	Y	Y	2.5	83.33
[50]	P	P	Y	2	66.67
[51]	P	P	Y	2	66.67
[52]	P	P	Y	2	66.67
[53]	P	P	Y	2	66.67
[54]	N	N	N	0	0
[55]	P	P	Y	2	66.67
[56]	P	Y	Y	2.5	83.33
[57]	P	Y	Y	2.5	83.33
[58]	N	N	N	0	0
[59]	P	P	Y	2	66.67
[60]	P	Y	Y	2.5	83.33
[61]	N	N	N	0	0
[62]	N	N	N	0	0
[63]	P	Y	Y	2.5	83.33
[64]	0	0	0	0	0
[65]	P	P	Y	2	66.67
[66]	N	N	N	0	0
[67]	P	Y	Y	2.5	83.33
[68]	P	Y	Y	2.5	83.33
[69]	P	Y	Y	2.5	83.33
Total	10.5	16.5	22	49	
Max QA	21.42	33.68	44.9	100	
Total Score	47.62	73.81	100		

The total of the accumulated scores from the QA questions can be observed in the "Total Score" row, showing that QA3 has 22 points, corresponding to 44.9%, demonstrating that this question was more representative in the review. QA2 followed this with 33.68%, and QA1 followed with 21.42%. On the other hand, the last row identifies the percentage of points collected by the values assigned for a given QA question with respect to the points obtained if each selected study received the highest score. Refs. [45,46,49,56,57,60,63,67,69] obtained the highest score of 2.5, which represents 83.33% of the maximum score that a preliminary study could obtain; on the other hand, Refs. [38,39,41,44,48,50–53,55,59,65] obtained a score of 2, that represents 66.67% of the maximum score. Refs. [40,42,43,47,54,58, 61,62,64,66] failed to get any scores, which means that their title and abstract showed that they could answer the research question for this SLR, but after reviewing the full articles, no features related to fraud detection using machine learning techniques were discussed.

4. Discussion

In this work, we have reviewed contributions related to fraud detection, with a special emphasis on those addressing fraud detection from the perspective of the modeling of human behavior.

Applying techniques related to the analysis of human behavior allowed us to consider behavioral factors that could empower the detection of unusual transactions that would not have been considered if using traditional auditing methods. By observing people's behavior, it can be seen that the human factor is closely related to the Fraud Triangle Theory.

On the other hand, the use of machine learning techniques to detect fraud was also implemented in several works to predict behaviors related to this phenomenon. As a result of our research, a significant number of articles (24) addressed this approach. In this context, we found that mainly supervised and unsupervised algorithms are used for fraud-detection analysis. The supervised strategy enables the blocking of fraud attempts based on fraudulent and non-fraudulent samples. This is used in rule-based detection, which automatically infers discriminatory rules from a labeled training set. In addition, regarding fraud detection, our research unveiled that supervised algorithms regularly have to deal with unbalanced classes, which might result in poor detection. Furthermore, these techniques are unable to identify new fraud patterns. Unsupervised learning, however, concentrates on the discovery of suspicious behavior as a proxy of fraud detection and, thus, does not require prior knowledge about verified fraudulent cases.

Our review focuses on fraud detection performed by means of machine learning techniques or through analysis of human behavior based on the Fraud Triangle Theory. By answering three research questions, we tried to unveil how both approaches are addressed in the literature and how they may be jointly applied.

By answering RQ1, keywords such as human behavior and theories related to fraud were linked, resulting in several related studies. The answer to RQ2 linked machine learning techniques with fraud detection; this question was the one that generated the most results. The analyzed questions each produced results in a specific field, but when trying to combine these fields by answering RQ3, we did not find works linking fraud detection by means of machine learning techniques with any theory related to fraud.

Despite the existence of works about detecting fraud in the areas of data mining and fraud theories, no literature reviews that jointly covered these two areas were identified. Table 10 presents a comparative summary of seven relevant SLRs and surveys performed in the area of fraud detection, including our contribution.

Table 10. Comparison of related systematic literature reviews.

SLR Work	Year	Context	Period	Data Sources	# of Screened Works/ Primary Studies	Quality Assessment of Primary Studies
[25]	2010	Data-mining-based fraud detection	2000–2010	N/A	N/A	No evaluation criteria applied
[73]	2020	Fraud-detection metrics in business processes	N/A	1, 4, 5, 7, 9, 14	12,000/75	No well-defined evaluation criteria applied
[26]	2018	Data-mining-based fraud detection and credit scoring	N/A	N/A	N/A	No evaluation criteria applied
[74]	2020	Graph-based anomaly-detection approaches	2007–2018	1, 2, 5, 9	585/39	No evaluation criteria applied
[75]	2019	Fraud Triangle Theory	No specific	7	1169/33	Based on evaluation criteria proposed by authors
[28]	2011	Data mining techniques in financial fraud detection	1997–2008	1, 2, 5, 9, 11, 12, 13	1200/49	No well-defined evaluation criteria applied
[29]	2007	Data-mining-based financial fraud detection	N/A	N/A	N/A	No evaluation criteria applied
This SLR	2021	Fraud detection using the Fraud Triangle Theory and data mining techniques	2010–2021	1, 2, 4, 10	1891/32	Based on evaluation criteria proposed by [76]

1: IEEE Xplore; 2: ACM DL; 3: Engineering Village (Compendex); 4: ISI Web of Science; 5: ScienceDirect; 6: Wiley Inter Science Journal; 7: Google Scholar; 8: Citeseer; 9:Springerlink; 10: Scopus; 11: Business Source Premier (EBSCO); 12: Emerald Full Text; 13: World Scientific Net; 14: ProQuest.

In the "Context" column of Table 10, there are four SLRs that are exclusively related to some aspect of data mining [25,26,28,29], while only one is related to some aspect of fraud theory [75], in addition to other approaches [73,74]. The last row of Table 10 also presents information about the SLR covered in this document, the context of which explores both data mining and fraud theories together, unlike the other seven presented in this table. These SLRs were published between 2007 and 2020, with the novelty that some of them [26,29,73] do not mention the related search period. The research periods of [25,28,74] range from 10 to 11 years, but include primary studies without making cuts in any specific year. Some works do not specify the sources of data, and those doing so report a variable number of data sources. Studies that mention data sources do not clearly explain their reasons for selecting them. On the other hand, for our research, four data sources were chosen to maximize the probability of identifying relevant candidate works as primary studies.

Both the number of candidate articles from the data sources and the number of selected primary studies are presented in this table for each SLR. The differences in these numbers may be related to the context of each investigation, e.g., data sources used, keywords, etc. For our SLR, the number of reviewed works resulted from the searches in the different data sources used in combination with the chosen keywords, while the final number of primary studies was similar to those of other works. It should be noted that there are works that do not mention this metric.

Although quality evaluation is not a mandatory parameter in the structure of an SLR, according to [76], it is an essential contribution in this type of work in order to improve its quality. None of the analyzed works clearly showed how an evaluation was carried out in this regard. No criteria were mentioned for assessing the quality of the primary studies. Our work was based on the evaluation criteria proposed by [77].

5. Conclusions and Future Work

Fraud detection is complex, as it requires the interpretation of human behavior, but this is not the only issue. The lack of data available for training or testing detection models significantly complicates the assessment of detection strategies. Even when data are available, unbalanced datasets are the norm in this domain.

Accordingly, there are very different approaches that tackle the problem of fraud detection, as well as systematic literature reviews that are intended to address these limitations from a more global perspective. Thus, the purpose of this research was to identify publications related to fraud detection through the use of ML techniques based on the Fraud Triangle Theory. The proposed reference frameworks focus on developing tools that allow auditors to perform fraud analyses more efficiently by shortening their detection time through support from data mining techniques. Most of the works concentrate on carrying out their analyses after fraud has been carried out in an attempt to shorten the time taken to find results; thus, these proposals are reactive to such events.

Through this research, it was found that there are a significant number of research projects that are being carried out in this specific area of fraud detection; in general, they have a solid level of maturity. The large number of publications in conferences and journals—representing 50% and 50% of primary studies, respectively—is substantial proof. In addition, the results of the quality evaluation carried out for the primary studies showed that the evaluation of their proposals was satisfactory in terms of the criteria of "relevance", "limitations", and "methodology". When we assumed an approach to fraud detection through data mining techniques and the use of fraud theories associated with human behavior, this SLR reveals very little evidence from studies supporting this approach, since only one primary study was found, corresponding to 3.13% of the studies. When we allowed partial coverage, that is, fraud detection by applying only data mining techniques, 24 primary studies (corresponding to 75%) could be classified. On the other hand, when we analyzed the approach to the analysis and detection of fraud in which only theories related to fraud that were associated with human behavior were considered, seven primary studies (corresponding to 21.88%) were found to support this approach.

In this sense, only one study with evidence of the use of data mining techniques, the application of fraud theories, and a corresponding analysis of human behavior to detect fraud was identified, which means that there is a gap, and this is an appropriate field to investigate.

As future work, it is proposed that a review focused on detecting fraud and incorporates an analysis of the availability of data and the lack of access to this resource, including other data sources as possible alternatives, should be carried out.

Author Contributions: Conceptualization, M.S.-A. and L.U.-A.; methodology, M.S.-A. and J.E.-J.; validation, M.S.-A., L.U.-A. and J.E.-J.; investigation, M.S.-A.; writing—original draft preparation, M.S.-A.; writing—review and editing, L.U.-A. and J.E.-J.; supervision, L.U.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy limitations concerning the use of personal information.

Acknowledgments: This work was partially supported by Escuela Politécnica Nacional under the research project PII-DETRI-2021-02 "Detección de fraude mediante análisis de tópicos y métodos de clasificación". Marco Sánchez is a recipient of a teaching assistant fellowship from Escuela Politécnica Nacional for doctoral studies in computer science.

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

References

1. Shaikh, A.K.; Nazir, A. A novel dynamic approach to identifying suspicious customers in money transactions. *Int. J. Bus. Intell. Data Min.* **2020**, *17*, 143–158.
2. Panigrahi, P.K. A framework for discovering internal financial fraud using analytics. In Proceedings of the 2011 International Conference on Communication Systems and Network Technologies, Katra, India, 3–5 June 2011; pp. 323–327.
3. Silowash, G.; Cappelli, D.; Moore, A.; Trzeciak, R.; Shimeall, T.; Flynn, L. *Common Sense Guide to Prevention and Detection of Insider Threats*, 4th ed.; Carnegie Mellon University CyLab: Pittsburgh, PA, USA, 2012.
4. Kassem, R. Detecting asset misappropriation: A framework for external auditors. *Int. J. Account. Audit. Perform. Eval.* **2014**, *10*, 1–42. [CrossRef]
5. Sayal, K.; Singh, G. What Role Does Human Behaviour Play in Corporate Frauds? *Econ. Political Wkly.* **2020**, *55*. Available online: https://www.epw.in/engage/article/what-role-does-human-behaviour-play-corporate (accessed on 1 September 2021).
6. Gabrielli, G.; Medioli, A. An overview of instruments and tools to detect fraudulent financial statements. *Univ. J. Account. Financ.* **2019**, *7*, 76–82. [CrossRef]
7. Dimitrijević, D.; Kalinić, Z. Software Tools Usage in Fraud Detection and Prevention in Governmental and External Audit Organizations in the Republic of Serbia1. In *Knowledge–Economy–Society*; Cracow University of Economics: Cracow, Poland, 2017; p. 71.
8. Vynokurova, O.; Peleshko, D.; Bondarenko, O.; Ilyasov, V.; Serzhantov, V.; Peleshko, M. Hybrid Machine Learning System for Solving Fraud Detection Tasks. In Proceedings of the 2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 21–25 August 2020; pp. 1–5. [CrossRef]
9. Lebichot, B.; Paldino, G.M.; Bontempi, G.; Siblini, W.; He, L.; Oble, F. Incremental learning strategies for credit cards fraud detection: Extended abstract. In Proceedings of the 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA), Sydney, Australia, 6–9 October 2020; pp. 785–786. [CrossRef]
10. Saia, R. A Discrete Wavelet Transform Approach to Fraud Detection. In Proceedings of the International Conference on Network and System Security, Helsinki, Finland, 21–23 August 2017.
11. Vynokurova, O.; Peleshko, D.; Zhernova, P.; Perova, I.; Kovalenko, A. Solving Fraud Detection Tasks Based on Wavelet-Neuro Autoencoder. In Proceedings of the International Scientific Conference "Intellectual Systems of Decision Making and Problem of Computational Intelligence", Zalizniy Port, Ukraine, 25–29 May 2021; pp. 535–546. [CrossRef]
12. Omair, B.; Alturki, A. Taxonomy of Fraud Detection Metrics for Business Processes. *IEEE Access* **2020**, *8*, 71364–71377. [CrossRef]
13. Omair, B.; Alturki, A. Multi-Dimensional Fraud Detection Metrics in Business Processes and their Application. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 570. [CrossRef]
14. Ruankaew, T. The Fraud Factors. *Int. J. Manag. Adm. Sci. (IJMAS)* **2013**, *2*, 1–5.

15. Mansor, N.; Abdullahi, R. Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *Int. J. Acad. Res. Account. Financ. Manag. Sci.* **2015**, *1*, 38–45.
16. Burke, D.D.; Sanney, K.J. Applying the fraud triangle to higher education: Ethical implications. *J. Legal Stud. Educ.* **2018**, *35*, 5. [CrossRef]
17. Awang, N.; Hussin, N.S.; Razali, F.A.; Lyana, S.; Talib, A. Fraud Triangle Theory: Calling for New Factors. *Editor. Board* **2020**, *7*, 54–64.
18. Wolfe, D.T.; Hermanson, D.R. The fraud diamond: Considering the four elements of fraud. *CPA J.* **2004**, *74*, 38.
19. Ruankaew, T. Beyond the fraud diamond. *Int. J. Bus. Manag. Econ. Res. (IJBMER)* **2016**, *7*, 474–476.
20. Christian, N.; Basri, Y.; Arafah, W. Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fraud in Indonesia. *Int. J. Bus. Manag. Technol.* **2019**, *3*, 73–78.
21. Manolopoulos, Y.; Spathis, C.; Kirkos, E. Data Mining techniques for the detection of fraudulent financial statements. *Expert Syst. Appl.* **2007**, *32*, 995–1003.
22. Meenatkshi, R.; Sivaranjani, K. Fraud detection in financial statement using data mining technique and performance analysis. *JCTA* **2016**, *9*, 407–413.
23. Al-Hashedi, K.G.; Magalingam, P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Comput. Sci. Rev.* **2021**, *40*, 100402. [CrossRef]
24. Deng, W.; Huang, Z.; Zhang, J.; Xu, J. A Data Mining Based System For Transaction Fraud Detection. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 15–17 January 2021; pp. 542–545.
25. Phua, C.; Lee, V.; Smith, K.; Gayler, R. A comprehensive survey of data mining-based fraud detection research. *arXiv* **2010**, arXiv:1009.6119.
26. Zhou, X.; Cheng, S.; Zhu, M.; Guo, C.; Zhou, S.; Xu, P.; Xue, Z.; Zhang, W. A state of the art survey of data mining-based fraud detection and credit scoring. In *MATEC Web of Conferences*; EDP Sciences: Les Ulis, France, 2018; Volume 189, p. 03002.
27. Gupta, S.; Mehta, S.K. Data Mining-based Financial Statement Fraud Detection: Systematic Literature Review and Meta-analysis to Estimate Data Sample Mapping of Fraudulent Companies Against Non-fraudulent Companies. *Glob. Bus. Rev.* **2021**. [CrossRef]
28. Ngai, E.W.; 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]
29. Yue, D.; Wu, X.; Wang, Y.; Li, Y.; Chu, C.H. A review of data mining-based financial fraud detection research. In Proceedings of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007; pp. 5519–5522.
30. Sasirekha, M.; Thaseen, I.S.; Banu, J.S. An Integrated Intrusion Detection System for Credit Card Fraud Detection. In *Advances in Computing and Information Technology*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 55–60.
31. Dyba, T.; Kitchenham, B.A.; Jorgensen, M. Evidence-based software engineering for practitioners. *IEEE Softw.* **2005**, *22*, 58–65. [CrossRef]
32. Staples, M.; Niazi, M. Experiences using systematic review guidelines. *J. Syst. Softw.* **2007**, *80*, 1425–1437. [CrossRef]
33. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE 2007-001, Keele University and Durham University Joint Report; Kitchenham: Newcastle, UK, 2007. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471&rep=rep1&type=pdf (accessed on 1 September 2021).
34. Cronin, P.; Ryan, F.; Coughlan, M. Undertaking a literature review: A step-by-step approach. *Br. J. Nurs.* **2008**, *17*, 38–43. [CrossRef]
35. Zhang, H.; Babar, M.A.; Tell, P. Identifying relevant studies in software engineering. *Inf. Softw. Technol.* **2011**, *53*, 625–637. [CrossRef]
36. Rouhani, B.D.; Mahrin, M.N.; Nikpay, F.; Ahmad, R.B.; Nikfard, P. A systematic literature review on Enterprise Architecture Implementation Methodologies. *Inf. Softw. Technol.* **2015**, *62*, 1–20. [CrossRef]
37. Li, Y.; Peng, R.; Wang, B. Challenges in Context-Aware Requirements Modeling: A Systematic Literature Review. In Proceedings of the Asia Pacific Requirements Engeneering Conference, Melaka, Malaysia, 9–10 November 2017; pp. 140–155.
38. Hoyer, S.; Zakhariya, H.; Sandner, T.; Breitner, M.H. Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2382–2391.
39. Sánchez, M.; Torres, J.; Zambrano, P.; Flores, P. FraudFind: Financial fraud detection by analyzing human behavior. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 281–286.
40. Sandhu, N. Behavioural red flags of fraud—A qualitative assessment. *J. Hum. Values* **2016**, *22*, 221–237. [CrossRef]
41. Mackevičius, J.; Giriūnas, L. Transformational research of the fraud triangle. *Ekonomika* **2013**, *92*, 150–163. [CrossRef]
42. Zulaikha, Z.; Hadiprajitno, P.; Rohman, A.; Handayani, R. Effect of attitudes, subjective norms and behavioral controls on the intention and corrupt behavior in public procurement: Fraud triangle and the planned behavior in management accounting. *Accounting* **2021**, *7*, 331–338. [CrossRef]
43. Omar, N.B.; Din, H.F.M. Fraud diamond risk indicator: An assessment of its importance and usage. In Proceedings of the 2010 International Conference on Science and Social Research (CSSR 2010), Kuala Lumpur, Malaysia, 5–7 December 2010; pp. 607–612.

44. Sravanthi, T.; Sruthi, M.; Reddy, S.T.; Prakash, T.C.; Reddy, C.V.K. Fiscal Scam Illuminating Through Analyzing Human Behaviour. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2020; Volume 981, p. 022057.
45. Wang, S. A comprehensive survey of data mining-based accounting-fraud detection research. In Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation, Changsha, China, 11–12 May 2010; Volume 1, pp. 50–53.
46. Yao, J.; Zhang, J.; Wang, L. A financial statement fraud detection model based on hybrid data mining methods. In Proceedings of the 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, 26–28 May 2018; pp. 57–61.
47. Jayabrabu, R.; Saravanan, V.; Tamilselvi, J.J. A framework for fraud detection system in automated data mining using intelligent agent for better decision making process. In Proceedings of the 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Coimbatore, India, 6–8 March 2014; pp. 1–8.
48. Ahmed, M.; Mahmood, A.N. A novel approach for outlier detection and clustering improvement. In Proceedings of the 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), Melbourne, Australia, 19–21 June 2013; pp. 577–582.
49. Kumar, V.; Sriganga, B. A review on data mining techniques to detect insider fraud in banks. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2014**, *4*, 370–380.
50. Vikram, A.; Chennuru, S.; Rao, H.R.; Upadhyaya, S. A solution architecture for financial institutions to handle illegal activities: A neural networks approach. In Proceedings of the 37th Annual Hawaii International Conference on System Science, Big Island, HI, USA, 5–8 January 2004; pp. 181–190.
51. Mishra, A. Fraud Detection: A Study of AdaBoost Classifier and K-Means Clustering. 2021. Available online: https://www.researchsquare.com/article/rs-247874/latest.pdf (accessed on 1 September 2021).
52. Rizki, A.A.; Surjandari, I.; Wayasti, R.A. Data mining application to detect financial fraud in Indonesia's public companies. In Proceedings of the 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, Indonesia, 25–26 October 2017; pp. 206–211.
53. Kim, Y.J.; Baik, B.; Cho, S. Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. *Expert Syst. Appl.* **2016**, *62*, 32–43. [CrossRef]
54. Ravisankar, P.; Ravi, V.; Rao, G.R.; Bose, I. Detection of financial statement fraud and feature selection using data mining techniques. *Decis. Support Syst.* **2011**, *50*, 491–500. [CrossRef]
55. Seemakurthi, P.; Zhang, S.; Qi, Y. Detection of fraudulent financial reports with machine learning techniques. In Proceedings of the 2015 Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 24 April 2015; pp. 358–361.
56. Mohanty, L.T.K.M.G. Enron Corpus Fraud Detection. *Int. J. Recent Technol. Eng. (IJRTE)* **2019**, *8*, 315–317.
57. Li, H.; Wong, M.L. Financial fraud detection by using Grammar-based multi-objective genetic programming with ensemble learning. In Proceedings of the 2015 IEEE Congress on Evolutionary Computation (CEC), Sendai, Japan, 25–28 May 2015; pp. 1113–1120.
58. Sorkun, M.C.; Toraman, T. Fraud detection on financial statements using data mining techniques. *Intell. Syst. Appl. Eng.* **2017**, *5*, 132–134. [CrossRef]
59. El Bouchti, A.; Chakroun, A.; Abbar, H.; Okar, C. Fraud detection in banking using deep reinforcement learning. In Proceedings of the 2017 Seventh International Conference on Innovative Computing Technology (INTECH), Luton, UK, 16–18 August 2017; pp. 58–63.
60. Mardani, S.; Akbari, M.K.; Sharifian, S. Fraud detection in process aware information systems using MapReduce. In Proceedings of the 2014 6th Conference on Information and Knowledge Technology (IKT), Shahrood, Iran, 27–29 May 2014; pp. 88–91.
61. Mallika, R. Fraud Detection Using Supervised Learning Algorithms. *Int. J. Adv. Res. Comput. Commun. Eng.* **2017**, *6*. [CrossRef]
62. Save, P.; Tiwarekar, P.; Jain, K.N.; Mahyavanshi, N. A novel idea for credit card fraud detection using decision tree. *Int. J. Comput. Appl.* **2017**, *161*. [CrossRef]
63. Holton, C. Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decis. Support Syst.* **2009**, *46*, 853–864. [CrossRef]
64. Jans, M.; Lybaert, N.; Vanhoof, K. Internal fraud risk reduction: Results of a data mining case study. *Int. J. Account. Inf. Syst.* **2010**, *11*, 17–41. [CrossRef]
65. Heryadi, Y.; Warnars, H.L.H.S. Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM. In Proceedings of the 2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom), Phuket, Thailand, 20–22 November 2017; pp. 84–89.
66. Yaram, S. Machine learning algorithms for document clustering and fraud detection. In Proceedings of the 2016 International Conference on Data Science and Engineering (ICDSE), Cochin, India, 23–25 August 2016; pp. 1–6.
67. John, S.N.; Anele, C.; Kennedy, O.O.; Olajide, F.; Kennedy, C.G. Realtime fraud detection in the banking sector using data mining techniques/algorithm. In Proceedings of the 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2016; pp. 1186–1191.
68. West, J.; Bhattacharya, M. Some Experimental Issues in Financial Fraud Detection: An Investigation. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 December 2015; pp. 1155–1158.
69. Lin, C.C.; Chiu, A.A.; Huang, S.Y.; Yen, D.C. Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. *Knowl.-Based Syst.* **2015**, *89*, 459–470. [CrossRef]

70. Mekonnen, S.; Padayachee, K.; Meshesha, M. A Privacy Preserving Context-Aware Insider Threat Prediction and Prevention Model Predicated on the Components of the Fraud Diamond. In Proceedings of the 2015 Annual Global Online Conference on Information and Computer Technology (GOCICT), Louisville, KY, USA, 4–6 November 2015; pp. 60–65. [CrossRef]
71. Asuncion, A.; Newman, D. *UCI Machine Learning Repository*; School of Information and Computer Science, University of California: Irvine, CA, USA, 2007. Available online: http://www.ics.uci.edu/~mlearn/MLReposit-ory.html (accessed on 1 September 2021).
72. ENRON. (This Dataset Contains 517,431 Emails with 3500 Folders from 151 Users). Available online: https://www.cs.cmu.edu/~enron/ (accessed on 1 September 2021).
73. Omair, B.; Alturki, A. A Systematic Literature Review of Fraud Detection Metrics in Business Processes. *IEEE Access* **2020**, *8*, 26893–26903. [CrossRef]
74. Pourhabibi, T.; Ong, K.L.; Kam, B.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decis. Support Syst.* **2020**, *133*, 113303. [CrossRef]
75. Homer, E. Testing the fraud triangle: A systematic review. *J. Financ. Crime* **2019**, *27*, 172–187. [CrossRef]
76. Dybå, T.; Dingsøyr, T. Strength of Evidence in Systematic Reviews in Software Engineering. In Proceedings of the Second ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, Bari, Italy, 5–7 October 2008; pp. 178–187. [CrossRef]
77. Dybå, T.; Dingsøyr, T. Empirical studies of agile software development: A systematic review. *Inf. Softw. Technol.* **2008**, *50*, 833–859. [CrossRef]