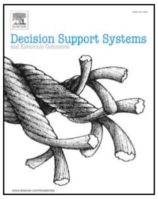
Decision Support Systems 133 (2020) 113303

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss



Fraud detection: A systematic literature review of graph-based anomaly detection approaches

Tahereh Pourhabibi[a,*], Kok-Leong Ong[b], Booi H. Kam[a], Yee Ling Boo[a]

[a] School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, Australia
[b] Centre for Data Analytics and Cognition, La Trobe University, Melbourne, Australia

ARTICLE INFO

Keywords:
Fraud detection
Graph-based anomaly detection
Graph data
Systematic literature review
Social network
Big data analytics

ABSTRACT

Graph-based anomaly detection (GBAD) approaches are among the most popular techniques used to analyze connectivity patterns in communication networks and identify suspicious behaviors. Given the different GBAD approaches proposed for fraud detection, in this study, we develop a framework to synthesize the existing literature on the application of GBAD methods in fraud detection published between 2007 and 2018. This study aims to investigate the present trends and identify the key challenges that require significant research efforts to increase the credibility of the technique. Additionally, we provide some recommendations to deal with these challenges.

1. Introduction

Advances in communication and digital technologies have created a highly connected world [1]. Different types of networks – social media, e-commerce websites, blogs, industry trading networks, telecommunication networks, banking networks, and insurance networks – have emerged, generating an increasing volume of data among them [1]. These networks offer a vast array of information easily accessible via anonymous accounts, making them easy platforms for misinformation, mischiefs, and misdemeanors: fraudsters and attackers can conceal their malicious activities within the mountains of data [2]. With the relentless growth of such networks, opportunities for fraudsters to manipulate them for their benefits have also expanded [2].

Until recently, social networks have been relatively "relaxed" regarding third parties gaining access to their users' details. This allows fraudsters to engage in deceptive and destructive activities, such as enabling sexual predators to interact with unsuspecting vulnerable youngsters [3] or foreign interests to influence election outcomes [4]. Other networks have also been targets of fraudulent manipulations. For instance, in the United States, fraudulent claims in healthcare and insurance led to financial losses amounting to $98 billion [5] and $300 billion [6] a year, respectively.

Not surprisingly, many organizations have been spending considerable resources, including the adoption of technologies and sophisticated mechanisms, to protect their networks and data from internal and external threats [7,8]. Specifically, attention has been directed to examining the interactions and activities of business clients or users within a network [9]. These interactions, which are represented as interdependencies and relationships between data objects in graphs,[1] are analyzed using data mining and machine learning techniques to detect possible embedded anomalies to be flagged as potential frauds [9].

In the era of Big Data, detecting fraudulent activities within networks is analogous to finding a needle in a haystack. Graph-based anomaly detection (GBAD) approaches, a branch of data mining and machine learning techniques that focuses on interdependencies between different data objects, have been increasingly used to analyze relations and connectivity patterns in networks to identify unusual patterns [1]. In recent years, GBAD techniques have considerably contributed to identifying fraudulent activities within networks and have been recognized by fraud detection experts as robust, reliable, and promising anomaly detection techniques [1,9].

There have been several comprehensive survey studies on anomaly detection [10], anomaly detection using graph-based methods [3,9,11,12], and anomaly detection for fraud detection [13–15]. However, our investigation suggests that no study has conducted review studies of GBAD techniques that consider the interdependencies between different data objects in a graph to detect fraudulent activities. Furthermore, none of these studies have provided an in-depth exploration of graph-based methods for graph data in fraud detection. In

* Corresponding author.
E-mail address: tahereh.pourhabibi@rmit.edu.au (T. Pourhabibi).

[1] Throughout this paper, we use the terms "network" and "graph" interchangeably.

https://doi.org/10.1016/j.dss.2020.113303
Received 5 August 2019; Received in revised form 13 April 2020; Accepted 14 April 2020
Available online 17 April 2020

this study, we aim to consolidate existing research know-hows in the context of analyzing interdependent data objects in a graph for fraud detection using GBAD, making this review notably different from other survey studies on the subject.

We focus on research undertaken between 2007 and 2018 to provide a synthesized understanding of the state-of-the-art GBAD methods, identify key research issues raised against application contexts, and establish future directions to expand GBAD research in fraud detection. To achieve these objectives, we focus on studies using GBAD techniques with data containing interrelations between actors (nodes) in the network. Additionally, to synthesize existing works, we develop a classification framework, which also serves as our analytic platform in identifying gaps and challenges to aid in further studies.

2. Overview of surveys on GBAD methods

Over the past few years, several survey articles on anomaly detection methods [10], anomaly detection for fraud detection [13–15], and application of graph-based methods on anomaly detection [3,9,11,12] have been published. Our focus is to review papers on anomaly detection using graph-based methods. As such, the review study by Chandola et al. [10], who surveyed different anomaly detection techniques on multidimensional data, existing challenges in anomaly detection, and different types of detected anomalies in various application areas, is considered outside our scope of review. Likewise, the review studies by Abdallah et al. [14], Bhattacharyya et al. [13], and Ngai et al. [15], which specifically examined anomaly detection techniques to detect fraud in multidimensional data within various financial sectors, also belong to a different domain.

Our focus on anomaly detection studies using graph-based methods aligns with the studies conducted by Savage et al. [3], Akoglu et al. [9], Anand et al. [11], and Ranshous et al. [12].

Savage et al.'s [3] review primarily focused on existing computational techniques for detecting different types of anomalies (such as anomalous nodes, edges, or subgraphs) in online social networks (OSNs). They summarized the process of anomaly detection in OSNs in two steps: (i) selection and calculation of network features and (ii) classification of observations from this feature space. Owing to the lack of publicly available datasets, the reviewers also noted that the proposed solutions were tested on a limited number of datasets. This limitation led them to question if the solutions might be "over-fitted" to a particular type of anomaly, and therefore, the results may not be applicable across an extensive range of datasets or problems.

Akoglu et al. [9] also surveyed GBAD approaches by focusing on existing difficulties in anomaly detection and the importance of graph-based methods to resolve the proposed challenges. They analyzed the technical characteristics and definitions of these approaches and discussed the application of GBAD methods in several real-world scenarios, including fraud detection.

In their conference paper, Anand et al. [11] reviewed several studies in anomaly detection in OSNs and classified them into two major categories: behavior-based methods, which analyze user behavior and interactions, and structure-based approaches, which focus on identifying special types of network structures, such as cliques, clusters or communities, stars, and ego nets. In Ranshous et al.'s [12] review, anomaly detection in dynamic social networks was the main focus, covering a critical discussion on the technical aspects of existing methods and types of detected anomalies.

However, none of these reviews explicitly scrutinized the application of graph-based methods in fraud detection to identify recent problems and challenges, a gap that this paper aims to fill. Through a rigorous systematic literature analysis, we map out the research trends, methods, and key challenges when using GBAD methods in fraud detection. We present an overview of the current state-of-the-art GBAD methods in detecting frauds but exclude the technical details of the GBAD methods employed.

Our review of existing works contributes to four areas of GBAD research in fraud detection. First, we propose a classification framework to categorize GBAD research studies and spotlight challenges. The proposed framework offers a systematic probe for researchers and provides an in-depth understanding of how GBAD techniques can be used to analyze and detect frauds.

Second, we synthesize the findings of extant literature into a cataloging framework (see Table 3) to enable practitioners to appreciate the correspondence between the nature of their data network, types of anomalies, and appropriate graph-based methods that suit the needs of their specific application areas.

Third, this paper highlights the existing trends and significant challenges in fraud detection using GBAD approaches. Additionally, it suggests directions for future research to minimize the impact of the highlighted issues.

Finally, we outline possible future research directions in applying GBAD techniques to fraud detection in emerging areas, such as the financial technology (FinTech) industry [16], which is vulnerable to various forms of online fraud as it starts to grow rapidly.

3. Research methodology

In this study, we adopted Booth et al.'s [17] systematic approach to literature review and followed the three-phase methodology employed by Ngai et al. [15,18], as depicted in Fig. 1.

The first phase is "research definition." It includes identifying the research area, formulating review goals, and defining the research scope. The research area in this review is "fraud detection" with three main goals: (1) to identify current trends, (2) to highlight current challenges and provide directions for future research, and (3) to introduce a classification framework for analyzing current studies. The scope covers studies that have employed GBAD techniques.

The second phase is "research methodology," which starts with identifying scientific databases hosting articles related to our research context. Five major online scientific databases were selected: ScienceDirect, ACM Digital Library, IEEE Xplore, Springer, and ABI/Inform. The literature search process began with the creation of criteria to determine the articles to include in, or exclude from, our analysis. Following Ngai et al. [15,18] and Frost [19], we set four criteria, stipulating that the article must (1) be published in a peer-reviewed academic research journal, (2) be written in English, (3) be published between 2007 and 2018, and (4) have its full text available in at least one of the five databases.

To achieve a more effective and comprehensive search strategy, we employed Boolean expressions to combine three terms: "graph," "anomaly detection," and "fraud detection" (i.e., "graph" AND "anomaly detection" AND "fraud detection"). A total of 585 papers met the inclusion criteria. Then, we pruned the papers through a two-step process. The first step ("Abstract Reading and Skimming") involved reading titles and abstracts, which resulted in eliminating 428 unrelated papers, white papers, and tutorials, 12 duplicated titles, and 80 literature review articles. The remaining 65 papers underwent second-level pruning, accomplished by "Reading the Whole Article." This process eliminated another group of 26 unrelated papers, leaving 39 papers for the final analysis.

For the final "classification and analysis" phase, we applied a series of guided questions to sort the 39 papers, similar to the approach adopted by Chan et al. [20]. To ensure the reliability of the classification, each paper was independently reviewed by two authors. Classification discrepancies (e.g., incompatibility in the type of detected anomaly or nature of the input network (see Table 3)) were resolved by having the third author read the paper. The guided questions used were as follows:

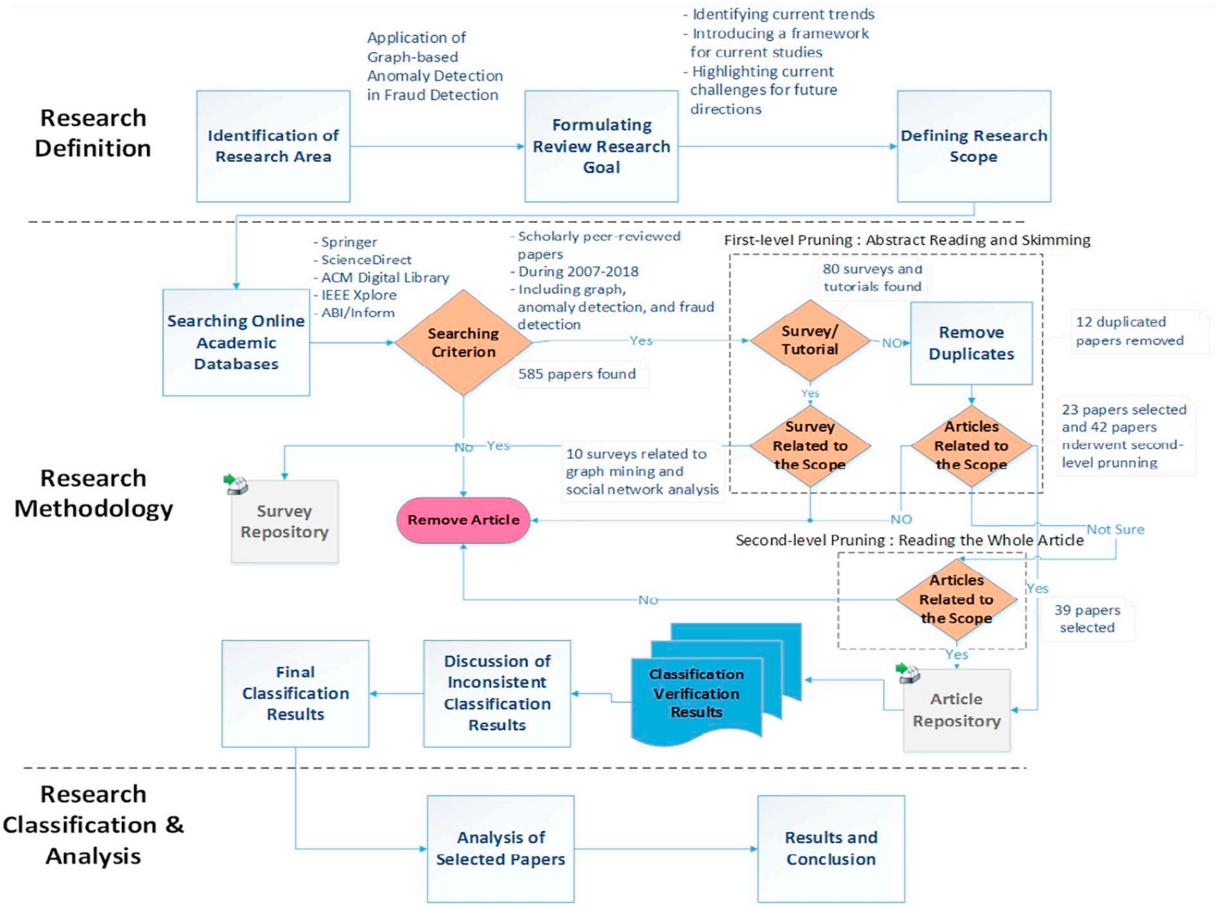

Research Definition
Identification of Research Area
Application of Graph-based Anomaly Detection in Fraud Detection
Formulating Review Research Goal
- Identifying current trends
- Introducing a framework for current studies
- Highlighting current challenges for future directions
Defining Research Scope
Research Methodology
Searching Online Academic Databases
- Springer
- ScienceDirect
- ACM Digital Library
- IEEE Xplore
- ABI/Inform
Searching Criterion
- Scholarly peer-reviewed papers
- During 2007-2018
- Including graph, anomaly detection, and fraud detection
585 papers found
Yes
First-level Pruning : Abstract Reading and Skimming
80 surveys and tutorials found
Survey/ Tutorial
NO
Remove Duplicates
12 duplicated papers removed
Yes
Survey Related to the Scope
Articles Related to the Scope
23 papers selected and 42 papers nderwent second-level prunning
10 surveys related to graph mining and social network analysis
No
Yes
Survey Repository
Remove Article
NO
Not Sure
Second-level Pruning : Reading the Whole Article
Articles Related to the Scope
No
Yes
39 papers selected
Yes
Article Repository
Classification Verification Results
Discussion of Inconsistent Classification Results
Final Classification Results
Research Classification & Analysis
Analysis of Selected Papers
Results and Conclusion

Fig. 1. Systematic literature review process.

1. What were the study trends and focus?
2. How did the availability of existing labeled data influence the choice of anomaly detection techniques used in different studies?
3. What were the types of analyzed networks?
4. What were the types of detected anomalies?
5. What were the principal graph-based methods used?
6. What were the representation methods used?
7. What were the available research data samples?
8. What were the measures used to evaluate the findings?
9. What were the contributions of the studies, challenges faced during the research, and possible future directions?

The first six questions provide six distinct levels of analysis set within the data samples available for experimental studies (Question 7) and the range of measures used for evaluating the findings (Question 8). We structured the eight questions into a hierarchical classification framework to systematically categorize the 39 papers selected for review (see Fig. 2). The last question, Question 9, does not constitute part of the classification framework. It is included to remind us to compile the challenges identified by the review studies, including suggested directions for future research. The next section explains the classification framework developed based on the above-proposed questions.

4. Classification framework

Along with the sequence of the nine guiding questions stated in Section 3, the proposed classification framework begins with identifying the domain of interest (i.e., study trends and focus). The other five components of this framework (Questions 2–6) are described below.

4.1. Availability of data labels

Depending on the available data labels, anomaly detection approaches are classified into three broad categories: (i) supervised, (ii) unsupervised, and (iii) semi-supervised [10]. Table 1 presents the comparison of the characteristics of the three approaches.

4.2. Nature of the input network

With GBAD approaches, the nature of the input network can influence the process of anomaly detection and design of the algorithm. As outlined in Table 2, these features include (i) information propagation in the network (such as the direction of links, and the time the links were established), (ii) node characteristics (such as node types and node attributes), and (iii) peer influences (such as link structures and link attributes) [22].

4.3. Types of anomalies

Various GBAD approaches have been designed to detect different anomalies. These methods [12,26] detect anomalies in various networks, such as dynamic or static graphs (attributed or unattributed) by capturing (a) anomalous nodes, (b) edges, (c) subgraphs, and (d) events. Therefore, the type of anomaly is a critical characteristic of our classification framework.

Anomalous nodes are a subset of nodes where every node in the subset has an irregular feature in comparison with the other nodes in the graph. Typically, each node is assigned an anomaly score based on its characteristics (e.g., the ratio of input/output degree and ego net density) [12,26]. Similar to anomalous nodes, anomalous edges are a

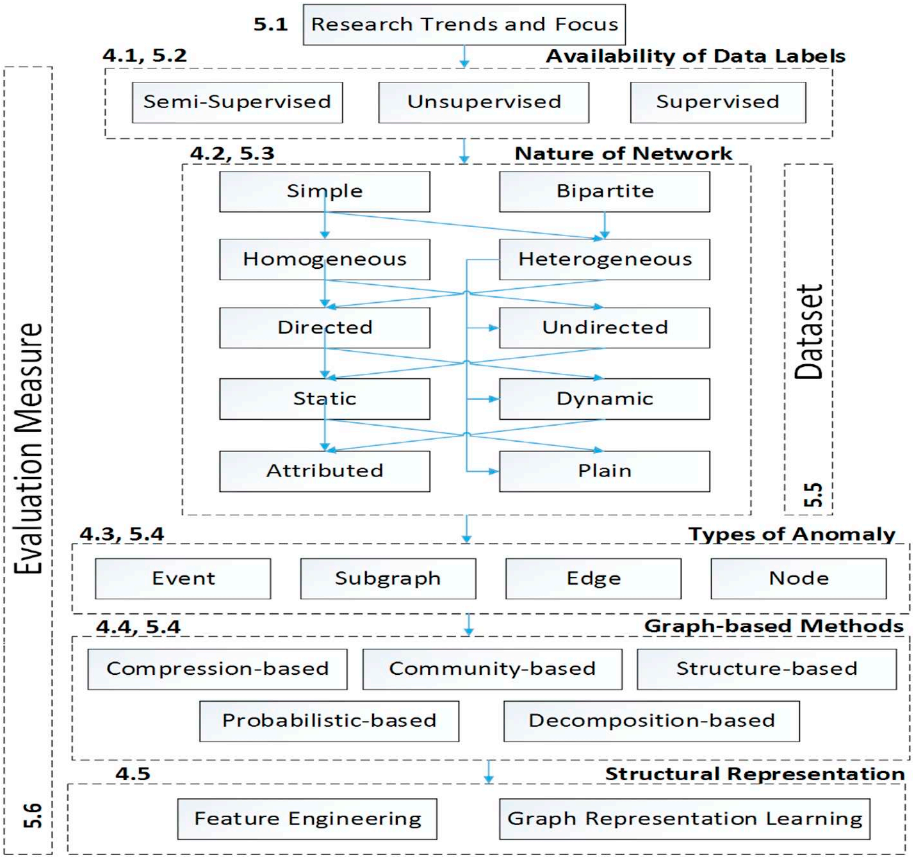


Fig. 2. Framework for the literature analysis and classification of GBAD fraud detection papers.
Note: Numbers refer to the subsections in this paper, e.g., 4.5 means Section 4.5 of this paper.

Table 1
Characteristics of the anomaly detection approaches based on the available data labels.

Supervised [13,21]	Unsupervised [14]	Semi-supervised [14]
● Require labeled data samples of legitimate and fraudulent samples ● Build models based on patterns revealed in existing data samples ● Unable to detect unseen suspicious activities	● Do not need labeled data samples ● Able to detect unseen suspicious activities	● Use both labeled and unlabeled samples ● Requires a few instances of labeled samples ● Able to detect unseen suspicious activities

Table 2
Characteristics of the different types of input networks.

Types of input network	Characteristics
Simple [23]	- One subset of nodes
vs.	
Bipartite [23]	-Two disjoint subsets of nodes
Homogeneous[a] [23]	- One type of node or link
vs.	- Different types of nodes or links
Heterogeneous[b] [24]	- Difficult to detect suspicious activities [25]
Directed [23]	- Symmetric relations between nodes
vs.	- Asymmetric relations between nodes
Undirected [23]	
Static [9,12]	- A single snapshot of a network [26]
vs.	- Structure constantly changing over time [9]
Dynamic [9,12]	- More difficult to analyze anomalies [9,12,26]
Attributed [9,12,26]	- Nodes or links with attributes
vs.	- Attributes revealing considerable information regarding the network entities and their interactions [27]
Unattributed	
	- No attribute assigned to either nodes or links

[a] Also called simple, simplex, or monoplex.
[b] Also called multiplex or multilayer networks.

subset of edges where every edge exhibits abnormal behavior, i.e., having scores higher than a specific threshold. This characteristic, in turn, suggests the existence of an anomaly, such as anomalous nodes. By contrast, the approach to finding an irregular subgraph is quite different. Typically, subgraphs are first identified by community detection methods (see Section 4.4), and then each subgraph is assigned an anomaly score based on intra-graph comparisons (see Noble and Cook [28] for more information). The last anomaly type is event and change detection. This type of anomaly is exclusively found in dynamic networks and designed to locate the specific time period(s) in which activities are significantly different from those in the rest of the periods [12].

4.4. Graph methods

Graph methods include the machine learning algorithm(s) that are applied to the networks to detect different types of anomalies. Depending on the available data labels, nature of the input network, and types of anomalies that are to be discovered in a network, prior studies have captured different anomalies across five approaches, as described in Fig. 3.

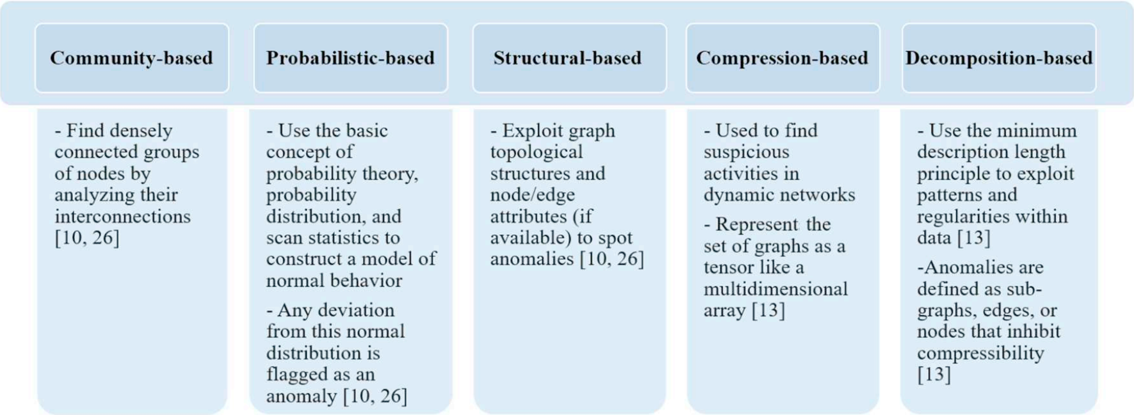

Community-based
- Find densely connected groups of nodes by analyzing their interconnections [10, 26]
Probabilistic-based
- Use the basic concept of probability theory, probability distribution, and scan statistics to construct a model of normal behavior
- Any deviation from this normal distribution is flagged as an anomaly [10, 26]
Structural-based
- Exploit graph topological structures and node/edge attributes (if available) to spot anomalies [10, 26]
Compression-based
- Used to find suspicious activities in dynamic networks
- Represent the set of graphs as a tensor like a multidimensional array [13]
Decomposition-based
- Use the minimum description length principle to exploit patterns and regularities within data [13]
-Anomalies are defined as sub-graphs, edges, or nodes that inhibit compressibility [13]

Fig. 3. Five different types of GBAD approaches.

4.5. *Structural representation*

The success of graph methods depends on the choice of data representation being used [29,30]. Generally, feature engineering and graph representation learning (also called graph embedding) techniques aim to embed the structural representation of a graph into a vector space (or feature space), in which the machine learning models are then built [29]. Therefore, defining measures that can best map a network structure into a vector space is highly important. This method helps preserve the topological and structural characteristics of nodes and network information, which can then be more explicitly analyzed by machine learning methods to detect anomalies [29].

Feature engineering is a useful way of capturing human ingenuity and prior knowledge [31]. In this technique, features are designed based on analysts' foreknowledge regarding the network entities and known suspicious activities. These features range from simple attributes, such as in-degree,[2] out-degree,[3] and reciprocity, to more complex ones, such as clustering coefficients[4] [32]. Thus, the learning algorithms in feature engineering are highly dependent on human intervention, creating scalability problems. In recent years, GBAD researchers have started developing new methods, such as graph representation learning or graph embedding techniques [33], that aim to build graph structures without any human intervention. These techniques use different methods, such as deep learning [29,34], to quickly construct models and reveal hidden explanatory factors previously unknown to security experts.

5. Findings and discussions

Using the proposed classification framework (Fig. 2), we cataloged the 39 reviewed papers into five areas: graph methods, application areas, data label availability, input network, and types of anomalies (see Table 3). This cataloging aims to increase the understanding of a particular type of GBAD method while dealing with certain application areas and support researchers to explore which approach or paper to focus on when looking for specific types of anomalies in accordance with the nature of their input network and availability of their data labels. We discuss the findings of our review following the guiding questions presented in Section 3.

5.1. *Research trends and focus*

Fig. 4 shows the distribution of the 39 studies analyzed from 2007 to 2018 (none of the 39 papers reviewed were published in 2007 and 2008). This finding suggests a growing trend in the application of GBAD techniques for fraud detection.

Our analysis suggests that studies using GBAD methods to detect fraudulent activities generally fall into two major streams: traditional and OSNs (Fig. 5). The traditional stream, with applications in insurance [37,46,59], telecommunication [51], banking [45,46], online credit applications (OCA) [66], anti-money laundering (AML) [38], retail holding [53], trading [47], and internal organizational fraud (IOF) [67,68], has heavily relied on GBAD methods to analyze its data. However, the data used in these studies were not explicitly linked together. These studies have used graph data to detect fraud by inferring the links within the data. This growing trend is becoming significant and demonstrates the applicability and importance of GBAD methods for fraud detection in various applications.

Although research studies using GBAD methods are still sparse, the efforts devoted to detecting frauds in insurance and banking applications have become prevalent since 2017. Fig. 6 shows the diversity of research studies applying GBAD techniques on fraud detection by research area during the selected period. Since 2014, the analysis of OSNs where data are inherently linked to one another in networks [54,69,70] has also become an emerging stream. This observation implies the increasing popularity of online social activities. As businesses turn to social media to promote their products and services, they also create an additional opportunity and a fertile channel for fraudsters to conduct malicious activities [71]. For example, fake reviewers can earn between $0.5 and $3 for each fake review [71] by demoting or promoting a product, service, or business. As the range of online social activities increases, the possibility of different types of fraud in such networks also grows, necessitating a need to filter any suspicious behavior to mitigate the consequences.

5.2. *Availability of data labels*

From the data label perspective, approximately 87.2% of the reviewed research studies have exclusively developed their models using unsupervised learning techniques. The reason is that data labels are often in short supply or nonexistent in many real-world problems, such as fraud detection [14]. Consequently, unsupervised learning techniques have been the focus of many research studies. There are exceptions, such as Shehnepoor et al.'s [63] work, which can be applied in unsupervised and semi-supervised settings (2.6%), and the works of Bangcharoensap et al. [50] and Molloy et al. [46], which both exclusively used a semi-supervised-based approach. From our review, only 5.1% of the studies applied supervised learning methods.

[2] For a vertex v in a graph, the number of edges adjacent v is called the *in-degree*.

[3] For a vertex v in a graph, the number of edges leaving v is called the *out-degree*.

[4] The clustering coefficient is a measure of the degree to which nodes in a graph tend to cluster together.

Table 3
Cataloging of graph-based fraud detection[a].

Graph methods	Application areas	Reference	Availability of data labels	Nature of the input network				Types of anomalies
Structural-based	OSN	[35]	US	SH	ST	D	A	SG
		[2]	US	BH	ST	UD	UA	SG
		[36]	US	SH	DY	UD	UA	N
	Insurance	[5]	S	SH	ST	D	A	N
		[37]	US	SH	ST	UD	A	N
	AML	[38]	US	SH	ST	D	A	SG
		[39]	US	SH	ST	D	A	N
Community-based	OSN	[40], [41,42]	US	BH	ST	UD	A	SG
		[43]	US	SH	DY	D	A	SG
		[44]	US	SH	ST	D	A	SG
	AML	[45]	US	SH	ST	D	A	SG
	Banking	[46]	SS	SH	ST	D	A	SG
	Trading	[47]	US	SH	ST	D	A	SG
	IOF	[48]	US	SH	ST	UD	UA	SG
	Online Auction	[49]	US	BH	ST	UD	A	SG
		[50]	SS	BH	ST	UD	A	SG
	Telecom	[51]	US	SH	ST	UD	UA	SG
		[52]	S	BH	DY	UD	A	SG
	Retail Holding	[53]	US	SH	ST	D	A	SG
Decomposition-based	OSN	[54,55]	US	SH	DY	D	A	SG
		[56]	US	SH	DY	D	A	N
		[57]	US	SH	DY	D	A	N, SG
Compression- based	Trading	[7,8]	US	SH	ST	D/UD	A/UA	SG
	OSN	[27]	US	BH/SH	ST	UD	A	N
	Insurance, AML, Banking, Trading	[58]	US	BH/SH	ST	UD/D	A	N
Probabilistic-based	Insurance	[59]	US	BH	ST	UD	A	N
		[60]	US	SH	ST	D	A/UA	N, SG
	OSN	[61]	US	BH	ST	UD	A	N
		[62]	US	BH	DY	UD	UA	N
		[63]	US, SS	BH	ST	UD	A	N
		[64]	US	SH	DY	D	A	SG
	Online auction	[65]	US	BH	ST	UD	A	SG
	OCA	[66]	US	SH	DY	D	A	E
	IOF	[67]	US	SH	ST	D	A	N
		[68]	US	SH	DY	D	A	SG

SH, simple and homogenous; BH, bipartite and heterogeneous;
DY, dynamic; ST, static;
D, directed; UD, undirected;
A, attributed; UA, unattributed;
S, supervised; U, unsupervised; SS, semi-supervised;
N, node; SG, subgraph; E, edge; EV, event;
AML, anti-money laundering; IOF, internal organizational fraud; OCA, online credit application.

[a] Note:

(1) Graph representation learning was only used in decomposition-based methods in [54,56].

(2) Studies that model the input network as a bipartite graph are heterogeneous networks with different types of nodes and the rest of the studies are homogeneous networks.

(3) None of the reviewed studies worked on anomalous event detection.

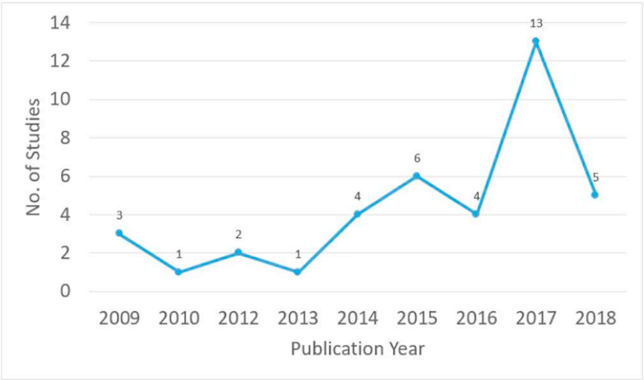


Fig. 4. Distribution of papers reviewed, 2009–2018.

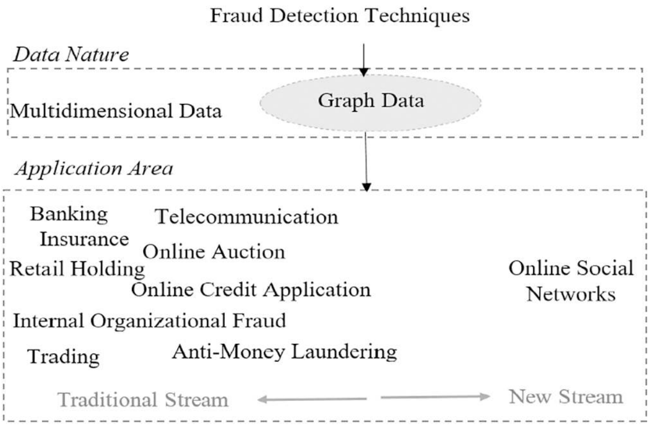


Fig. 5. Data nature and application areas of GBAD techniques for fraud detection.

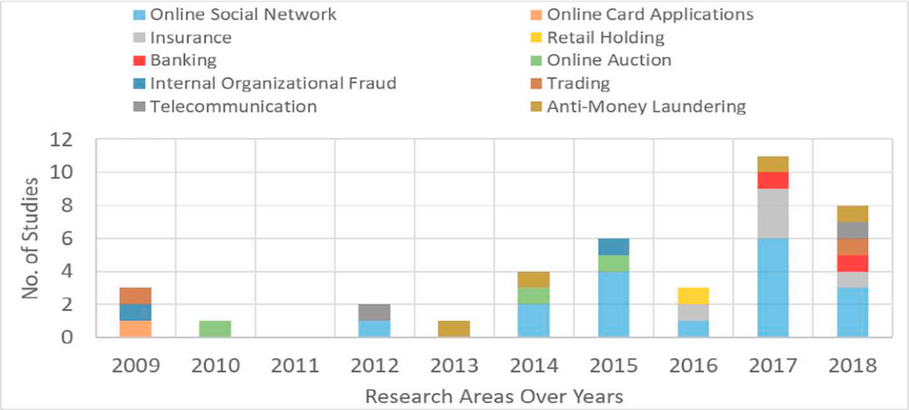


Fig. 6. Distribution of research studies using GBAD techniques for fraud detection, 2009–2018.

The shortcomings related to supervised and semi-supervised learning techniques, as outlined in Section 4.1, may hinder the use of GBAD approaches in some cases. These methods are among the least commonly used methods found in this review.

5.3. Nature of the input network

The nature of the input network is a fundamental feature of GBAD approaches. Therefore, we unpack them into several units of analysis, which are described in this section.

5.3.1. Simple vs. bipartite

Among the papers that modeled the input network as a bipartite graph, the most represented application is OSNs with 20.5% (8 of the 39 papers). The other applications are insurance (5.1%; two papers), auction (7.7%; three papers), and telecommunication fraud detection (2.6%; one paper). We can explain this finding based on the nature of the above application areas, where the connections between users and products or services should be analyzed to detect suspicious behaviors (e.g., the number of parties bidding a seller's product in auction fraud, number of ratings to a product in online business websites, and claims submitted by a specific insurance provider). The remaining 25 papers analyzed user-to-user connections (e.g., the number of messages sent by a specific user to others) to detect suspicious activities, thus modeling their input network as simple graphs.

5.3.2. Homogeneous vs. heterogeneous

The reviewed research papers on OSNs, insurance, and auction frauds have extensively considered the analysis of suspicious activities in bipartite networks. These studies model bipartite networks using two different sets of nodes, mainly users and products or users and services. These networks are considered heterogeneous networks with different types of nodes (Table 3). Among the studies, only two [27,44] have considered different types of activities (e.g., different types of links). However, in [44], each type of relationship was simulated as a simple network and analyzed separately. Another study [27] also simulated the input network as a heterogeneous bipartite network. As mentioned in Section 5.3.1, 25 papers investigated users' behavior on simplex networks and only considered one type of user activity, thus ignoring the inherent multiplex nature of human interactions in their analysis [25]. These studies did not consider different types of users' activities in the network to detect suspicious activities (see Section 4.2).

5.3.3. Directed vs. undirected

As the information summarized in Table 3 indicates, approximately 48.7% of the research studies are solely applied to directed networks, 43.6% are practiced only on undirected networks, and the remaining 7.7% are applied to directed and undirected networks.

Studies modeling their input network as an undirected network mainly explore user-to-product or user-to-service relationships and are mostly bipartite networks (14 of the reviewed papers employed bipartite networks).

5.3.4. Static vs. dynamic

In recent years, dynamic networks have increased in popularity owing to their applications in social networks, insurance, and online banking [54,56,66,68]. The relentless growth of social networks, in particular, has provided opportunities for fraudsters to infiltrate these networks and spread their illusive activities by frequently establishing new connections with other users or changing their relations with existing users [72]. In other words, fraudsters can easily evade current detection mechanisms. Although the importance of analyzing dynamic networks for suspected fraud has surged, it is still a nascent research area [54,56,66,68]. Of the papers reviewed, only 28.2% of research studies worked on fraud detection in dynamic networks, whereas the remaining 71.8% (28/39) merely searched for suspicious activities in static networks.

5.3.5. Attributed vs. unattributed

The link and node attributes are essential elements for differentiating users' behavior in a communication network [27]. They provide useful information for detecting anomalies in a network. Table 3 shows that only five papers that were reviewed (12.8%) ignored the importance of attributes. Among those that used attributes to distinguish suspicious activities (87.2%), most employed link attributes, such as interaction strength.

5.4. Graph methods and types of anomalies detected

Depending on the available data labels and nature of the input network, five different GBAD methods were employed to capture different types of anomalies in the network among the 39 papers reviewed. Community-based approaches were the most widely used (35.9%) with probabilistic-based methods as the second most popular approach (25.6%). Around 17.9% of the studies used structural-based techniques, whereas compression-based (10.3% of the studies) and decomposition-based approaches (10.3% of studies) were among the least-used methods (see Fig. 7).

Fraud is characteristically manifested as a collective behavior in networks, as fraudsters attempt to coordinate their behavior as a group [72]. Detection of such illusive user communities (also referred to as groups or clusters) has become a key focus. Table 3 reveals that around two-thirds of the research studies focused on identifying anomalous subgraphs. Among them, the top two GBAD methods, community-based and probabilistic-based methods, exhibited the highest share. By contrast, the other three GBAD methods were mostly used to detect the

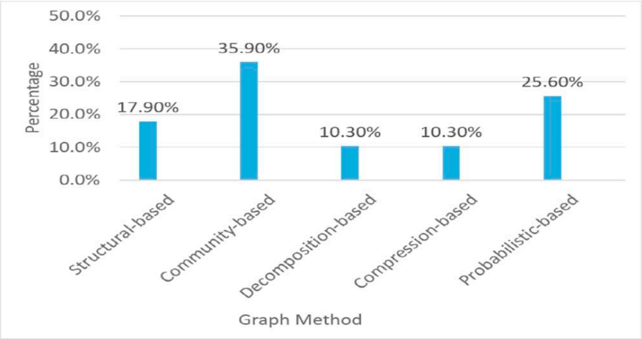


Fig. 7. Spread of different GBAD methods in the papers reviewed.

most suspicious nodes or edges within the network.

5.5. Dataset

Research studies on fraud detection have mostly used real-world data as their test platforms [73,74]. Many have also used synthetic data to simulate specific scenarios [73,74]. Owing to privacy considerations, organizations and stakeholders are reluctant to share their fraud information [73]. This hinders research and affects the reproducibility of the experiments conducted. One possible solution is to use synthetically created data [74]. However, generating a realistic dataset presents enormous challenges in terms of topologies, attribute values of nodes and edges, community structures, data distributions, and correlations [74]. Furthermore, the similarity between synthetically generated networks and the original networks extracted from human behavior remains unanswered.

Table 4 presents an overview of the different publicly available data and datasets used among the studies reviewed. It shows that 87.2% of the studies tested their approach using real-world data (34/39), of which 41.0% are publicly available for research studies (16/39). A third of the 39 studies used synthetic data. Among the studies using publicly available datasets, 81.3% used OSN data (13/16), reflecting their broad availability for anomaly detection research.

5.6. Evaluation measures

As presented in Table 4, research studies have used different mathematical measures to evaluate the outcome of their proposed algorithms. For those with sufficiently available labeled data, the classical criteria based on receiver operating characteristic (ROC) or precision–recall (PR) curves have been used to analyze the performance of the proposed algorithms. ROC curves are commonly used to present the results for binary decision problems in machine learning [75,76]. However, with highly skewed datasets, ROC does not provide much insight into the data, and PR curves tend to provide a more informative picture of an algorithm's performance. In fraud detection, the number of negative samples considerably exceeds that of positive examples. Consequently, a substantial change in the number of false positives (FPs) can lead to a small change in the FP rate used in the ROC analysis [75,76].

Furthermore, precision captures the effect of many negative examples on the algorithm's performance by comparing FPs to true positives rather than to true negatives [75,76]. F-measure is the second most commonly used performance measure. This preference over the next measure, i.e., accuracy, comes as no surprise given the nature of fraud problems. Accuracy favors true negative, which is inconsequential in fraud detection. Instead, a measure that weighs higher on false negative (FN) and FP is of better value in an uneven class distribution. In such cases, the F-measure is preferred as it balances precision and recall, resulting in a better evaluation of a fraud detection model. Moreover, we observe that accuracy is only used in five studies [58,62,65,67,68] (see Table 4).

Although some measures are preferred over others, no measure is perfect, and they can only serve as an approximation to a technique's performance on a specific dataset. Ideally, the evaluation is checked against authentic data sourced from the specific problem, which the fraud detection technique is designed for. However, in practice, authentic labeled datasets are in short supply or nonexistent [14]. This limitation is further complicated by the need for expert knowledge to create a labeled dataset or evaluate results during model development, a time-consuming and expensive process. As a compromise or balance, many have used a case study analysis on samples of the data as a proxy of a technique's true capability. Nevertheless, evaluating the performance of fraud detection algorithms will always be a problem given the insufficient data samples and scenarios. An alternative is to use an ensemble of fraud detectors along with computer-based knowledge sources [77]. Lastly, a recent study [78] discussed two new approaches, called excess-mass (EM) and mass–volume (MV) curves, to evaluate the performance of anomaly detection approaches on dimensional data without data labels. However, to the best of our knowledge, the two approaches have not been applied in anomaly detection or fraud detection on graph data.

5.7. Recommendations

Table 5 summarizes the main contributions and specific types of fraud across the 39 research studies. It highlights their problem focus, approaches to finding solutions, challenges faced in the process, and recommended directions for future studies. This table offers a quick guide of relevant works for researchers using GBAD approaches to investigate frauds in networks, informing them of the range and nature of application problems faced, GBAD baseline approaches to consider, and unsettled areas for further investigations. In preparing Table 5, we further identified four key challenges. We propose some recommendations and considerations that serve as a scaffold for the future design of fraud detection mechanisms to address these challenges.

5.7.1. Dealing with unavailability of data

Fraud is a highly sensitive topic, and many stakeholders are reluctant to share their information on fraud. One of the major challenges in data sharing in various application areas, such as healthcare, insurance, and banking, are regulations that prohibit the transmission and distribution of highly confidential personal and financial data. This challenge poses a major obstacle in fraud detection research in sectors where data contain confidential information. Consequently, many fraud detection algorithms resort to mathematical evaluation measures, which, as we noted, are the best that we can get in a scenario where only a few databases are available for research. This issue has also urged researchers using synthetic datasets with different characteristics to test their solution for the problem they are looking to address. Synthetic network generators generally duplicate a small subset of the original network's properties for specific applications, such as community detection [79]. Usually, some sets of abnormal samples are injected into a predefined normal distribution of data (e.g., power-law networks) to generate synthetic data for fraud or anomaly detection [79]. If we further consider the fact that the proposed method is evaluated over mathematical measures, then the overall reliability of the empirical evaluation of a fraud detection model may not be a good reflection of the actual problem and use case [74,79,80].

The main challenge in producing synthetic datasets is to make the generated networks mimic various aspects of human behavior, including noise and randomness, as how these characteristics are incorporated will determine the realism of the simulated networks [74]. With synthetic data, the characteristics of the dataset can impact the performance of any new methods developed. Researchers should ensure that the simulated data are reflective of the actual network that the new

Table 4
Mapping catalog for types of datasets, public data used, and evaluation measures.

Graph methods	Application areas	Reference	Availability of data labels	Types of dataset	Types of evaluation measures
Structural-based	OSN	[35]	US	P (Twitter, Tencent Weibo), SY, RW	PR curve, run-time, accuracy
		[2]	US	P (Amazon, TripAdvisor, Epinions, WikiVote), SY, RW	F-measure, run-time
		[36]	US	RW	PR, F-measure
	Insurance	[5]	S	RW	F-measure, ROC
		[37]	US	P (Medicare-B), RW	Case study
	AML	[38]	US	No experimental data	No experimental study
		[39]	US	RW	Pearson's correlation of features
Community-based	OSN	[40]	US	SY, RW	Run-time, recall, convergence time
		[41]	US	P, SY, RW (Amazon, iTunes)	AUC of PR, NMI
		[42]	US	P, RW (Amazon, Yelp)	Precision, F-measure, CDF
		[43]	US	P, RW (Twitter)	Power-law analysis
		[44]	US	P, RW (Twitter Honeypot)	TPR, FPR, PR, F-measure
	AML	[45]	US	SY	Visual analytics
	Banking	[46]	SS	RW	ROC
	Trading	[47]	US	RW (Roget, Stock)	Run-time, case study
	IOF	[48]	US	P, RW (CERT)	Case study
	Online Auction	[49]	US	RW	NDCG
		[50]	SS	RW	NDCG
	Telecom	[51]	US	RW	CDF
		[52]	S	RW	PR, F-measure, ROC
	Retail Holding	[53]	US	RW	Case study
Decomposition-based	OSN	[54]	US	SY	ROC
		[55]	US	P, RW (Yelp, Amazon, BeerAdvocate)	F-measure, ROC
		[56]	US	P, RW (Yelp, Android, YahooM, KoWiki, ENWiki, YouTube)	ROC, detection time
		[57]	US	P, SY, RW (Software Marketplace, Reddit)	PR, F-measure
Compression- based	Trading	[7]	US	SY	Case study
		[8]	US	SY, RW	Case study
	OSN	[27]	US	P, RW (Flipkart)	Precision
	Insurance, AML, Banking, Trading	[58]	US	P, SY, RW (German Credit Card, ICIJ Offshore Leaks, COIL2000 insurance)	Accuracy
Probabilistic-based	Insurance	[59]	US	RW	Case study
		[60]	US	RW	AUC
	OSN	[61]	US	P, SY, RW (Goodreads, Buzzcity)	Precision
		[62]	US	P, RW (Yelp)	PR, F-measure, accuracy, AP, ROC
		[63]	US, SS	P, RW (Yelp)	AP, AUC
		[64]	US	RW	PR, F-measure, accuracy
	Online auction	[65]	US	SY	AUC, TPR, FPR
	OCA	[66]	US	RW	Hit rate, TPR
	IOF	[67]	US	SY, RW	Accuracy, ROC
		[68]	US	SY, RW (CMU-CERT Insider Threat)	AUC, ROC

S, supervised; U, unsupervised; SS, semi-supervised;
P, public datasets; SY, synthetic datasets; RW, real-world datasets;
PR, precision–recall; ROC, receiver operating characteristics; AP, average precision; NMI, normalized mutual information; TPR, true positive rate; FPR, false positive rate;
CDF, cumulative distribution function;
NDCG, normalized discounted cumulative gain.

algorithm is designed to detect fraud [74,80]. Otherwise, the performance of the algorithm evaluated within simulated environments will not reflect real-world networks [80]. Hence, we recommend evaluating algorithms on synthetic data and real-world datasets whenever possible.

On real-world datasets, studies published to support the research community are not without their own challenges. During our review, we noted that some real-world datasets have missing elements or that only part of the dataset is made publicly available. These issues create a challenge in terms of allowing the community to effectively evaluate any new methods developed against a published piece of work that used the full dataset. Without the means to adequately benchmark new algorithms, the progress of research in this area will be slow or limited [80].

Data anonymization can address this issue by hiding confidential information while maintaining the analytical utility of the data [81]. This technique allows data scientists and organizations to engage in a win–win collaboration. Data scientists will have the chance to analyze data in different areas and share their discoveries with businesses. In turn, businesses can be equipped with new fraud detection methodologies.

However, in some cases, even anonymized data have business value for the party owning them. Unauthorized disclosure of such data, as such, may damage the party owning them or other parties affected by their disclosure [82]. Here, data confidentiality still matters even after data anonymization, because clever adversaries can reidentify or deanonymize the information hidden in anonymized data by linking anonymized data to outside information to unearth the true identity of the data subjects [82]. While not suggesting that all anonymization techniques fail to protect privacy, we caution that some techniques have proven to be difficult to reverse [82]. Some researchers reject anonymization as a privacy-protecting panacea [82].

Nevertheless, this challenge should motivate us to continue to explore, or reexamine, the possibility of adapting synthetic data as an

Table 5
Domain of interest, highlights of the research, challenges faced, and future directions.

Graph methods	Application areas	Reference	Focus of analysis	Highlights of approach and detection improvements	Challenges (C) and future directions (D)
Structural-based	OSN	[35]	Detecting synchronized behavior (suspicious nodes that have an extremely similar behavioral pattern) and rare behavior (nodes with connectivity patterns very different from the majority) to spot fake followers and fake accounts	- Effectiveness: high accuracy in spotting synchronized behaviors and catching suspicious source-target groups - Scalability: linear complexity with the number of edges - Parameter-free - Oblivious side information	**D:** Incorporate temporal information and other additional features
		[2]	Spotting fraudsters in the presence of camouflage or hijacked accounts to detect fake followers and fake accounts	- Effectiveness: using sufficient condition to detect fraudsters perfectly (e.g., 100% precision and recall) - Scalability: linear complexity with the number of edges	**D:** Incorporate temporal information
		[36]	Spotting suspicious behaviors in online social communities	- Scalability: scalable to a large volume of data using big data in-memory cluster computing	**C:** Dependent on a user-selected similarity threshold
	Insurance	[5]	Assessing healthcare fraud risk to detect fraudulent providers	- Effectiveness: F-measure of 0.919 and an ROC area of 0.960	**C:** Lack of providers known to have committed healthcare fraud **D:** Include additional types of information relevant to healthcare fraud prediction
		[37]	Analyzing healthcare fraud to detect fraudulent insurance claims	- Effectiveness: detecting previously unreported anomalies	**C:** Model fuzzy graphs
	AML	[38]	Detecting patterns of money laundering and financing terrorism	- Incorporating fuzzy concepts	**C:** Use user parameters based on data from past events **D:** Analyze bigger data samples **D:** Include additional control variable, such as age and size of the companies
		[39]	Detecting patterns of money laundering to assess risk profiles of clients involved in the factoring business	- Introducing a predictive (rather than just a detective model) model for AML - Using a visual analysis of network data for any suspiciousness detection	**C:** Use user-defined parameters that depend on data from past events
Community-based	OSN	[40]	Detecting fraud in Internet advertising for crowd fraud detection	- Requiring nearly no human interaction - Scalability: scalable to a large volume of data - Effectiveness: accuracy over 90%	**C:** Capture fraud from a vast number of attack sources with low fraudulent traffic
		[41]	Detecting opinion spammer groups in the existence of camouflage	- Effectiveness: NMI of over 0.94 for various settings and over 0.95 AUC of PR curve on synthetic data and high accuracy on real-world data - Robustness: robust with a variety of parameters, so it requires almost no tweaking of parameters to work correctly	
		[42]	Detecting product review spammers	- Effectiveness: outperforming baselines over all databases used in experiments	**C:** Evaluate the annotation of a huge volume of review data manually **C:** Sloppiness in user evaluation
		[43]	Analyzing re-tweeting to find fake users in the presence of camouflage	- Introducing RTGEN, a scalable realistic synthetic data generator	**C:** Spot long-term spam activities in the presence of camouflage
		[44]	Analyzing tweeting activities for spamming community detection	- Effectiveness: outperforming baseline methods with a precision, recall, F-measure, and TP rate over 0.85 and FP rate of 0.132	**D:** Evaluate the approach based on more realistic data
	AML	[45]	Analyzing mobile payments to detect money laundering	- Introducing an interactive visualization application	**C:** Use limited visualization techniques
	Banking	[46]	Analyzing payment transactions for cross-channel frauds	- Effectiveness: reducing FPR by 63%	
	Trading	[47]	Analyzing trading ring patterns to discover cross-account collaborative fraud for market manipulation	- Scalability: several orders of magnitude faster than the baseline	**C:** Correlate user behaviors across multiple trading accounts
	IOF	[48]	Analyzing enterprise users' web access pattern to detect insider threats	- Introducing an interactive visualization application	**C:** Rely on some user-defined threshold parameter that should be refined
	Online Auction	[49]	Analyzing the social graph of online auction users to detect auction fraud	- Effectiveness: detects suspicious nodes as the compared baseline	
		[50]	Analyzing the social graph of online auction users to detect auction fraud	- Effectiveness: outperforming baseline with 5.3% in NDCG - Scalability: parallelize in MapReduce	**C:** Detect the homophilic behavior of auction fraudsters who frequently bid in auctions hosted by a seller(s) working in the same collusion group
	Telecom	[51]	Analyzing voice calls to detect fraud in a cellular network	- Effectiveness: detecting 85% of all the victims and the root cause of 78% of fraud calls	**D:** Apply additional (expensive) approaches, e.g., incorporating billing information, manual investigation,

(*continued on next page*)

Table 5 (*continued*)

Graph methods	Application areas	Reference	Focus of analysis	Highlights of approach and detection improvements	Challenges (C) and future directions (D)
					user calls history, and instant user fraud reports to analyze the detection results to further confirm the fraud activities
		[52]	Detecting telecom fraud	- Effectiveness: outperforming baseline methods with a precision, AUC, and F-measure over 0.80 and recall over 0.74	**C:** Analyze varieties of callers' and callees' behaviors in the telecom network to capture all types of telecom fraud
	Retail Holding	[53]	Detecting fraudulent transfer pricing when two subsidiaries agree to overprice imports or underprice exports to declare less profit to pay less tax	- Using data visualization to find hot spots for fraud	**C:** Rely on data quality and availability to reveal internal relations between companies and their affiliated domain users
Decomposition-based	OSN	[54]	Detecting random link attackers	- Effectiveness: low false negatives	**C:** Rely on some historical data for further analysis
		[55]	Detecting suspicious spikes of bursts and drops, in the existence of camouflage	- Scalability: sub-quadratic time complexity - Effectiveness: achieving higher accuracy than the competitors	**C:** Aggregate suspiciousness signals from different attributes
		[56]	Analyzing stream changes in tensors for fake rating detection	- Scalability: a million times faster - Effectiveness: detecting previously unreported anomalies	
		[57]	Analyzing dense blocks in tensors to detect bot-like behaviors	- Scalability: linearly scalable with the size of the data - Generalizability: being applied to a variety of domains - Effectiveness: scoring the suspicious entities with high accuracy and detected previously unreported anomalies	
Compression- based	Trading	[7,8]	Analyzing business transactions and processes to detect deceptive orders	- Effectiveness: minimum or no false positives	**C:** Find anomalies in graph-based data where the anomalous substructure in a graph is part of (or attached to or missing from) a non-anomalous substructure or the normative substructure
	OSN	[27]	Analyzing user-product ratings to find rating fraud	- Effectiveness: 0.87 precision over the top 100 results - Scalability: logarithmic scalability with the number of nodes and linear to the number of edges	**C:** Granularity in user behavior (e.g., different users may rate products in different ways)
	Insurance, AML, Banking, Trading	[58]	Analyzing financial and trading transaction to detect financial fraud	- Effectiveness: better detection results on sparse graphs - Ability to trace the origin of suspicious activities	**D:** Incorporate temporal information
Probabilistic-based	Insurance	[59]	Analyzing the relations between providers (hospitals) and consumers (cities) to find healthcare fraud committed by hospitals	- Effectiveness: detecting previously unreported anomalies - Visual analysis and manual labeling	**D:** Detect anomalies in big cities with very distributed anomalies **D:** Use more precise evaluations because of the limitation of evaluation using visual analysis and manual labeling
		[60]	Detecting automobile insurance fraud	- No requirement for the availability of large data - The imputation of the domain expert's knowledge - Adopted to new types of fraud as soon as they are noticed	**C:** Rely on some user-defined threshold/ factor parameters that should be refined
	OSN	[61]	Detecting opinion spammers	- Effectiveness: significant performance gains compared with the baselines	**C:** Make a clear split between opinion groups
		[62]	Analyzing online reviews for fake review detection	- Robustness: robust to data sparsity - Effectiveness: highly outperforms the baselines - Model parameters are refined through a learning algorithm	**C:** Model the distributions of objects' reviews and users' credibility from sparse review data
		[63]	Analyzing online reviews for spam review detection	- Effectiveness: outperforming the existing methods in AUC and AP - Scalability: linearly scalable with the number of edges	**D:** Incorporate product feature for spammer detection **D:** Incorporate meta-path concept for group spammer detection
		[64]	Detecting organized spammers in micro-blogging	- Effectiveness: accuracy of 93.6% for all the topics and an F1-score of 82.1% for anomalous topics	**C:** Detect anomalous topics hijacked by spammer groups from numerous trending topics **C:** Detect the hijacked long-term topics that lasted for days **C**: Scalability issue on large data **D:** Detect new evolving types of spammers

(*continued on next page*)

Table 5 (*continued*)

Graph methods	Application areas	Reference	Focus of analysis	Highlights of approach and detection improvements	Challenges (C) and future directions (D)
	Online auction	[65]	Analyzing the social graph of online auction users and detect auction fraud, including shilling fraud, reputation manipulation, and non-delivery fraud	- Effectiveness: ability to detect all three types of fraud (with an AUC of over 0.98, TPR of over 0.97, and an FPR of 0.05) that may happen in an auction, while the existing methods are tuned to detect just one of those types each - Scalability: linearly scalable with the number of bids	**C/D:** Rely on some user-defined parameters that should be refined
	OCA	[66]	Analyzing transaction data for credit application fraud detection	- Real-time scoring of incoming transaction streams - Effectiveness: low false alarm rates and achievement of consistent hit rates	**C:** Scalability is a major limitation as there is a trade-off between efficiency (rapid detection time and high scalability) and effectiveness (high hit and low false alarm rates)
	IOF	[67]	Analyzing companies' general ledger to find accounting fraud	- Scalable: linearly scalable with the number of edges - Robustness: robust with a variety of parameters, so it requires almost no tweaking of parameters to work correctly - Effectiveness: high labeling accuracy of up to 97% compared with spectral clustering - Generalizability: can be applied to a variety of domains	**C:** Rely on experts to assess fraudulent behaviors based on the associated risk of each account
		[68]	Detecting insider threats in a company	- Effectiveness: AUC of 0.9520, 6% improvement of ROC over the best performing baselines	**C:** Make more genuine alarms over a user profile that usually undergoes some continuous changes over time

alternative to alleviate the data privacy issue. Synthetic network generators offer a common benchmark allowing multiple groups of researchers to evaluate their research on the same dataset. However, many algorithms that perform well on synthetically generated networks may perform poorly in real applications [80] because real data are often messy, possessing isolated nodes, strange degree distributions, and unbalanced class distributions. Thus, many challenges relating to synthetically generated networks remain. While it is important to continue to develop new and better algorithms, there should also be research into areas that answer the following questions: How good or realistic are the synthetically generated networks? Should this be a measure, or are there other ways to gauge this? How can noise and randomness be incorporated in the generated networks so that it is as close to the type of network that we wish our fraud detection algorithms to be dealing with [74]? How can the efficiency of different synthetic network generators be evaluated?

5.7.2. *Keeping track of network user activities over different timestamps*

Most real-world networks evolve and fraudsters leverage their dynamics to evade detection by spreading and altering their activities over time, thus camouflaging their real intent, i.e., their fraudulent activities [41]. This characteristic makes detecting fraudsters behavior even more challenging. Therefore, core criminal behavior that can withstand such changes over time should be understood [41].

Our literature review shows that research on fraud detection in dynamic networks is scarce (see Section 5.3.4), leaving a research gap that needs to be urgently filled, particularly with the prevalence of OSNs. Therefore, we strongly suggest that the design of fraud detection solutions should consider employing a time-evolving network structure to continuously track suspicious activities across different time-based snapshots.

Dealing with these time-evolving network structures requires several key considerations (see Table 5). One consideration is that solutions for these networks need to be scalable to balance the trade-off between efficiency (rapid detection time and high scalability) and effectiveness (high hit and low false alarm rates) [66]. It is also important to ensure that the solution is robust because a time-evolving network structure has data sparsity issues [62]. Hence, suspicious activities from different attributes and times of evolving network structures should be aggregated [55]. As a result, the algorithms developed for such networks need to consider new data characteristics.

5.7.3. *Investigating the inherent multiplex behavior of network users*

Our review analysis shows that many current studies do not consider the intrinsic multiplex nature of human interactions. They tend to investigate users' behavior in simplex social networks, focusing on just one type of activity. However, capturing different aspects of relations and activities among the same individuals can give more clues to detect any suspicious activity (e.g., individuals may have different kinds of activities within an online social media platform, such as making friends, sending messages, reviewing profiles, liking posts, and poking). Thus, all kinds of activities should be analyzed to reveal any suspicious activity [25].

A multiplex network contains multiple layers that share the same sets of nodes, with each layer representing one type of communication among entities. Analyzing just one mode of interaction cannot provide a complete picture of the relationships among network users. Therefore, to identify anomalies and suspicious activities in multiplex networks, we suggest examining the rich information hidden in individual network layers [72]. Detecting suspicious activities in multiplex networks remains a relatively unexplored research area.

We suggest that multiplex networks should be given higher attention because social interactions in communities comprise different and multiple relationship types [25,72]. Therefore, it will be inadequate, if not unrealistic, to focus on a singular view using simplex social networks to detect fraudulent activities. We advocate that a pragmatic design for fraud detection solutions or algorithms should acknowledge and consider the varieties and abundance of human interactions that multiplex networks better capture. Neglecting such a multiplicity of human interactions can lead to information loss and may obscure important information from being discovered [25,72]. Furthermore, such interactions in multiplex networks are digital footprints of potential fraudsters that need to be holistically represented and extracted as important evidence for combating frauds and possibly crimes [25,72]. Consequently, feature engineering and graph representation learning (also called graph embedding) techniques are reported as the two main families of approaches for extracting and representing the structural features or characteristics of multiplex networks (see Section 4.5).

5.7.4. Eliminating human intervention in structural information extraction

Recently, there has been a surge towards the use of graph representation learning (or graph embedding) techniques to automatically encode the structural information about the network [33]. The key idea behind these approaches is to learn a mapping that embeds nodes, links, or the entire network into a lower-dimensional vector space to extract important hidden structural features. This is different from traditional approaches, such as feature engineering, which relies on prior knowledge of domain experts to hand-engineer features (e.g., degrees, clustering coefficients). In large and time-evolving networks, feature engineering is time-consuming, expensive, and, ultimately, lack scalability as detection models will need to be regularly updated to reflect the fraudster's altered behavior and activities [83]. Hence, we recommend the use of graph representation learning techniques to overcome these issues.

Graph representation learning techniques have shown to extract structural information from networks without the need for knowledge experts and can be adopted to learn and capture the structural information of time-evolving multiplex networks. This characteristic is attractive for fraud detection in our setting as it allows us to track fraudulent activities over time in a massive multiplex network for continuous learning in the detection model. As a result of recent developments in deep learning methods [29,34], there are now many graph representation learning techniques that can deal with massive network data. These techniques include graph convolutional networks [84], graph attention networks [85], and recurrent networks [86]. Another reason to seriously consider graph representation learning is that in many of the literature we reviewed, subsequent stages of fraud detection require the topological and structural characteristics of the network to be preserved. For example, many solutions include an anomaly detection stage that uses machine learning tasks (e.g., clustering and classifications) and require this information to operate.

All said, the role of human experts is irreplaceable for the time being. Any detected anomaly will still require domain knowledge assessment to make adjustments based on the given complex situations of an application domain. As far as automation goes, algorithms can assist with scoring to create blocking mechanisms [66] and block any suspicious fraudulent activities or behaviors by having regular expert input to improve the detection capability [68].

The four challenges are important considerations for those trying to develop new algorithms to effectively detect fraud within a time-evolving multiplex network. As we have learned from the various works in this review, a good algorithmic solution should follow a solution sketch (or exhibit characteristics):

- Ensure access to good multiplex network data that are either from the problem source or, if synthetically generated, capture the network characteristics;
- Exploit characteristics of time and multiplicity of relationships in these networks for better detection capabilities;
- Avoid feature engineering but, instead, consider a range of graph representation learning approaches for scalability and intrinsically capture important structural information; and
- Consider methods to automate feedback for continuous model learning and minimize human intervention using suitable machine learning techniques (see Section 4.4).

6. Conclusion and future research directions

This study aimed to identify, analyze, and synthesize various GBAD approaches employed in fraud detection research disseminated in data mining. Using eight questions that probe into specific aspects of GBAD-based fraud detection research, we developed a classification framework to systematically analyze 39 academic papers identified through a systematic literature search.

This study makes significant contributions in theory and practice. The proposed classification framework offers a systematic probe for researchers to gain a more insightful understanding of the application of GBAD techniques. The highlighted gaps challenge data scientists to embark on new empirical research in this domain. Equally, this paper also offers practitioners a roadmap to appreciate the correspondence between the nature of their network, different types of anomalies, and appropriate graph-based methods that serve their needs and application areas.

Our review also reveals that GBAD approaches have been employed for fraud detection in various application areas. Owing to the unavailability of public data, most research using GBAD approaches have focused on OSNs. Consequently, we see a dearth of research works on datasets where personal confidential information is embedded, e.g., in areas, such as banking, insurance, and healthcare.

GBAD techniques have potential applications in the FinTech enterprise. As an emerging term in the financial industry in recent years, FinTech has provided a convenient gateway to different online financial services [87]. The rapid growth and pervasive use of FinTech have made the financial industry vulnerable to various forms of online frauds and cyber-crimes [87]. As a result, the financial sector is ripe to embrace new technological advances to prevent and detect digital identity frauds [87], opening up directions for researchers to investigate the application of GBAD techniques in fraud detection in the FinTech industry. For example, Blockchain, an innovation by FinTech, has attracted considerable attention by enabling bitcoin-based online transactions [16]. As a form of digital currency that is fully transparent and not controlled by any central authority, Bitcoin is another example where the GBAD techniques can be used. Many websites are now involved in Bitcoin trading, and different forms of fraudulent activities may occur in this trading process. With no central authority to set the price of Bitcoin, various websites can offer different prices. For instance, a fake profile on a social media website can send false news regarding Bitcoin exchanges, with unsuspecting individuals conducting Bitcoin trading based on those fraudulent exchanges [88]. GBAD techniques can be used to predict a person's digital identity and to detect fraudulent connections, unreliable data patterns, or irregular activities. Some latest applications of GBAD techniques have shown that it is possible to assign a trust level to individual users to indicate how likely each individual will, for instance, repay a loan or if these individuals are who they say they are, based on data on each individual uncovered from the Internet [88].

Although these advancements increase the ability to identify high-risk individuals in advance, aggregating various sources of data to achieve predictive analytics raises ethical implications for a privacy violation, as was the case with Cambridge Analytica, which used Facebook data for predictive analysis [89]. The challenge is to identify new ways to safeguard individual privacy.

Another finding from our review is the dependency of research studies on domain knowledge for analyzing connectivity patterns in networks to detect suspicious activities. Our review found that only 28.2% of studies considered the dynamic nature of networks when analyzing anomalous activities. To address these problems, we suggest that (i) research studies should employ representation learning to lessen their dependence on domain knowledge [83] and (ii) business vendors should share their anonymized data for further analysis by data scientists to provide opportunities for new discoveries.

Our systematic literature review, although extensive, may have omitted some relevant studies owing to the limitations of the scientific databases, specific keywords employed in the search, and timeframe selected for this review. Furthermore, GBAD techniques have been widely employed for fraud detection in the OSN area, which covers a vast range of applications, such as e-commerce, online shopping, dating, online recommendation, and social media websites. Each application may be under the threat of different types of fraud (e.g., spam, deception and fake reviews, fake opinions, “Like” farms, advertising fraud, and cyberbullying), which may have been inadvertently excluded from our review because of the choice of keyword search. Therefore, a detailed analysis of different types of fraudulent activities in OSNs and the application of GBAD approaches for detecting such activities can be addressed in future review studies. Lastly, we exclusively selected papers from academic sources for review in this study. Future work will benefit by including non-academic sources where the application of GBAD techniques is reported.

References

[1] S. Velampalli, W. Eberle, Novel graph based anomaly detection using background knowledge, Proceedings of FLAIRS 2017, AAAI Press, 2017, pp. 538–543.
[2] B. Hooi, K. Shin, H.A. Song, A. Beutel, N. Shah, C. Faloutsos, Graph-based fraud detection in the face of camouflage, ACM Transactions on Knowledge Discovery 11 (4) (2017) 1–26.
[3] D. Savage, X. Zhang, X. Yu, P. Chou, Q. Wang, Anomaly detection in online social networks, Soc. Networks 39 (2014) 62–70.
[4] G.R. Kelly, Social media’s contribution to political misperceptions in U.S. presidential elections, PLoS One 14 (3) (2019) e0213500.
[5] L.K. Branting, F. Reeder, J. Gold, T. Champney, Graph analytics for healthcare fraud risk estimation, ASONAM 2016, IEEE, 2016, pp. 845–851.
[6] V. Chandola, S.R. Sukumar, J.C. Schryver, Knowledge discovery from massive healthcare claims data, Proceedings of SIGKDD 2013, ACM, 2013, pp. 1312–1320.
[7] W. Eberle, L. Holder, Mining for insider threats in business transactions and processes, CIDM 2009, IEEE, 2009, pp. 163–170.
[8] W. Eberle, L. Holder, Discovering structural anomalies in graph-based data, ICDMW 2007, IEEE, 2007, pp. 393–398.
[9] L. Akoglu, H. Tong, D. Koutra, Graph based anomaly detection and description: a survey, Data Min. Knowl. Disc. 29 (3) (2015) 626–688.
[10] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: a survey, ACM Comput. Surv. 41 (3) (2009) 1–58.
[11] K. Anand, J. Kumar, K. Anand, Anomaly detection in online social network: a survey, ICICCT 2017, IEEE, 2017, pp. 456–459.
[12] E. Ranshous, S. Shen, D. Koutra, S. Harenberg, Anomaly detection in dynamic networks: a survey, Comput. Stat. 7 (3) (2015) 223–247.
[13] S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland, Data mining for credit card fraud: a comparative study, Decis. Support. Syst. 50 (3) (2011) 602–613.
[14] A. Abdallah, M.A. Maarof, A. Zainal, Fraud detection system: a survey, J. Netw. Comput. Appl. 68 (2016) 90–113.
[15] E.W.T. Ngai, Y. Hu, Y.H. Wong, Y. Chen, X. Sun, The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature, Decis. Support. Syst. 50 (3) (2011) 559–569.
[16] J.J. Xu, Are blockchains immune to all malicious attacks? Financial Innovation 2 (25) (2016).
[17] A. Booth, A. Sutton, D. Papaioannou, Systematic Approaches to a Successful Literature Review, 2nd ed., Sage, London, 2011.
[18] E.W.T. Ngai, L. Xiu, D.C.K. Chau, Application of data mining techniques in customer relationship management: a literature review and classification, Expert Syst. Appl. 36 (2) (2009) 2592–2602.
[19] R.B. Frost, C.W. Choo, Revisiting the information audit: a systematic literature review and synthesis, Int. J. Inf. Manag. 37 (1) (2017) 1380–1390.
[20] T.K.H. Chan, C.M.K. Cheung, Z.W.Y. Lee, The state of online impulse-buying research: a literature analysis, Inf. Manag. 54 (2) (2017) 204–217.
[21] R.J. Bolton, D.J. Hand, Statistical fraud detection: a review, Stat. Sci. 17 (3) (2002) 235–255.
[22] R. Agrawal, M. Potamias, E. Terzi, Learning the nature of information in social networks, Proceedings of ICWSM 2012, AAAI Press, 2012.
[23] A. Kaveh, Introduction to graph theory and algebraic graph theory, Optimal Analysis of Structures by Concepts of Symmetry and Regularity, Springer Vienna, Vienna, 2013, pp. 15–35.
[24] S. Lee, S. Park, M. Kahng, S.-g. Lee, Pathrank: ranking nodes on a heterogeneous graph for flexible hybrid recommender systems, Expert Syst. Appl. 40 (2) (2013) 684–697.
[25] S. Fakhraei, J. Foulds, M. Shashanka, L. Getoor, Collective spammer detection in evolving multi-relational social networks, Proceedings of KDD15, ACM, 2015, pp. 1769–1778.
[26] P.V. Bindu, P.S. Thilagam, Mining social networks for anomalies: methods and challenges, J. Netw. Comput. Appl. 68 (Supplement C) (2016) 213–229.
[27] N. Shah, A. Beutel, B. Hooi, L. Akoglu, S. Gunnemann, D. Makhija, M. Kumar, C. Faloutsos, Edgecentric: Anomaly detection in edge-attributed networks, ICDMW 2016, IEEE, 2016, pp. 327–334.
[28] C.C. Noble, D.J. Cook, Graph-based anomaly detection, Proceedings of SIGKDD 2003, ACM, 2003, pp. 631–636.
[29] P. Goyal, E. Ferrara, Graph embedding techniques, applications, and performance: a survey, Knowledge Based Systems 151 (2018) 78–94.
[30] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi, Fame for sale: efficient detection of fake twitter followers, Decis. Support. Syst. 80 (2015) 56–71.
[31] Y. Bengio, A. Courville, P. Vincent, Representation learning: a review and new perspectives, IEEE Trans. Pattern Anal. Mach. Intell. 35 (8) (2013) 1798–1828.
[32] S.Y. Bhat, M. Abulaish, Community-based features for identifying spammers in online social networks, ASONAM 2013, IEEE, 2013, pp. 100–107.
[33] H. Cai, V.W. Zheng, K. Chen-Chuan Chang, A comprehensive survey of graph embedding: problems, techniques and applications, IEEE Trans. Knowl. Data Eng. 30 (9) (2017) 1616–1637.
[34] G. Zhong, L.-N. Wang, X. Ling, J. Dong, An overview on data representation learning: from traditional feature learning to recent deep learning, Journal of Finance and Data Science 2 (4) (2016) 265–278.
[35] M. Jiang, P. Cui, A. Beutel, C. Faloutsos, S. Yang, CatchSync: catching synchronized behavior in large directed graphs, Proceedings of SIGKDD 2014, ACM, 2014, pp. 941–950.
[36] H.C. Manjunatha, R. Mohanasundaram, BRNADS: big data real-time node anomaly detection in social networks, ICISC 2018, IEEE, 2018, pp. 929–932.
[37] J. Seo, O. Mendelevitch, Identifying frauds and anomalies in medicare-b dataset, EMBC 2017, IEEE, 2017, pp. 3664–3667.
[38] L.S. Bershtein, A. Tselykh, A clique-based method for mining fuzzy graph patterns in anti-money laundering systems, Proceedings of SIN 2013, ACM, 2013, pp. 384–387.
[39] A. Fronzetti Colladon, E. Remondi, Using social network analysis to prevent money laundering, Expert Syst. Appl. 67 (2017) 49–58.
[40] T. Tian, J. Zhu, F. Xia, X. Zhuang, T. Zhang, Crowd fraud detection in internet advertising, WWW 2015, International World Wide Web Conferences Steering Committee, 2015, pp. 1100–1110.
[41] J. Ye, L. Akoglu, Discovering opinion spammer groups by network footprints, ECML PKDD 2015, Springer International Publishing, 2015, pp. 267–282.
[42] Z. Wang, S. Gu, X. Zhao, X. Xu, Graph-based review spammer group detection, Knowl. Inf. Syst. 55 (3) (2018) 571–597.
[43] M. Giatsoglou, D. Chatzakou, N. Shah, C. Faloutsos, A. Vakali, Retweeting Activity on Twitter: Signs of Deception, PAKDD 2015, Springer International Publishing, 2015, pp. 122–134.
[44] P.V. Bindu, R. Mishra, P.S. Thilagam, Discovering spammer communities in twitter, J. Intell. Inf. Syst. 51 (3) (2018) 503–527.
[45] E. Novikova, I. Kotenko, Visual analytics for detecting anomalous activity in mobile money transfer services, Cd-Ares 2014, Springer International Publishing, 2014, pp. 63–78.
[46] I. Molloy, S. Chari, U. Finkler, M. Wiggerman, C. Jonker, T. Habeck, Y. Park, F. Jordens, R. van Schaik, Graph Analytics for Real-Time Scoring of Cross-Channel Transactional Fraud, FC 2016, Springer, Berlin Heidelberg, 2017, pp. 22–40.
[47] Z. Li, H. Xiong, Y. Liu, Mining blackhole and volcano patterns in directed graphs: a general approach, Data Min. Knowl. Disc. 25 (3) (2012) 577–602.
[48] A. Gamachchi, S. Boztaş, Web access patterns reveal insiders behavior, IWSDA 2015, IEEE, 2015, pp. 70–74.
[49] S. Liang, J. Zeng, C. Li, H. Chen, A framework for spotting anomaly, FSKD 2010, IEEE, 2010, pp. 2260–2264.
[50] P. Bangcharoensap, H. Kobayashi, N. Shimizu, S. Yamauchi, T. Murata, Two step graph-based semi-supervised learning for online auction fraud detection, ECML PKDD 2015, Springer International Publishing, 2015, pp. 165–179.
[51] J. Nan, J. Yu, S. Ann, H. Wen-Ling, J. Guy, P. Siva, Z. Zhi-Li, Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis, Proceedings of MobiSys 2012, ACM, 2012, pp. 253–266.
[52] H. Yan, Y. Jiang, G. Liu, Telecomm fraud detection via attributed bipartite network, ICSSSM 2018, IEEE, 2018, pp. 1–6.
[53] A. Tselykh, M. Knyazeva, E. Popkova, A. Durfee, A. Tselykh, An attributed graph mining approach to detect transfer pricing fraud, Proceedings of SIN 2016, ACM, 2016, pp. 72–75.
[54] P. Moriano, J. Finke, Model-based fraud detection in growing networks, CDC 2014, IEEE, 2014, pp. 6068–6073.
[55] S. Liu, B. Hooi, C. Faloutsos, HoloScope: Topology-and-spike aware fraud detection, Proceedings of CIKM 2017, ACM, 2017, pp. 1539–1548.
[56] K. Shin, B. Hooi, J. Kim, C. Faloutsos, DenseAlert: incremental dense-subtensor detection in tensor streams, KDD 2017, ACM, 2017, pp. 1057–1066.
[57] H. Lamba, B. Hooi, K. Shin, C. Faloutsos, J. Pfeffer, ZOORANK: Ranking Suspicious Entities in Time-Evolving Tensors, ECML PKDD 2017, Springer International Publishing, 2017, pp. 68–84.
[58] D. Huang, D. Mu, L. Yang, X. Cai, CoDetect: financial fraud detection with anomaly feature detection, IEEE Access 6 (2018) 19161–19174.
[59] L.F.M. Carvalho, C.H.C. Teixeira, W. Meira, M. Ester, O. Carvalho, M.H. Brandao, Provider-consumer anomaly detection for healthcare systems, ICHI 2017, IEEE, 2017, pp. 229–238.
[60] L. Subelj, S. Furlan, M. Bajec, An expert system for detecting automobile insurance fraud using social network analysis, Expert Syst. Appl. 38 (1) (2011) 1039–1052.
[61] H. Dai, F. Zhu, E.P. Lim, H. Pang, Detecting anomalies in bipartite graphs with mutual dependency principles, ICDM 2012, IEEE, 2012, pp. 171–180.
[62] X. Wu, Y. Dong, J. Tao, C. Huang, N.V. Chawla, Reliable fake review detection via modeling temporal and behavioral patterns, IEEE BigData 2017, IEEE, 2017, pp. 494–499.
[63] S. Shehnepoor, M. Salehi, R. Farahbakhsh, N. Crespi, NetSpam: a network-based spam detection framework for reviews in online social media, IEEE Transactions on Information Forensics and Security 12 (7) (2017) 1585–1595.
[64] Q. Dang, Y. Zhou, F. Gao, Q. Sun, Detecting cooperative and organized spammer

groups in micro-blogging community, Data Min. Knowl. Disc. 31 (3) (2017) 573–605.

[65] S. Tsang, Y.S. Koh, G. Dobbie, S. Alam, SPAN: finding collaborative frauds in online auctions, Knowl.-Based Syst. 71 (2014) 389–408.

[66] C. Phua, R. Gayler, V. Lee, K. Smith-Miles, On the communal analysis suspicion scoring for identity crime in streaming credit applications, Eur. J. Oper. Res. 195 (2) (2009) 595–612.

[67] M. McGlohon, S. Bay, M.G. Anderle, D.M. Steier, C. Faloutsos, SNARE: A link analytic system for graph labeling and risk detection, Proceedings of SIGKDD 2009, ACM, 2009, pp. 1265–1274.

[68] S.D. Bhattacharjee, J. Yuan, Z. Jiaqi, Y.P. Tan, Context-aware graph-based analysis for detecting anomalous activities, ICME 2017, IEEE, 2017, pp. 1021–1026.

[69] R.F. Lima, A.C.M. Pereira, A fraud detection model based on feature selection and undersampling applied to web payment systems, Wi-IAT 2015, IEEE, 2015, pp. 219–222.

[70] J. Meng, C. Peng, B. Alex, F. Christos, Y. Shiqiang, Catching synchronized behaviors in large networks: a graph mining approach, ACM Trans. Knowl. Discov. Data 10 (4) (2016) 1–27.

[71] M. Rahman, R. Recabarren, B. Carbunar, D. Lee, Stateless puzzles for real time online fraud preemption, WebSci 2017, ACM, 2017, pp. 23–32.

[72] T. Pourhabibi, Y.L. Boo, K.L. Ong, B. Kam, X. Zhang, Behavioral analysis of users for spammer detection in a multiplex social network, AUSDM 2018, Springer Singapore, 2019, pp. 228–240.

[73] J. West, M. Bhattacharya, Intelligent financial fraud detection: a comprehensive review, Computers & Security 57 (2016) 47–66.

[74] D.F. Nettleton, A synthetic data generator for online social network graphs, Soc. Netw. Anal. Min. 6 (1) (2016) 44.

[75] J. Davis, M. Goadrich, The relationship between precision-recall and roc curves, Proceedings of ICML 2006, ACM, 2006, pp. 233–240.

[76] L.A. Jeni, J.F. Cohn, F. De La Torre, Facing imbalanced data recommendations for the use of performance metrics, ACII 2013, IEEE, 2013, pp. 245–251.

[77] H. Fanaee, J. Gama, Event labeling combining ensemble detectors and background knowledge, Progress in Artificial Intelligence 2 (2) (2014) 113–127.

[78] N. Goix, How to evaluate the quality of unsupervised anomaly detection algorithms? ArXiv.1607.01152, 2016. https://arxiv.org/abs/1607.01152.

[79] L. Akoglu, C. Faloutsos, RTG: a recursive realistic graph generator using random typing, Data Min. Knowl. Disc. 19 (2) (2009) 194–209.

[80] A.M. Ali, Synthetic Generators for Simulating Social Networks, Department of Electrical Engineering and Computer Science, University of Central Florida, 2014.

[81] B. Eze, L. Peyton, Systematic literature review on the anonymization of high dimensional streaming datasets for health data sharing, Procedia Computer Science 63 (2015) 348–355.

[82] P. Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, UCLA Law Rev. 57 (2009) 1701.

[83] W.L. Hamilton, R. Ying, J. Leskovec, Representation learning on graphs: methods and applications, IEEE Data Engineering Bulletin 40 (2017) 52–74.

[84] M. Schlichtkrull, T.N. Kipf, P. Bloem, R. van den Berg, I. Titov, M. Welling, Modeling relational data with graph convolutional networks, ESWC 2018, Springer International Publishing, 2018, pp. 593–607.

[85] P. Shaw, J. Uszkoreit, A. Vaswani, Self-attention with relative position representations, ArXiv.1803.02155, 2018. https://arxiv.org/abs/1803.02155.

[86] R.B. Palm, U. Paquet, O. Winther, Recurrent relational networks, ArXiv.1711.08028, https://arxiv.org/abs/1711.08028, (2018).

[87] Y. Shim, D.H. Shin, Analyzing China's fintech industry from the perspective of actor-network theory, Telecommun. Policy 40 (2) (2016) 168–181.

[88] A. Viswam, G. Darsan, An efficient bitcoin fraud detection in social media networks, ICCPCT 2017, IEEE, 2017, pp. 1–4.

[89] T. Jiya, Ethical implications of predictive risk intelligence, ORBIT Journal 2 (2) (2019).

Tahereh Pourhabibi is a Ph.D. candidate in the School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, Australia. She received her Master of Science in Artificial Intelligence from Al-Zahra University, Tehran, Iran. Her research interests include machine learning, data mining, anomaly detection, and their application in suspicious activity detection and fraud detection.

Kok-Leong Ong is an Associate Professor at the Centre for Data Analytics and Cognition, La Trobe University. He received his Ph.D. in 1999 and B. A. Sc. (Hons) in 2004 from the Nanyang Technological University, Singapore. His research interest includes data mining and analytics, and machine learning and AI, and his works have been supported by over $1.46m of grants to-date. He has published over 80 peer-reviewed papers and has served in over 60 Program Committees.

Booi H Kam is a Professor in the School of Accounting, Information Systems and Supply Chain, RMIT University. His current research interests are in areas of strategic digital supply chain operations and supply chain relationships. A recipient of an Emerald Literati Network Awards for Excellence, Booi is regularly invited by universities in China, England, France, Korea, and Taiwan to give public lectures and teach into their degree programs. Booi holds a Ph.D. from the University of California at Los Angeles. He co-authors Consumer Logistics, a book by Edward Elgar Publishing.

Yee Ling Boo received her Ph.D. in Information Technology from Monash University Australia. She is currently a lecturer at the School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, Australia. Her research interests include Data Mining, Brain-Inspired Computing, Cognitive Analytics, and their applications in business, education, and health. Before the pursuit of her Ph.D. degree, she was a software engineer in Malaysia. Her research works have appeared in reputable journals and conferences.