BIG DATA MINING AND ANALYTICS
ISSN 2096-0654 09/15 pp419–444
DOI: 10.26599/BDMA.2023.9020023
Volume 7, Number 2, June 2024

E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review

Abed Mutemi* and Fernando Bacao

Abstract: The e-commerce industry's rapid growth, accelerated by the COVID-19 pandemic, has led to an alarming increase in digital fraud and associated losses. To establish a healthy e-commerce ecosystem, robust cyber security and anti-fraud measures are crucial. However, research on fraud detection systems has struggled to keep pace due to limited real-world datasets. Advances in artificial intelligence, Machine Learning (ML), and cloud computing have revitalized research and applications in this domain. While ML and data mining techniques are popular in fraud detection, specific reviews focusing on their application in e-commerce platforms like eBay and Facebook are lacking depth. Existing reviews provide broad overviews but fail to grasp the intricacies of ML algorithms in the e-commerce context. To bridge this gap, our study conducts a systematic literature review using the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) methodology. We aim to explore the effectiveness of these techniques in fraud detection within digital marketplaces and the broader e-commerce landscape. Understanding the current state of the literature and emerging trends is crucial given the rising fraud incidents and associated costs. Through our investigation, we identify research opportunities and provide insights to industry stakeholders on key ML and data mining techniques for combating e-commerce fraud. Our paper examines the research on these techniques as published in the past decade. Employing the PRISMA approach, we conducted a content analysis of 101 publications, identifying research gaps, recent techniques, and highlighting the increasing utilization of artificial neural networks in fraud detection within the industry.

Key words: E-commerce; fraud detection; Machine Learning (ML); systematic review; organized retail fraud

1 Introduction

1.1 Background

The COVID-19 pandemic has accelerated the shift towards online communication and e-commerce platforms. Today, more people than ever before carry out everyday tasks online and at home, such as work, school, shopping, doctor's appointments, and entertainment[1]. Noteworthy growth has especially been witnessed on e-commerce platforms, like Amazon, eBay, and the Facebook Marketplace, most of which has been fueled by reduced mobility for fear of contracting the virus.

As more people utilize digital devices and e-commerce platforms, cybercrimes and frauds have significantly increased[2], continuing the trend of costing the global economy billions of dollars and jeopardizing public safety[3].

Cybercrime and fraud cover a wide range of abhorrent behaviors, including extortion and blackmail,

• Abed Mutemi and Fernando Bacao are with NOVA Information Management School (NOVA IMS), Universidade Nova de Lisboa, Campus de Campolide, Lisboa 1070-312, Portugal. E-mail: d20200455@novaims.unl.pt; bacao@novaims.unl.pt.
* To whom correspondence should be addressed.
Manuscript received: 2023-05-13; revised: 2023-07-15; accepted: 2023-08-22

denial of service, phishing, malware, fraudulent e-commerce, romance scams, and tech support scams[2]. Additionally, credit card theft, money laundering, and fraudulent financial transactions are widespread in the digital age[2, 4]. These actions have a negative impact on businesses and clients, posing serious risks to their finances, reputations, and mental health.

According to a recent analysis by Juniper Research, losses related to online payments on e-commerce platforms are growing at a staggering rate of 18 percent annually[5]. This highlights the critical importance of studying this area to inform fraud detection or prevention strategies to slow down the upward trend.

Frequently, current strategies are unable to keep up with fraudsters, who are constantly adapting and changing their methods to exploit the platforms[6]. What is more, low research and development efforts fueled by a lack of practical data and the need for businesses to protect their platform vulnerabilities further exacerbate the issue. For example, it makes no sense to describe fraud detection or prevention methods in the open since doing so would arm fraudsters with the knowledge they need to avoid detection[1].

In literature, addressing fraud of any kind can take two forms: (1) Prevention, which refers to steps taken to avert the occurrence of the acts in the first place. This includes intricate designs, personal identity numbers, internet security for online interactions with digital platforms, and passwords and authentication mechanisms for computers and mobile devices[7]. Prevention techniques are not perfect; frequently, a trade-off between cost (for the business) and discomfort (for the customer) must be made. (2) On the other hand, detection entails recognizing fraudulent acts as soon as they occur[7]. When prevention fails, detection becomes material. For example, we can prevent credit card fraud by protecting our cards insidiously, but if the card information is stolen, we must notice the fraud as soon as possible[8]. Since neither form above is perfect in reducing the risks and effects of fraud, production systems often consider a combination of the two to combat fraud. In this review, we limit our focus to detection systems.

There are two schools of thought regarding fraud detection systems. The first is in favor of statistical and computational methods, and researchers in this area include Refs. [6–8]. To identify fraud, this way of thinking applies statistical tools, including ML algorithms. Typically, labeled data are used to train classifiers to distinguish between the two classes (fraudulent and non-fraudulent). This implementation feeds classifiers information from user profiles, including transaction values, day of the week, item category, age, gender, and geographic location. Those who argue against statistical and computational methods claim that these features are easy for sophisticated fraudsters to fabricate[9]. Irani, Pu, and Webb[10, 11] believe that once fraudsters discover that authorities have picked up on their jargon, they can avoid keyword traps by switching to new expressions. Network analysis is advocated by the second school of thought as an alternative approach to creating fraud detection features[9, 12]. In order to derive graph-theoretical variables or scores that specifically characterize nodes of fraud, the concept makes use of the connectedness between the nodes, which are often users or items in a dataset. The theory underlying identification strategies is that abnormal users display connection patterns that are different from those of typical users[9]. In our review, we focus on the first school of thought.

E-commerce platforms have intricate design architectures and multiple points of vulnerability (explored later in Section 4), which fraudsters and attackers could use against them. In Figs. 1 and 2, we illustrate a commonly used e-commerce/marketplace architecture in the industry to illustrate the complexity of these platforms. At a high level, an e-commerce platform comprises three layers, as shown in Fig. 1. (1) The presentation layer, which is the part that is presented to the customer. It is the user interface and communication part of the architecture, where the customer interacts with the website on the front end and the application collects data and processes requests on the back end; (2) The business layer, also known as the application or service layer, uses business logic, a specific set of business rules, to gather and process information. It can also delete, add, or change information in the data layer; (3) The data layer, which is also known as the database layer, is the final layer and is used for storing data and processing requests. In light of this complex design, we posit that the statistical and computational approach (application of ML and data mining techniques) is best suited for combating fraud on these platforms. Figure 2 not only shows the detailed connections between the tiers presented in Fig. 1, but also includes third-party connections that

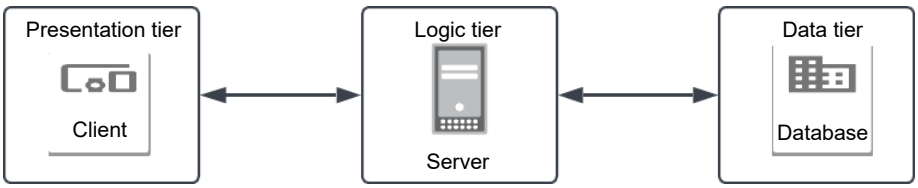

Fig. 1 High-level diagram of an e-commerce platform design architecture.

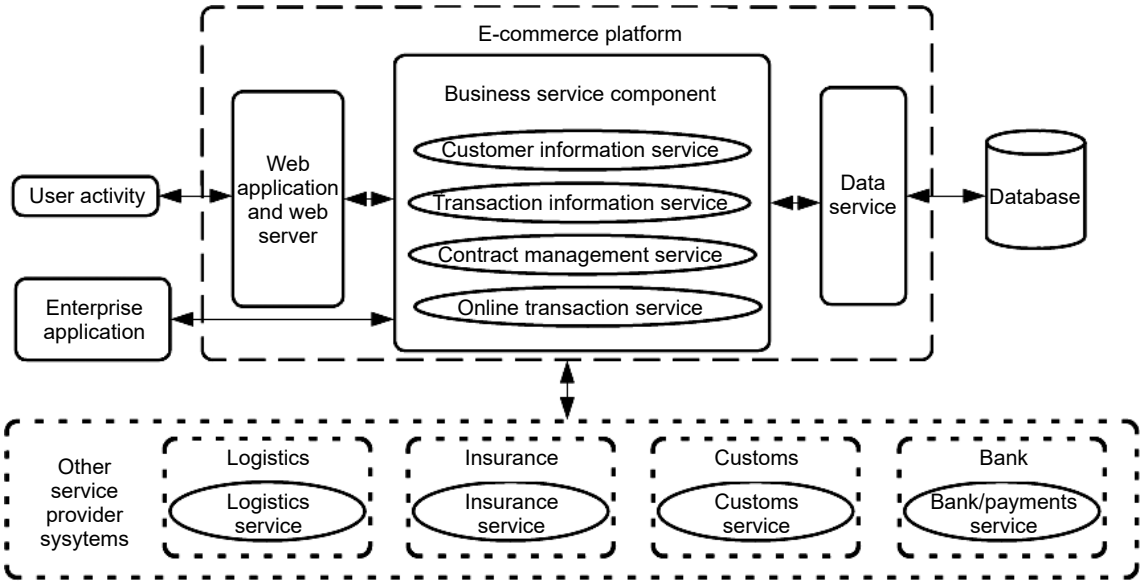

Fig. 2 Detailed-level diagram of an e-commerce platform design architecture.

offer ancillary services on the e-commerce platform.

1.2 Problem statement

Machine learning and data mining techniques have become popular in fraud detection across many domains[13], partly explained by the rapid development of artificial intelligence and the availability of affordable cloud computing technology. A review specifically concentrating on the use of these methods on e-commerce platforms like eBay and Facebook has not been published, though. What we observe is that past reviews frequently use a broad brush to describe all methodologies and domains, for example, reviews by Refs. [6, 14]. Such high-level coverage fails to produce a nuanced understanding of machine learning algorithms and their applications in the e-commerce domain.

On the other hand, the majority of the specific fraud literature reviews, like: Refs. [15–19] only cover the financial domain, such as credit card fraud. What is more, a large number of these articles do not employ systematic literature review methodology to support replication[20].

In this work, we acknowledge these gaps and propose a systematic literature review using the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) methodology[21] to examine the use and application of machine learning and data mining techniques for fraud detection on digital marketplaces or in the e-commerce domain. This is a crucial area given the soaring trends in fraud incidents and their associated costs[22]. Understanding the current literature and trends is essential to identifying new research opportunities as well as informing the industry on the main machine learning and data mining techniques for fraud detection in this area.

To accomplish this work, we answer four research questions as described in Section 3.1. From our methodology and corpus, we contribute to the state-of-the-art as follows:

(1) Provide an array of machine learning and data mining techniques used for fraud detection on digital marketplaces or e-commerce domains in the last decade.

(2) Highlight gaps, trends, and future research directions on the application of machine learning and

data mining techniques for fraud detection in the digital marketplace or e-commerce domain.

The remainder of this paper is organized as follows: In Section 2, we present related research. In Section 3, we present the PRISMA methodology used to compile research articles from the literature. Our literature corpus is examined in Section 4 in light of the study's research questions. In Section 5, we go over the key findings and open issues. Finally, we reach a conclusion in Section 6.

2 Related Work

Reviews of general fraud detection have recently been written and published in the literature. A general review of articles on automated detection techniques (supervised, unsupervised, and hybrid) from the previous ten years is published by Unam et al.[23]. The authors of that review formalize the major fraud types and subtypes for a wide range of industries while presenting alternative information and solutions for each. Amir and Hamid[24] conducted yet another general review of articles related to fraud detection. The researchers outline five common fraud types, including credit card fraud, telecom fraud, fraud involving health insurance, fraud involving auto insurance, and fraud involving online auctions. Their work does not employ a systematic review methodology, and the review period is from 1994 to 2014.

A few reviews of a particular domain are also included in the literature. Adewumi and Akinyelu[25] used the Kitchenham approach to conduct a systematic review of the financial fraud field between 2010 and 2021. Their focus is on the use of machine learning techniques in the detection of financial fraud. Ahmed et al.'s[18] review of anomaly detection methods for fraud detection is yet another review in the financial domain.

The type of fraud that receives the most reviews is credit card fraud. Reviewing credit card fraud, highlighting misuses of supervised and unsupervised techniques, and offering advice for new researchers are among Sorournejad. et al.'s[26] highlights.

Techniques for data mining are the focus of another group of reviews. For instance, Pourhabibi et al.[15] explored the interdependency between various data objects with a focus on graph-based anomaly detection. Reviewing data mining techniques with an emphasis on machine learning classification methods, Aziz and Ghous[27] provided another review in this area.

In Table 1, we provide a list of the articles we consider related to our work. We develop this list by instantiating our search based on three well-known articles in this fraud domain[6, 8, 37] and snowballing to similar articles. We prioritize the list on the basis that an article covers fraud in e-commerce or a related domain.

According to the results, there are no studies that

Table 1 Related work.

Article	Year	Coverage	Review type	Domain
[23]	2010	2000–2010	Unknown	General fraud
[28]	2016	–	Unknown	Online fraud
[24]	2016	1994–2014	Unknown	General fraud
[18]	2016	–	Unknown	Financial fraud
[26]	2016	–	Unknown	Credit card fraud
[17]	2016	1997–2016	Unknown	Credit card fraud using nature inspired machine learning
[29]	2017	–	Systematic literature review	Credit card fraud using ML
[30]	2018	–	Unknown	General fraud using ML
[30, 31]	2018	–	Unknown	Credit card fraud in e-commerce
[14]	2020	–	Systematic literature review	General fraud with graph-based anomaly detection
[32]	2021	–	Unknown	Credit card fraud with ML
[33]	2021	–	Systematic literature review	E-commerce
[34]	2021	–	Unknown	E-commerce
[35]	2021	–	Systematic literature review	E-commerce fake reviews
[36]	2021	–	Unknown	Credit card fraud
[20]	2022	–	Systematic literature review	e-commerce (detection and prevention)
[13]	2022	–	Systematic literature review	Financial fraud (Machine learning)

concentrate on fraud detection using machine learning or data mining techniques on digital marketplaces or e-commerce platforms. In the few places where e-commerce is mentioned in the domain column, the focus is on common fraud types, and little to no attention is paid to the fraud detection methods used. Additionally, the majority of the surveys do not apply a systematic literature review methodology. Our study's main goal is to fill in these gaps.

3 Research Method

We adopt the PRISMA approach[21] to search and select articles in the scope of fraud detection in e-commerce or digital marketplaces based on machine learning or data mining techniques. The PRISMA approach generates high-quality results and supports reproducibility. It is structured in a manner that allows the identification and summarization of problems (domains), techniques, and methods used to solve the problem. The implementation of this approach follows a checklist of title, abstract, introduction, methods, results, discussion, and funding. In this structure, the title and abstract are constructed to achieve comparable objectives to any other approach, but the introduction must provide the rationale for the review and the questions to be addressed. Study characteristics, information sources, search strategy, including limits, statement process for selected studies, eligibility criteria, data collection, and data items are specified in the methods section[21]. The discussion involves a summary of the findings, a discussion of the limitations, and a general conclusion of the results and future work.

Systematic reviews give researchers and practitioners, who would otherwise be overwhelmed by the volume of research on a given topic, a rigorous mechanism upon which to base their decisions. There is a wide variety of literature review approaches for all kinds of topics and disciplines. In our approach, we take the following steps: (1) topic definition; (2) research question formulation; (3) keyword identification; (4) identification and search of electronic paper repositories; (5) publication assessment; (6) data acquisition and cleaning; (7)–(9) testing and revising publication; (10) production and revision of summary tables and figures; (11) draft methods; (12) and (13) evaluation and draft of key results; (14) introduction draft, abstract, and references; (15) paper revision. During the initial stages, we apply guidelines from Petticrew and Roberts[38] on how to scope Systematic Literature Review (SLR), avoid possible biases, and synthesize the results.

3.1 Research questions

Understanding the literature on the use of machine learning and data mining techniques for fraud detection on e-commerce or digital marketplace platforms is the primary goal of this research. Our Research Question three (RQ3) ultimately encapsulates this, but in order to accomplish this successfully, we first use Research Questions one and two (RQ1 and RQ2) to establish the context. These inquiries help us understand the design architecture of e-commerce platforms and contextualize major vulnerabilities discovered therein as well as related frauds. Finding research gaps, trends, and opportunities for further research in the field is the goal of our last research question. Below, we list our research questions.

- RQ1: What are the common vulnerabilities on e-commerce platforms?
- RQ2: What are the common frauds in the marketplace or e-commerce domain?
- RQ3: What are the commonly used machine learning and data mining techniques for fraud detection on digital marketplaces or e-commerce platforms, and what does good performance of these techniques look like?
- RQ4: What are the research gaps, trends, and opportunities for future research in this area?

3.2 Data and search strategy

By extracting potential search terms from the titles, abstracts, and subject indexing of three pertinent publications[17, 23, 24], we develop an initial search strategy. We use its results to expand the list of key words and restrict it to only English-language articles in order to further hone this strategy. We then test the validity of our search strategy by checking whether it could retrieve the three known relevant studies and two more studies referenced in Ref. [17]. All the five studies are successfully identified by the strategy. A group of peer reviewers approves the final search strategy.

Using an iterative search approach, we look for publications within our search period (2010–2023) that have the following keywords in their title or abstract: e-commerce, fraud detection, machine learning, systematic review, organized retail fraud, data mining,

and digital marketplace. We display the iterative approach in the workflow diagram shown in Fig. 3. To reduce the amount of noise in the results, our search strategy employs the search logics "AND", "OR", "LIMIT TO", and "EXCLUDE".

3.3 Publications Repositories

We focus our search on three international digital repositories: Scopus, Web of Science (WoS), and Google Scholar, which together hold the majority of global scientific research. The initial search query in each repository yields a wide range of publications in a multidisciplinary setting covering, among other things, computer science, engineering, decision science, mathematics, energy, physics, and astronomy. We approach our search with the knowledge that the coverage, accuracy, and access fees of these digital repositories vary. For instance, Scopus and Web of Science overlap in two out of three instances[39], with Scopus offering 20 percent more coverage than Web of Science[40]. Depending on the search terms, Google Scholar frequently provides inaccurate and inconsistent results. Additionally, many of its articles are subpar and out of date (Falagas et al.[40]). Therefore, it helps to think of a way to minimize noise and duplicates in the combined search results. To this end, we apply the inclusion and exclusion criteria defined in Table 2 to meet that need.

3.4 PRISMA flow diagram

We use the flow diagram shown in Fig. 4 to illustrate how we apply our inclusion and exclusion criteria to narrow down the most relevant articles for our literature search.

Three hundred and sixty-six articles total in the combined search results are reduced to three hundred and thirty-five after duplicates are eliminated. The first step of our exclusion criteria is when EF1 eliminates three papers written in a language other than English. Our exclusion criterion, EF2, eliminates twenty-six papers in the second step that come from interdisciplinary fields like medicine. EF3 and EF4 eliminate a combined total of two hundred and nine publications, leaving us with one hundred and one

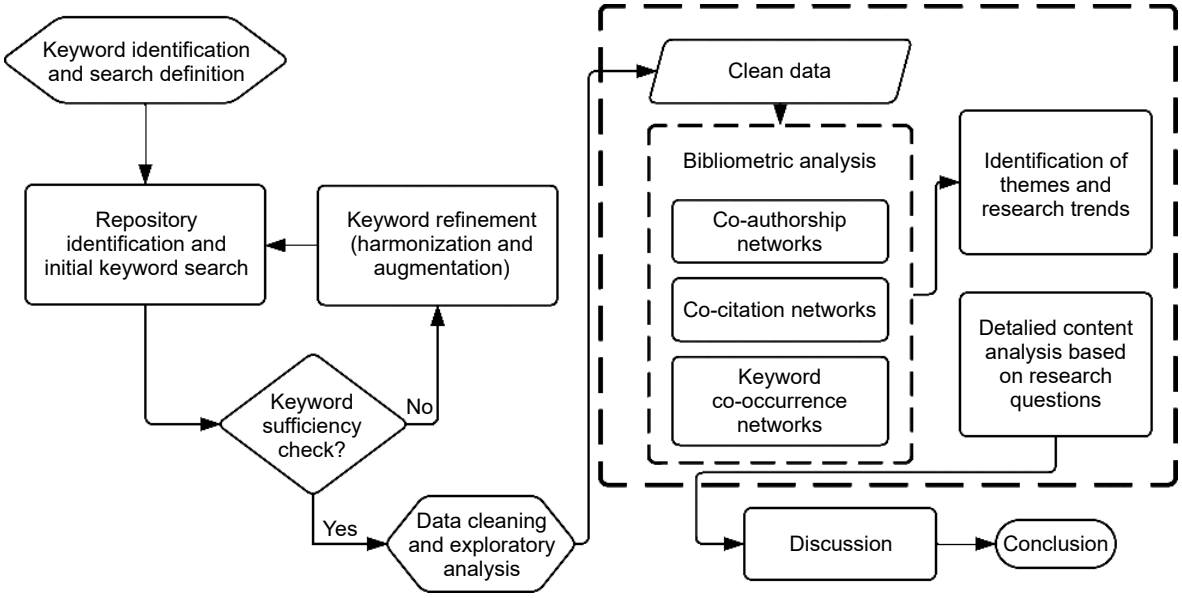

Fig. 3 Iterative search strategy and SLR process workflow diagram.

Table 2 Inclusion and exclusion criteria used to denoise search results from the electronic repositories.

Inclusion Filter (IF)	Exclusion Filter (EF)
IF1: Articles within the study period (2010–2022)	EF1: Articles not published in English
IF2: Articles that focus on fraud detection on fraud detection on e-commerce platforms	EF2: Articles in unrelated disciplines, e.g., medicine
IF3: Peer reviewed articles	EF3: Articles that are in the form of lecture notes, short papers, posters and book chapters, thesis or dissertations, reviews, and survey articles
IF4: Journal and conference papers	EF4: Articles that do not focus on fraud detection, ML, data mining on e-commerce

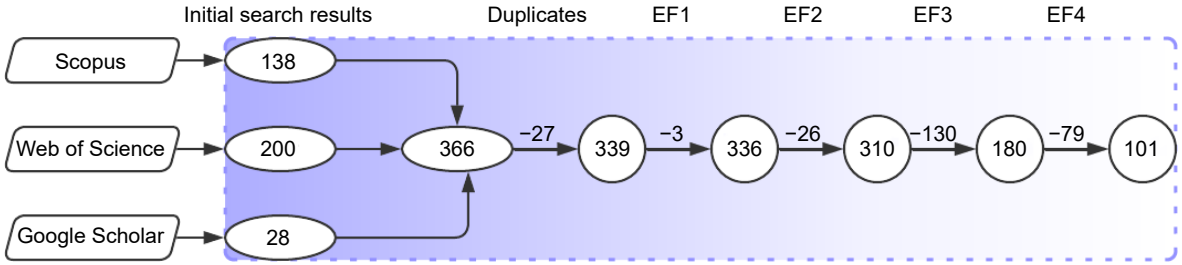

Fig. 4 PRISMA flow diagram showing detailed filtering levels from a high-level representation of publications from initial search query to a final set of publications for SLR analysis.

papers for our final corpus.

Figure 5 displays the total number of publications over the years of our study period, broken down by article type, conference paper, and journal article. Between 2010 and 2018, there were very few articles published on the topic of e-commerce fraud detection using machine learning and data mining techniques. However, 2019 and later years see more articles published with an almost equal split between the two document types, except for 2020, where the number of conference articles is more than double that of journal articles.

3.5 Bibliographic analysis context

For our exploratory work, we use a bibliometric analysis approach to identify the authors of the research articles, their citations, geographic breakdown, and high-level content of their articles. In the end, this exercise aids in our continued refinement of the articles we choose to use to answer our research questions.

3.5.1 Bibliometric analysis

From the combined search results, we create a CSV file that includes the following fields: authors, author(s) ID, title, year, source title, publisher, country, field, ranking, volume, issue, article number, cited by, DOI, link, affiliations, country affiliation, authors with affiliations, abstract, author keywords, index keywords, tradenames, manufacturers, references, correspondence, address, editors, sponsors, publisher, conference name, conference date, conference location, conference code, ISSN, ISBN CODEN, PubMed ID, language of original document, abbreviated source title, document type, publication stage, open access, source EID. We perform our analysis using VOSviewer[41] as the analysis software and the CSV as the input. This tool enables the creation of bibliometric networks of scientific publications, authors, institutions, and keywords. Co-authorship, co-occurrence, citations, bibliometric coupling, or co-citation links are used to connect the items in these networks[42]. In our analysis, we identify a number of network properties, including clusters and node centrality. These analyses highlight recurring themes in the publications that serve as the basis for our state-of-the-art analysis and discussion.

3.5.2 Constructing bibliometric networks

Building bibliometric networks can be done in a variety of ways, but in this case, we concentrate on two methods: full counting and fractional counting[42]. The

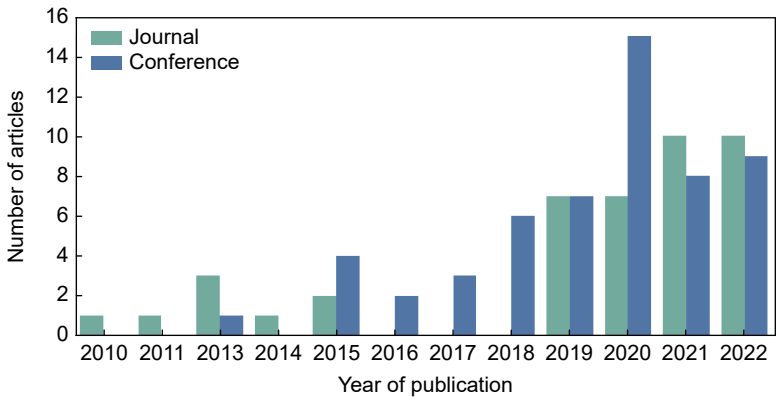

Fig. 5 Bar graph showing the number of publications focusing on e-commerce fraud detection using machine learning and data mining techniques for each year within our search range (2010–2022).

article mentioned above provides a detailed analysis of the two approaches, including mathematical formulation, but the following co-authorship network example highlights the key distinctions between the two examples quickly. Take four authors (R1, R2, R3, and R4), and three documents (P1, P2, and P3), as shown in Fig. 6a. P1 is authored by R1, R2, and R3, P2 is authored by R1 and R3, and P3 is authored by R2 and R4. As shown in Fig. 6b, the networks created using full and fractional counting can be visualized. The assignment of the strength of the links is the primary distinction between the two strategies.

In the full counting network, the link between R1 and R3 has a strength of 2, indicating that authors 1 and 3 collaborated on the creation of publications P1 and P2. The associated authors of the other links have co-authored one publication and have a strength of 1.

Fractional counting is used to lessen the impact of publications with numerous co-authors. The total number of authors of each co-authored publication, as well as the number of documents each author has co-authored, determines the strength of the co-authorship link in fractional counting between two authors. This logic results in a link strength of $1/n$ for each co-authorship link in the scenario where an author co-authored a work with n other authors. The strength of the n co-authorship links as a whole is then equal to 1. This is distinct from the full counting case, where each of the n-co-authorship links has a total strength of n[41]. The aforementioned illustration, which was taken from Ref. [42], applies to instances of keyword co-occurrence, bibliographic coupling, and co-citation links. The units of analysis could be researchers, research institutions, countries, and journals.

When the final SLR data is passed on to the VOSviewer software viewer, natural language processing algorithms take over to identify and select terms based on the following steps: (1) removal of copyright statements; (2) sentence detection; (3) part-of-speech tagging; (4) noun phrase identification; and (5) noun phrase unification. The results emitted by the algorithms above yield noun phrases identified from the titles and abstracts of the publications used. Phrases are selected from this list by setting certain preferences, such as the minimum number of occurrences and relevance score and excluding specific terms that do not add new information to thin the overall phrase population to only what is important[41]. In our case, we use the fractional counting approach, which gives equal weight to all units, as recommended by Ref. [42].

3.6 Bibliometric network analysis results

The example above was for co-authorship networks, but the same idea can be used for bibliometric coupling networks (with documents, sources, authors, organizations, and countries as units of analysis), co-citation networks (with cited references, cited sources, and cited authors as units of analysis), keyword co-occurrence networks (with author keywords and index keywords as units of analysis), and citation networks (with documents, sources, authors, organizations, and countries as units of analysis). We provide co-authorship, co-citation, and keyword co-occurrence network results below.

3.6.1 Co-authorship networks

As our two units of analysis, we select the country and the researcher. We also set the minimum number of documents co-authored between two countries to two and the minimum number of documents by an author to two as well. In both cases, we ignore documents co-

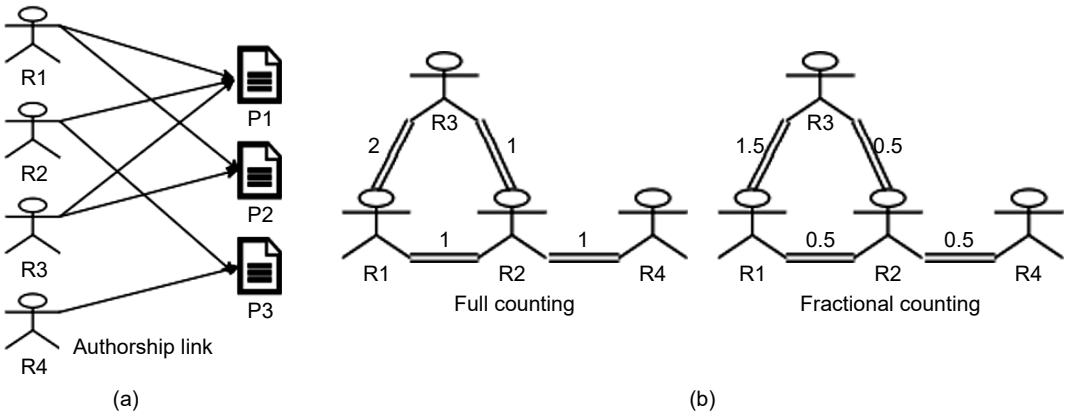

Fig. 6 (a) Authorship links and (b) counting techniques for constructing authorship networks.

authored by more than 25 countries or researchers. We find that five out of 25 countries and four out of 254 authors meet these thresholds. For each of the five countries and four authors, we calculate the total strength of the co-authorship links. China and the United States have strong co-authorship links, while researchers Carta S. and Saia R. have the strongest co-authorship links. The details of our co-authorship networks based on country and researcher are summarized in Tables 3 and 4, respectively.

In summary, our co-authorship networks portray that, in this domain, collaboration between researchers and across countries is low. This result could perhaps be explained by the sensitivity surrounding fraud data.

In Table 5, we observe that India leads in the authorship of research articles in this domain. China ranks second and the USA, Italy and Iran hold the third place in article authorship.

3.6.2 Co-citation networks

In a co-citation network analysis of researchers, the relatedness of researchers is determined based on the degree to which they are cited in the same publications. The more often researchers are cited in the same publications, the stronger their relatedness. We conduct co-citation networks for the cited reference, cited source, and cited authors. Setting the minimum number of citations for a cited reference to 3, we find that 87 of the cited references meet this threshold. We calculate the total link strength for each of the 87 references and select those with the greatest link strength, as shown in Table 6. Articles written by Refs. [43–46] show strong linkages in our co-citation networks.

Table 3 Selection top countries in terms of document co-authorship.

Country	Total link strength	Number of documents	Number of citations
China	3	10	166
USA	3	4	13
India	0	23	98
Indonesia	0	4	14
Italy	0	4	268

Table 4 Selection of the top authors in terms of co-authorship of documents.

Researcher	Total link strength	Number of documents	Number of citations
Carta Salvatore	2	2	48
Saia Roberto	2	3	52
Kawase Ricardo	0	2	3
Li Zou	0	3	142

Table 5 Top ten countries by authorship

Country	Number of articles	Country	Number of articles
India	30	UK	3
China	17	Indonesia	3
USA	5	Kingdom of Saudi Arabia	3
Italy	5	South Africa	2
Iran	5	Russia	2

3.6.3 Keywords co-occurrence networks

A crucial puzzle piece is the co-occurrence of keywords. It helps us understand the research themes of our search results as well as confirms the accuracy of our search criteria. For our context, we analyze the data using two units: all keywords and the author's keywords. 34 out of 593 keywords meet the criteria when the minimum number of instances for all keywords is set to 5. We determine the overall strength of the co-occurrence links between each of the 34 keywords and choose the ones that have the strongest links. Similar steps are taken for the author's keywords, and we discover that thirteen out of 251 keywords meet the necessary threshold and that seven out of the 13 have excellent link strength. We summarize the results of the keyword co-occurrence networks in Tables 7 and 8 below.

The most prominent topic in this area is credit card fraud detection, and the most widely used machine learning techniques are decision trees, random forests, and logistic regression. The frequency of keyword co-occurrences in our corpus is demonstrated in Fig. 7 below.

4 Detailed Analysis and Results from Corpus

To address each research question posed in Section 3.1, we present the findings of our analysis of the literature corpus in this section.

4.1 RQ1: What are the common vulnerability areas in the marketplace or e-commerce domain?

Our corpus surfaces key vulnerabilities on e-commerce platforms, as shown in the architecture diagram for e-commerce systems in Fig. 8. We describe each one of them in subsequent subsections.

Table 6 Topmost cited articles ranked on total link strength and illustration of the methods and domains covered in the articles.

Cited reference	Title	Method	Fraud domain	Number of citations	Total link strength
[43]	A blockchain, smart contract and data mining based approach toward the betterment of e-commerce	Rule-based methods	Phishing	216	18
[44]	A hybrid machine learning framework for e-commerce fraud detection	Artificial Neural Networks (ANNs), decision trees, and copula models	Bank/payments	120	15
[45]	A machine learning based credit card fraud detection using the GA algorithm for feature selection	Genetic algorithm, decision trees, random forest, Naïve Bayes, and logistic regression	Credit card	80	13
[46]	A proposed fraud detection model based on e-payments attributes a case study in Egyptian e-payment gateway	Decision tress	E-payments	79	13
[47]	A study on fraud detection in the C2C used trade market using Doc2vec	Natural language processing (Doc2Vec) and random forest	E-payments	68	10
[48]	Account takeover detection on e-commerce platforms	ANN	Account take-over	63	8
[49]	An analysis on fraud detection in credit card transactions using machine learning techniques	Decision trees, random forest, KNN, and logistic regression	Credit card	59	7
[50]	An innovative sensing machine learning technique to detect credit card frauds in wireless communications	Support Vector Machine (SVM)	Credit card	54	6
[51]	Analysis of supervised machine learning algorithms in the context of fraud detection	SVM, logistic regression, and imbalanced learning	Credit card	51	5

Table 7 Top keywords of all keywords.

Keyword	Total link strength	Number of occurrences
Crime	45	45
Fraud detection	43	52
Machine learning	37	37
Electronic commerce	21	21
Decision trees	20	20
Credit card fraud detection	19	19

Table 8 Top author's keywords.

Author's keyword	Total link strength	Number of occurrences
Fraud detection	29	44
Machine learning	22	24
E-commerce	11	14
Credit card fraud	9	9
Classification	8	9
Logistic regression	8	8
Random forest	6	6

4.1.1 Certificate duplicity

Users must authenticate themselves by providing their credentials to web hosts in order to use an e-commerce platform. In exchange, users are given an authentication credential as proof of certification. Once the user has received authentication, they can access the service. The authentication certificate's issuance procedure is managed by an Identity Management Service (IMS). It is possible to generate a duplicate certificate or forge one and issue it to the web server instead of the original user, bypassing identity authentication to grant access to the service. Attackers or fraudsters could take advantage of this vulnerability to place unauthorized orders for goods or make unauthorized purchases.

4.1.2 Unsecure protocol

"Man-in-the-middle" attacks, in which attackers or fraudsters establish a connection with message transmitters and receivers, could take advantage of this vulnerability. In this instance, attackers create the impression that the sender and the receiver are speaking directly to one another by relaying messages between them. The assailant can easily encode the communication and use it to commit heinous fraud.

4.1.3 No filters mentioned on the application level

An implementation of security code known as a filter is used in web applications to intercept, examine, and respond to requests made to those applications[52]. Without a filter at the application level, a hacker or fraudster may be able to send malicious code through

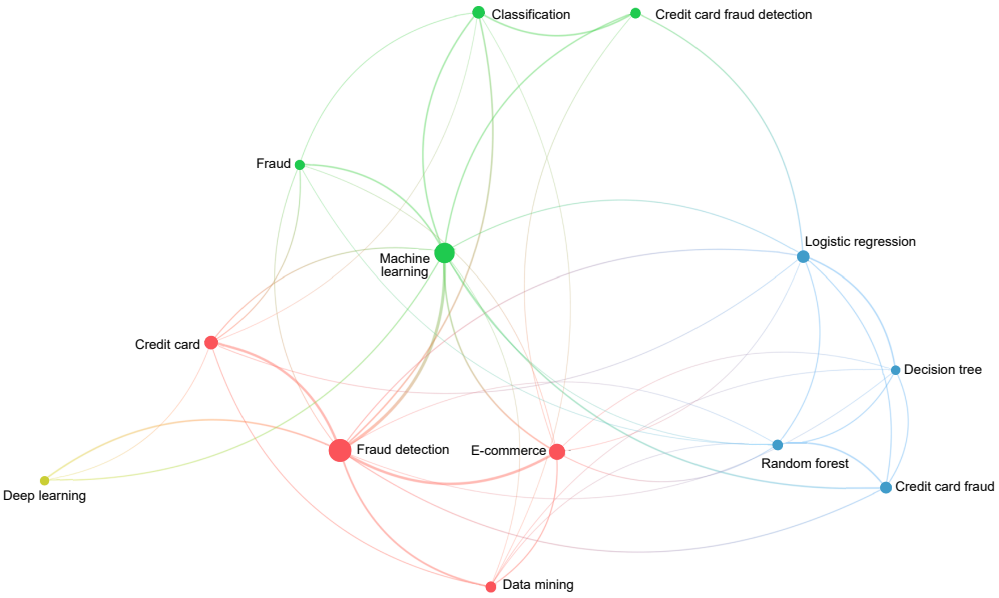

Fig. 7 Network map of keywords co-occurrence showing the most common keywords in the corpus.

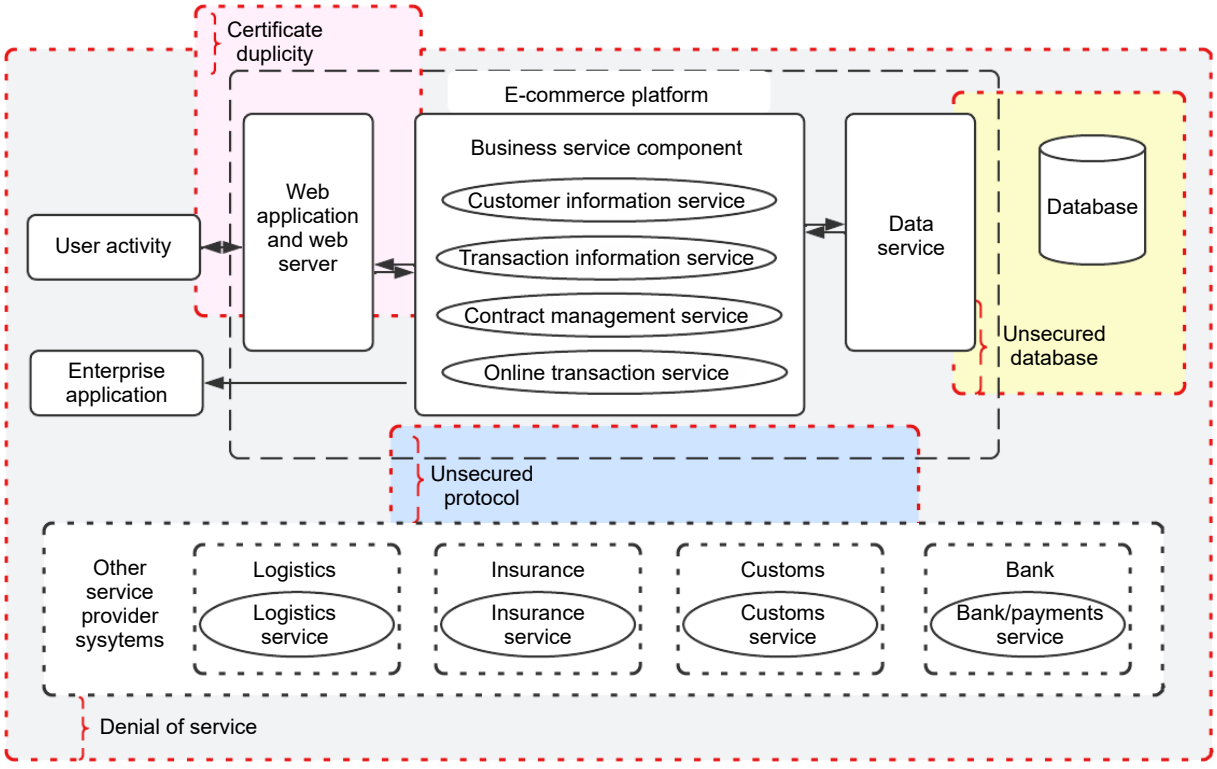

Fig. 8 Basic e-commerce architecture highlighting common vulnerability areas.

the web application and carry out actions such as cross-site scripting and local or remote file inclusion, among other things. Such actions could potentially lead to fraud.

4.1.4 Denial of service

A vulnerability can be exploited to make the e-commerce system unavailable to its intended users. This vulnerability can be leveraged by fraudsters targeting e-commerce traffic by rendering services unavailable to gullible consumers.

4.1.5 Unsecure database

The database is maintained on the same server in most e-commerce models without passing through additional security barriers. Such a flaw could be used by fraudsters to insert malware into the database, cause

important data leaks, and launch a variety of fraud schemes.

4.2 RQ2: What are the most common e-commerce frauds?

On e-commerce platforms, fraudsters use vulnerabilities known to them to wedge attacks and commit fraud. Once the weaknesses are clearly understood, countermeasures can be created to lessen the risk of fraud and combat its effects. In this question, we use our corpus to highlight significant e-commerce frauds and the solutions researchers have suggested. Our corpus reveals five types of fraud that can be thwarted using machine learning and data mining techniques. These include financial or payment frauds, web application frauds, spam or phishing frauds, triangulation frauds, and bot frauds. Figure 9 demonstrates where these frauds take place on the e-commerce platform, while Fig. 10 shows the share of articles within our corpus addressing each fraud type.

4.2.1 Financial frauds or payment frauds

This type of fraud is the most prevalent on e-commerce platforms and has existed since the beginning of businesses' shift from physical to online locations.

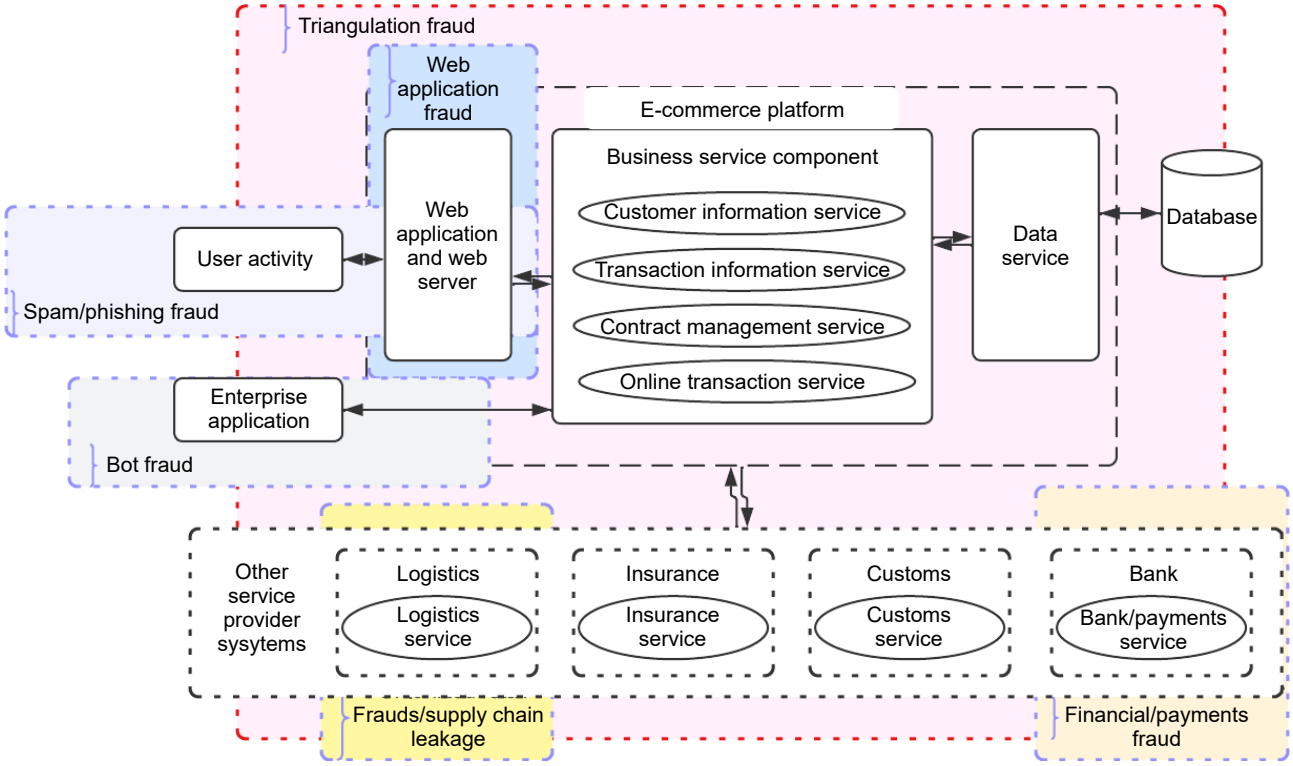

Fig. 9 Basic e-commerce architecture highlighting common fraud areas.

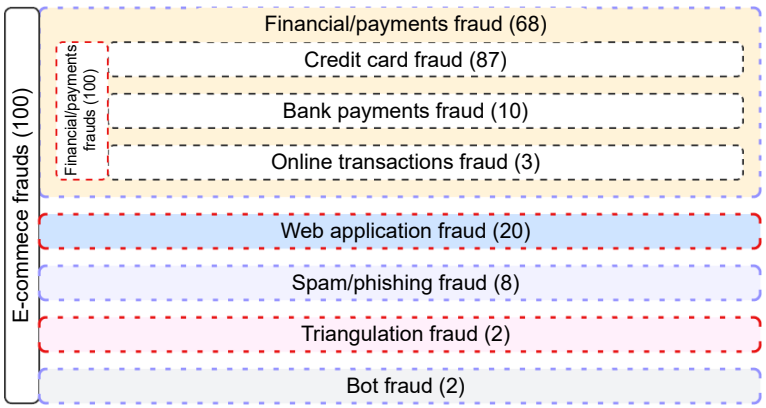

Fig. 10 E-commerce frauds and percentage of articles from our corpus addressing each fraud type.

Using financial or payment information obtained through the exploitation of the aforementioned vulnerabilities, fraudsters frequently carry out unauthorized transactions. In our work, we do not address the architecture of the online payment process or the classification of the sub-fraud types under financial frauds, but Ref. [20] provides a detailed illustration of the components related to e-commerce payments. Our work provides a high-level illustration of platform frauds and vulnerabilities (see Figs. 8 and 9). According to our research, there are three main types of financial or payment fraud: online transactions, bank payments, and credit card transactions. With 87 percent of the articles in the corpus focusing on it, credit card fraud is the most prevalent category. This is not surprising given that credit cards have become the most common form of payment used for shopping on e-commerce platforms.

Bank payment fraud comes in second with about 10 percent of the articles, and online transaction fraud is ranked as the third subcategory with 3 percent of the articles, see Fig. 11 for this breakdown. Due to the sheer volume of articles in this category, we will not list them all, but a few stand out, such as Ref. [53], who suggests a machine learning-based credit fraud detection engine using a genetic algorithm for feature selection. The authors use a data set generated from European market card holders to test the performance of their engine. A study by Ref. [54] proposes a deep learning-based algorithm for credit card fraud detection dubbed Multi-Class Neural Network (MCNN). This method incorporates a class rebalancing mechanism to deal with the class imbalance problem that often appears in fraud data sets. Another study in this domain addresses bank payment fraud by taking the initial detection problem and transforming it into a pseudo-recommendation problem, which is then solved using a ranking metric embedding-based method. This approach solves the data scarcity issue often encountered in situations where historical fraudulent behaviors are nonexistent for certain individuals by leveraging collaborative filtering techniques to create similarity profiles between individuals. In summary, there are more than 63 articles covering this category.

4.2.2 Web application fraud

This is the second-largest (20 percent) type of fraud addressed by articles in our literature. Fraudsters in this category exploit poorly developed e-commerce websites (front-end) to defraud unsuspecting shoppers. Common fraud activities in this type of fraud include fake transactions and gift card fraud[55]. In this category, researchers employ both machine learning and data mining techniques for detection. Reference [56] addresses the reduplication of accounts by users who seek to get more coupons or promotions fraudulently. This is a well-known type of abuse that bad consumers use and can lead to huge losses for companies as well as misleading user information. The researchers in this study use data mining techniques like J48 to detect promo misuse based on customer profiles. Another study by Ref. [57] proposes an unsupervised learning method based on a finite mixture model to identify pricing frauds on e-commerce web sites. A final study worth mentioning is by Ref. [58]. These researchers focus on detecting fictitious account registrations using Long Short-Term Memory (LSTM) and applying Synthetic Minority OverSampling Technique (SMOTE) and adaptive synthetic sampling (ADASYN) for class imbalance treatment. The remaining articles in this category are shown in Table 9.

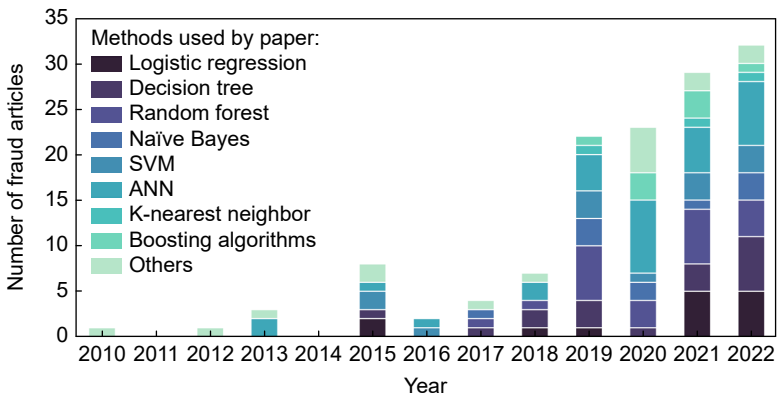

Fig. 11 Evolution of use machine learning and data mining techniques for e-commerce fraud detection over the years.

Table 9 Methods used to detect e-commerce frauds through the years.

Total	Algorithm	Article
14	Logistic regression	[45, 51, 61, 67–75]
17	Decision tree	[44–46, 61, 69, 70 , 74 , 76–84]
21	Random forest	[45, 63, 69, 81, 85–88]
10	Naïve Bayes	[45, 60, 62, 77, 81–83, 89, 90]
13	SVM	[50, 51, 60, 68, 69, 74 , 79, 82, 86, 91–94]
30	ANN	[44, 45, 48, 54, 59, 60, 68, 79, 86, 95–112]
3	K-nearest neighbor	[69, 76]
12	Boosting algorithm	[22, 53, 65, 85, 103, 113–119]
16	Others	[43, 62, 64, 66, 89, 120–127]

4.2.3 Spam/Phishing fraud

Phishing is a type of fraud to gain access to a user's credentials to defraud the user or connected services[59], for example, e-commerce platforms and online merchants. There are numerous tools used by phishers to lure users into traps (unsecure sites) where their sensitive information, like e-commerce account login credentials, payment passwords, home addresses, and birthdays, among others, is exposed. Emails and fake websites are good examples of such tools. Emails are a key marketing channel for e-commerce platforms, and fraudsters can exploit them to obtain customer details. Spam emails with links to fake e-commerce platforms and products are commonplace. We find seven articles in our literature corpus focused on spam or phishing detection, making it the third highest ranked category after financial and web application frauds. These articles are almost evenly split, with three of them looking at data mining techniques and the rest applying machine learning methods. Reference [59] proposed a data-driven framework for detecting phishing webpages using a deep learning approach. The researchers use a multi-layer perceptron (a feed-forward neural network). They use a public data set from Kaggle competition data that contains information about ten thousand web pages. Their proposed method uses ten features and achieves an accuracy of 95 percent on the training data set and 93 percent on the test data set. Another study by Ref. [60] proposed a stacking model to detect phishing websites. Researchers localize their solution to the Iranian e-banking system by identifying influential features of phishing that best fit the Iranian banking sites. They find a list of 28 potential features and, with a feature selection method based on rough sets theory, remain with the six most influential features, which are then applied to a fuzzy expert system. They achieve an accuracy of 88 percent. The other articles in this category include Refs. [45, 63, 64], who use a combination of data mining and machine learning methods to detect phishing fraud.

4.2.4 Triangulation fraud

It is an emerging fraud type on e-commerce platforms that occurs when a customer makes a genuine purchase on an e-commerce platform, but the seller (fake) fraudulently purchases the product from another merchant. First, the fraudster sets up operations as a third-party seller on the marketplace site, for example, eBay. The criminal then lists products for sale at unusually low prices. When a cardholder makes a purchase, the fraudster then turns around and buys the goods from a legitimate seller using stolen card information. The fraudster sets the shipping address to match that of the customer, and therefore the legitimate merchant ships the product to the buyer. The fraudster pockets money from the original sale, while the legitimate merchant gets paid with a stolen payment card. Eventually, the buyer requests a chargeback to their card when they notice an unauthorized transaction, leaving the legitimate merchant defrauded and with legal ramifications. We only find two articles focusing on this category of fraud. The first article[65] presented an approach to classifying fraudulent online shops based on the similarity of their source code structure using machine learning techniques. The trained models achieve an accuracy of 97 percent in detecting fake e-commerce sites, and 61 percent of those predictions are identical to those made by human experts. What is more, these researchers develop an open-source fake-shop detection API and middleware that enable risk assessment of any website. The second article[66] proposed a system for detecting e-commerce websites that is based on Statistical Learning Theory (SLT). The researchers conduct a series of

experiments, comparing their proposed solution with current methods on a test data set containing 900 websites. They determine that the SLT method can more accurately detect fake websites by utilizing a richer set of fraud cues in combination with domain-specific knowledge.

4.2.5 Bot fraud

Fraudsters are constantly evolving their methods to outsmart fraud detection systems. Bots can be used by fraudsters to defraud e-commerce enterprises. For example, bots can be used to mimic the behavior of real users without being detected. These, in effect, could dupe e-commerce enterprises into misleading investments to the detriment of consumers or investors. Bots could also be used by fraudsters to steal customer data, such as bank and payment details, which could in turn facilitate other types of fraud. We also find two articles in this category in our literature review. Reference [65] uses an extended boosting approach that incorporates prior human knowledge, inform of expert rules and blacklists to compensate for data shortages. The method is tested against a mobile application with over 150 million users and achieves an accuracy score of 98 percent and a recall of 94 percent. The researchers surface key behavior patterns of bots that include less spatial motion as detected by device sensors (1/10 of human users), a higher IP clustering ratio (60 percent in bots vs. 15 percent in human users), a higher jailbroken device rate (92 percent in bots vs. 4 percent in human users), more irregular device names, and fewer IP address changes in bots. The final article in the category[66] looks at this issue of cloud bots and how they can be used to perform click fraud, register fake accounts, and commit other types of fraud. The researchers proposed a traffic-based quasi-real-time method for cloud bot detection using machine learning that exploits a new sample partitioning approach as well as innovative multi-layer features that reveal the essential difference between bots and human traffic. Their approach achieves 93 percent precision in the experimental setting but also performs equally well in a real-world data setting and proves robust for detecting unknown cloud bots as well as addressing the concept of drift caused by varying time.

4.3 RQ3: What are the commonly used machine learning and data mining techniques for fraud detection on digital marketplaces or e-commerce platforms, and what does good performance of these techniques look like?

This is the most important question for our review, and we use the previous questions to set the scene for it. In this context, we focus on machine learning and data mining applications for tackling fraud detection in the e-commerce domain. This implies that we do not look at other methods like statistical inference techniques, ontologies, or even bespoke algorithms that could be relevant in the domain. One more thing to note is that we only focus on detection methods. In Table 9, we summarize the distribution of these methods across our corpus.

There are many algorithms applied in these articles, and therefore we only consider those that are used in more than two articles. In Table 9, we show the evolution and frequency of use of the algorithms from the corpus over the years, and a visual summary of the same is shown in Fig. 11. In Table 10, we show the types of fraud in our domain and the number of articles covering them. The family of artificial neural networks is the most frequently applied machine learning category in e-commerce fraud detection, featured in more than a third of the articles. It is used frequently in articles focusing on credit card, web application, and phishing frauds. While we present this set of algorithms under a broad category, the results show a variety of specific algorithms, such as deep recurrent

Table 10 Summary of fraud type and article representation from the corpus

Total	Fraud type		Article
68	Financial/Payments	Credit card	[16, 45, 50, 51, 53, 54, 67, 68, 70, 74, 77, 78, 80, 82, 83, 85, 87–90, 93–96, 98, 101, 104, 105, 109–113, 115, 118, 119, 121, 123, 124, 126, 128–159]
		Bank payments	[44, 84, 92, 116, 160–162]
		Online transactions	[46, 47, 69, 79, 163]
17	Web application		[43, 56, 57, 72, 81, 86, 97, 107, 114, 164–170]
6	Spam/Phishing		[43, 59, 60, 61, 62, 122]
4	Triangulation		[48, 63, 64, 91]
2	Bot		[66, 171]

neural networks, graph neural networks, multilayer perceptron networks, and LSTM. The results also show that the use of ANNs gained more traction in e-commerce fraud detection around 2019.

The second largest category of algorithms is the Random Forests algorithm, which features in about 21 articles in our literature corpus. Many articles conduct performance tests in experimental settings where, for each data set, several algorithms are jointly tested. In these cases, the authors report the Random Forest and the ANNs as the best performers[44, 60, 133]. Decision trees and logistic regression are some of the other notable algorithms.

Our search strategy exposes a couple of data mining strategies for e-commerce fraud detection in addition to common machine learning methods. The algorithms discussed in these strategies do not appear to be clustered, so we collectively refer to them as the "other" category. There are roughly 16 articles in this category, and they primarily cover three types of fraud: web application fraud, credit card fraud, and phishing. One such article focuses on an application in an emerging fraud area, triangulation fraud, as seen in Ref. [64]. These researchers apply SLT to build a prototype for fake site detection, which they test on about nine hundred sites.

4.4 RQ4: What are the research gaps, trends, and opportunities for future research in this area?

In this question, we show research gaps to inform future research directions. We synthesize all the articles in the final corpus to understand how the articles apply machine learning and data mining techniques for e-commerce fraud detection and to surface gaps in their usage. We cover bespoke gaps in the following subsections.

4.4.1 Class asymmetry

The issue of imbalanced classes between fraudulent and legitimate transactions is rife in fraud data[141]. It occurs when there is an asymmetric distribution between classes in the data. In the machine learning domain, most algorithms do not perform well on imbalanced data, as the minority class contributes less to the learning objective[172].

In training an imbalanced data set with a standard classification method, the minority class contributes less towards the minimization of the objective function[173], leading to lower classification accuracy for the minority class and poor performance of the classifier as a whole. For example, a binary classifier that achieves 99 percent training accuracy on imbalanced data with 1 percent minority samples would be irrelevant for predictions on out-of-sample data. In this case, the classifier is only accurate at predicting the majority, while its performance on the minority class is poor (often, all the instances of the minority class are misclassified as instances of the majority class). This is a costly decision because, in most practical applications, classifying the minority instances correctly is more important[173]. Therefore, it is of paramount importance to improve a classifier's ability to recognize the minority class in these settings.

Researchers have developed a variety of techniques to address this problem for all types of data. Techniques such as SMOTE[174] variants are easy to apply and frequently improve classifier performance significantly in both categorical and numeric data sets. In our literature corpus, we observe a mix of situations in which imbalanced learning techniques are applied to improve classifier performance; however, there are some articles that do not use them. What is more, accuracy—a highly misleading metric on imbalanced data—is used for performance evaluation in these articles. While we acknowledge that some of the machine learning algorithms could inherently be applying a rebalancing mechanism during training (algorithmic vs. data-level strategy for class balancing), we observe that only about 10 percent of all articles using machine learning for fraud detection explicitly talk about their class imbalance resolution strategies. Future work should factor in appropriate imbalanced learning techniques in their fraud detection designs whenever machine learning approaches are applied.

4.4.2 Training data

One criticism of machine learning and data mining for fraud detection is the lack of good practical data to use for training algorithms[23]. Real fraud data often carry sensitive information about consumers, and as such, companies are constrained by data protection laws from sharing such data. Additionally, it is counterintuitive to openly share data and fraud detection strategies, as fraudsters can use that information to escape detection systems. These challenges make it hard to advance fraud detection research in general. We observe minimal use of real-world fraud data in our corpus, and in those few cases, the actual details of features used for training the detection algorithms are hardly mentioned. Some of the

articles using real-world data include Ref. [44], which uses a real dataset from one of Egypt's top e-payment gateways, and Ref. [71], which tests their fraud detection system with real-world data from European banks' day-to-day transaction data. The implication of the lack of real-world data is that the majority of the research articles in this domain are experimental and likely will not result in real-world fraud detection systems. Future work could look for sandbox environments that can allow fraud researchers to work with real-world fraud data to advance the field.

We also observe a general overreliance on transaction data for training machine learning models. While these data still achieve good performance, there is likely a missed opportunity in training machine learning models on multimodal data such as images and text beyond the usual numeric and categorical features mined from transaction histories. The last decade has seen significant advances in Natural Language Processing (NLP) and computer vision techniques that can do well in creating multiple learning contexts to build detection systems that are robust to the high level of dynamism observed in various fraud domains. A few articles in our corpus incorporate text-based methods[47, 95, 104, 106] in their detection models, but there are no articles looking at multi-modal approaches incorporating image data into training. This is a future research opportunity area for this domain.

4.4.3 Detection algorithms

The use of ANNs to create fraud detection systems in the e-commerce fraud domain is a clear trend in our data. More than 30 percent of all articles use ANNs as their primary learning technique. ANNs use data and information processing techniques inspired by biological neural network behavior, and they are powerful when used on big data[154]. This explains their popularity in credit card fraud detection, where they can be trained using massive amounts of high-velocity transaction data. This trend is reflected in our data set, in which nearly 60 percent of all articles using ANNs are geared towards credit card fraud detection. Despite being widely used and achieving good discriminatory performance, these techniques lack interpretability, making it difficult for researchers and practitioners to comprehend the signals that lead to fraud. As a result, their use necessitates a conscious decision to optimize performance as opposed to deciphering the underlying indicators associated with fraudulent instances. Future research and applications can put their lack of interpretability into design considerations. We also observe that the random forest is highly featured in our data. It achieves high performance and is interpretable. It is possible to tease out the importance of features' contributions towards the minimization of the objective function. As such, researchers and practitioners can glean from features highly associated with fraudulent instances. In summary, ANNs and the Random Forest algorithm provide a healthy trade-off between performance and interpretability.

5 Discussion

The objective of the systematic review was to find the state-of-the-art literature on machine learning and data mining techniques for fraud detection in the e-commerce domain. We narrowed down our search to these methods because we believe they will be more effective than heuristics and rule-based approaches at thwarting different sorts of fraud in this domain. Additionally, they are simple to monitor for drift, quick to use in production, and extremely flexible in a highly dynamic fraud environment where fraudsters are constantly coming up with new and creative ways to beat bespoke fraud detection systems. To find and examine the most pertinent papers for this fraud topic, we use a combination of the PRISMA SLR technique and content analysis as part of our methodology. We choose to focus on e-commerce fraud detection with machine learning and data mining techniques because it has not been covered in previous literature reviews and, moreover, because our methodology has not been applied before in this context. As a result, compared to studies that covered more expansive domains, such as Refs. [13, 175], we surface more relevant articles. Our work spends less energy and time analyzing various fraud domains and types than the majority of fraud reviews we have encountered so far in the literature. Our attention is concentrated on the most significant fraud classes within the e-commerce fraud area that can be effectively addressed by the use of machine learning and data mining techniques. Our findings differ from those of similar research in that they show an increase in the use of artificial neural network approaches. In one such study[13], Naïve Bayes is found to be the most commonly used machine learning algorithm, while another finds the random forest and logistic regression as the most frequently used algorithms for fraud detection systems.

Among the list of common frauds identified by the literature for e-commerce platforms, credit card fraud is the most researched based on machine learning and data mining techniques. There are a few factors that we think explain this phenomenon. First, credit card payments are most preferred for online payments and have become ubiquitous for use on e-commerce sites[166], generating enormous amounts of high-velocity transaction data; second, with such large volumes of data, heuristics and basic rule-based methods are challenged; and third, access to artificial intelligence and machine learning tools has improved significantly in recent years due to advances in cloud computing technology and reduced compute costs. High detection rates and lower false-positive rates achieved by these methods also make them preferable for building these detection systems.

Notably, there is one common e-commerce fraud type that is not surfaced in detail by any of the articles in our corpus. Reseller fraud, a deceptive practice in which a seller purchases products from a company or retailer with the intent of reselling them at inflated prices, is a missed opportunity that can be addressed by subsequent work. It takes advantage of limited supply, high demand, or exclusive products to manipulate the market and profit from the price difference. We believe this could have been a common occurrence across some product domains during the COVID 19 pandemic when supply chain disruptions and limited manufacturing were rampant.

The final point worth highlighting for our discussion is the emerging fraud types within this domain. Triangulation and bot fraud are new to the e-commerce domain and have tremendous potential for huge losses to consumers and merchants alike because of their ability to scale quickly. For example, triangulation fraudsters can have the ability to gain access to the entire transacting base of a real e-commerce customer if undetected for a sufficiently long time. On the other hand, bots can work relentlessly, and their actions can achieve high multiplier effects; therefore, they can cause huge damages within short periods of time. In our literature corpus, we only find two articles representing each of these fraud types. Given their pervasiveness, more research should be generated on these subdomains.

Information asymmetry makes it possible for fraudsters to create fake sites and stay undetected for a long time, especially for market players without robust detection systems. This is where perpetrators of triangulation fraud step in to create fake e-commerce sites that are identical to existing real ones like Amazon and eBay, which they then use to commit fraudulent purchases using stolen payment and personal consumer information like residence addresses. Many forms of fake and deceptive websites have appeared in the recent past, including spoof and concocted sites. Spoof sites are replicas of real commercial sites intended to deceive the real site's customers into providing their information, while concocted sites are deceptive websites attempting to appear as unique, legitimate commercial entities[64]. Solutions such as, introducing regulations, providing warranties or guarantees on items sold, providing insurance, and making bottom-up efforts to inform consumers of products and sellers' quality and reputation could fix the information asymmetry problem and reduce the impact of these types of fraud on consumers and businesses.

Machine learning and data mining techniques have proven effective in detecting various types of current e-commerce fraud by leveraging pattern recognition, anomaly detection, and predictive modeling. However, they are not a panacea, particularly for emerging types of fraud. While mature types of fraud, such as account takeover fraud, phishing, social engineering, review and rating manipulation, and inventory and price manipulation, can be effectively detected using machine learning models, emerging types like bot fraud and triangulation fraud present challenges.

There are several factors contributing to the difficulty in addressing emerging fraud types. First, the quality and representativeness of training data are often lacking, as data logging and quality assurance systems may lag behind emerging fraud activity. Second, developing effective features specific to these fraud types requires time and specialized skills. Third, while transparent models like decision trees can provide explanations for fraud detection decisions, they may not perform well in emerging fraud types, necessitating the use of more complex models like deep learning algorithms. Fourth, emerging fraud types may actively try to manipulate machine learning models through adversarial attacks, posing additional challenges. Lastly, the effectiveness of machine learning models in detecting fraud degrades over time, necessitating regular updates, retraining, and evaluation.

To build a future e-commerce fraud detection system

using machine learning techniques, these factors must be considered during design, implementation, and maintenance to ensure ongoing effectiveness. Vigilance, collaboration, and adaptation are essential in this dynamic field. By addressing these factors, fraud detection systems can achieve higher accuracy, faster response times, and improved resilience against evolving fraud tactics.

It is important to note that the future state of e-commerce fraud detection is a dynamic environment, driven by ongoing research, technological innovation, and evolving fraud tactics. Regular updates, collaboration between data scientists and fraud prevention teams, and continuous evaluation and refinement of models are crucial to stay at the forefront of fraud detection capabilities in the e-commerce domain.

Finally, while this research aims to provide a comprehensive overview of the current state of knowledge in the domain, there are limitations to be acknowledged. Language and accessibility barriers exist, as the review is conducted in English and non-English articles are excluded, potentially omitting important work. Additionally, access limitations to subscription-based journals may have resulted in incomplete coverage of available publications in the domain.

6 Conclusion

In this article, we employed a combined PRISMA and content synthesis approach to identify and analyze relevant articles focusing on fraud detection in the e-commerce domain using machine learning and data mining techniques. Our survey encompassed a total of 101 articles, with 16 of them classified as “other” due to being unclustered data mining techniques, while the remaining articles fell under the mainstream machine learning cluster.

To structure our analysis, we formulated four research questions, with the first two providing context for our main question. Among the machine learning algorithms utilized, ANNs emerged as the most frequently employed, closely followed by random forest. Notably, the majority of articles centered around the detection of credit card fraud, showcasing its prevalence in the field. However, we found a dearth of detailed research addressing reseller fraud, also known as product flipping or scalping, within our corpus, highlighting a potential avenue for future investigation given its significance in the e-commerce domain and potential impact on the economy and households. Further exploration of various techniques, including machine learning, to combat reseller fraud could be a fruitful area for future work.

Our review also shed light on emerging fraud types in e-commerce, namely triangulation and bot fraud, which have received limited attention in the realm of machine learning and data mining techniques. This observation underscores the need for further research to address these novel fraud types effectively.

Furthermore, our analysis revealed a growing demand for the application of imbalanced learning techniques to enhance future fraud detection systems. This indicates an opportunity for the concerted use of such techniques to tackle the challenge posed by imbalanced datasets in fraud detection.

The findings of our work have practical implications for practitioners in the e-commerce industry. They can replicate the approaches discussed in our corpus and implement them to proactively identify and eliminate malicious actors from their platforms, thereby reducing losses and safeguarding their brand reputations. Additionally, our survey contributes to the existing body of knowledge and literature on fraud detection in the e-commerce domain, providing valuable insights for future research endeavors.

Overall, our study serves as a comprehensive survey that informs both practitioners and researchers, facilitating the advancement of fraud detection techniques in the e-commerce domain.

References

[1] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow, and T. Glenn, Increasing cybercrime since the pandemic: Concerns for psychiatry, *Curr. Psychiatry Rep.*, vol. 23, no. 4, p. 18, 2021.

[2] S. Kodate, R. Chiba, S. Kimura, and N. Masuda, Detecting problematic transactions in a consumer-to-consumer e-commerce network, *Appl. Netw. Sci.*, vol. 5, no. 1, p. 90, 2020.

[3] R. Samani and G. Davis, McAfee mobile threat report, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf, 2019.

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

[5] Sam Smith and Juniper Research, Online payment fraud: Market forecasts, emerging threats & segment analysis 2022-2027, https://www.juniperresearch.com/

press/losses-online-payment-fraud-exceed-362-billion/, 2024.
[6] A. Abdallah, M. A. Maarof, and A. Zainal, Fraud detection system: A survey, *J. Netw. Comput. Appl.*, vol. 68, pp. 90–113, 2016.
[7] R. J. Bolton and D. J. Hand, Statistical fraud detection: A review, *Statistical Science*, vol. 17, no. 3, pp. 235–255, 2002.
[8] C. Phua, V. Lee, K. Smith, and R. Gayler, A comprehensive survey of data mining-based fraud detection research, arXiv preprint arXiv: 1009.6119, 2010.
[9] L. Akoglu, H. Tong, and D. Koutra, Graph based anomaly detection and description: A survey, *Data Min. Knowl. Discov.*, vol. 29, no. 3, pp. 626–688, 2015,
[10] D. Irani, S. Webb, and C. Pu, Study of static classification of social spam profiles in MySpace, *Proc. Int. AAAI Conf. Web Soc. Med.*, vol. 4, no. 1, pp. 82–89, 2010.
[11] A. Bhowmick and S. M. Hazarika, Machine learning for E-mail spam filtering: Review, techniques and trends, arXiv preprint arXiv: 1606.01042, 2016.
[12] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, Anomaly detection in online social networks, *Soc. Netw.*, vol. 39, pp. 62–70, 2014.
[13] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, Financial fraud detection based on machine learning: A systematic literature review, *Appl. Sci.*, vol. 12, no. 19, p. 9637, 2022.
[14] T. Pourhabibi, K. L. Ong, B. H. Kam, and Y. L. Boo, Fraud detection: A systematic literature review of graph-based anomaly detection approaches, *Decis. Support Syst.*, vol. 133, p. 113303, 2020.
[15] R. Banerjee, G. Bourla, S. Chen, M. Kashyap, and S. Purohit, Comparative analysis of machine learning algorithms through credit card fraud detection, in *Proc. IEEE MIT Undergraduate Research Technology Conf.*, Cambridge, MA, USA, 2018, pp. 1–4.
[16] N. Carneiro, G. Figueira, and M. Costa, A data mining based system for credit-card fraud detection in e-tail, *Decis. Support Syst.*, vol. 95, pp. 91–101, 2017.
[17] A. O. Adewumi and A. A. Akinyelu, A survey of machine-learning and nature-inspired based credit card fraud detection techniques, *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, no. S2, pp. 937–953, 2017.
[18] M. Ahmed, A. N. Mahmood, and M. R. Islam, A survey of anomaly detection techniques in financial domain, *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, 2016.
[19] V. Rodrigues, L. Policarpo, and D. E. da Silveira, Fraud detection and prevention in e-commerce: A systematic literature review, https://www.sciencedirect.com/science/article/pii/S1567422322000904?casa_token=UOjgVT_FXuwAAAAA:YgIpy5PUX5dEdF_dJ2Nd1Hz-664Vr32oHJPDq_ZbevxtOazQ38tP_I-PVDtKsCBFXXu_6-Ri6Q, 2022.
[20] J. West and M. Bhattacharya, Intelligent financial fraud detection: A comprehensive review, *Comput. Secur.*, vol. 57, pp. 47–66, 2016.
[21] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al., The PRISMA 2020 statement: An updated guideline for reporting systematic reviews, *BMJ*, vol. 372, p. n71, 2021.
[22] S. Lei, K. Xu, Y. Huang, and X. Sha, An Xgboost based system for financial fraud detection, *E3S Web Conf.*, vol. 214, p. 02042, 2020.
[23] S. Unam, M. Godfrey, and O. Taiwo, Credit card fraud detection using machine learning algorithms, doi: 10.13140/RG.2.2.14806.63044.
[24] A. Amir and G. Hamid, Fraudulent transactions detection in credit card by using data mining methods: A review, https://www.researchgate.net/publication/348732395_Fraudulent_Transactions_Detection_in_Credit_Card_by_using_Data_Mining_Methods_A_Review, 2022.
[25] A. O. Adewumi and A. A. Akinyelu, A survey of machine-learning and nature-inspired based credit card fraud detection techniques, *International Journal of System Assurance Engineering and Management*, vol. 8, no. 2, pp. 937–953, 2017.
[26] S. Sorournejad, Z. Zojaji, R. E. Atani, and A. H. Monadjemi, A survey of credit card fraud detection techniques: Data and technique oriented perspective, arXiv preprint arXiv: 1611.06439, 2016.
[27] A. Aziz and H. Ghous, Fraudulent transactions detection in credit card by using data mining methods: A review, *Int. J. Sci. Prog. Res.*, vol. 79, no. 1, pp. 31–48, 2021.
[28] H. Paruchuri, Credit card fraud detection using machine learning: A systematic literature review, *ABC J. Adv. Res*. vol. 6, no. 2, pp. 113–120, 2017.
[29] B. B. Sagar, P. Singh, and S. Mallika, Online transaction fraud detection techniques: A review of data mining approaches, in *Proc. 3rd Int. Conf. Computing for Sustainable Global Development* (*INDIACom*), New Delhi, India, 2016, pp. 3756–3761.
[30] A. G. Oketola, T. Gbadebo-Ogunmefun, and A. Agbeja, A review of credit card fraud detection using machine learning algorithms, doi:10.13140/RG.2.2.22552.98562/1.
[31] S. J. Omar, K. Fred, and K. K. Swaib, A state-of-the-art review of machine learning techniques for fraud detection research, in *Proc. 2018 Int. Conf. Software Engineering in Africa*, Gothenburg, Sweden, 2018, pp. 11–19.
[32] I. Xournals, A review of credit card fraud detection techniques in e-commerce, https://www.academia.edu/39529497/A_review_of_Credit_card_Fraud_Detection_techniques_in_e_commerce, 2022.
[33] K. S. Lim, L. H. Lee, and Y. W. Sim, A review of machine learning algorithms for fraud detection in credit card transaction, *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 9, pp. 31–40, 2021.
[34] L. M. Policarpo, D. E. da Silveira, R. da Rosa Righi, R. A. Stoffel, C. A. da Costa, J. L. V. Barbosa, R. Scorsatto, and T. Arcot, Machine learning through the lens of e-commerce initiatives: An up-to-date systematic literature review, *Comput. Sci. Rev.*, vol. 41, p. 100414, 2021.

[35] S. Yin and X. Luo, A review of learning-based E-commerce, in *Proc. 16th Int. Conf. Intelligent Systems and Knowledge Engineering*, Chengdu, China, 2021, pp. 483–490.

[36] H. Paul and A. Nikolaev, Fake review detection on online E-commerce platforms: A systematic literature review, *Data Min. Knowl. Discov.*, vol. 35, no. 5, pp. 1830–1881, 2021.

[37] P. Gamini, S. T. Yerramsetti, G. D. Darapu, V. K. Pentakoti, and P. R. Vegesena, A review on the performance analysis of supervised and unsupervised algorithms in credit card fraud detection, *Int. J. Res. Eng. Sci. Manag.*, vol. 4, no. 8, pp. 23–26, 2021.

[38] M. Petticrew and H. Roberts, *Systematic Reviews in the Social Sciences*: *A Practical Guide*. Oxford, UK: Wiley-Blackwell, 2006.

[39] E. S. Gualberto, R. T. De Sousa, T. P. De B Vieira, J. P. C. L. Da Costa, and C. G. Duque, From feature engineering and topics models to enhanced prediction rates in phishing detection, *IEEE Access*, vol. 8, pp. 76368–76385, 2020.

[40] M. E. Falagas, E. I. Pitsouni, G. A. Malietzis, and G. Pappas, Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and weaknesses, *FASEB J.*, vol. 22, no. 2, pp. 338–342, 2008.

[41] N. J. van Eck and L. Waltman, Software survey: VOSviewer, a computer program for bibliometric mapping, *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[42] A. Perianes-Rodriguez, L. Waltman, and N. J. Van Eck, Constructing bibliometric networks: A comparison between full and fractional counting, *J. Informetr.*, vol. 10, no. 4, pp. 1178–1195, 2016.

[43] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach, *IEEE Access*, vol. 10, pp. 87115–87134, 2022.

[44] Y. Y. Festa and I. A. Vorobyev, A hybrid machine learning framework for e-commerce fraud detection, *Model Assist. Stat. Appl.*, vol. 17, no. 1, pp. 41–49, 2022.

[45] E. Ileberi, Y. Sun, and Z. Wang, A machine learning based credit card fraud detection using the GA algorithm for feature selection, *J. Big Data*, vol. 9, no. 1, p. 24, 2022.

[46] M. H. Nasr, M. H. Farrag, and M. M. Nasr, A proposed fraud detection model based on e-Payments attributes a case study in Egyptian e-Payment gateway, *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 5, pp. 179–186, 2022.

[47] D. H. Lim and H. Ahn, A study on fraud detection in the C2C used trade market using Doc2vec, *J. Korea Soc. Comput. Inform.*, vol. 27, no. 3, pp. 173–182, 2022.

[48] M. Gao, Account takeover detection on E-commerce platforms, in *Proc. IEEE Int. Conf. Smart Computing*, Helsinki, Finland, 2022, pp. 196–197.

[49] J. Mathew, C. K. Pang, M. Luo, and W. H. Leong, Classification of imbalanced data by oversampling in kernel space of support vector machines, *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 9, pp. 4065–4076, 2018.

[50] G. Sasikala, M. Laavanya, B. Sathyasri, C. Supraja, V. Mahalakshmi, S. S. S. Mole, J. Mulerikkal, S. Chidambaranathan, C. Arvind, K. Srihari, et al., An innovative sensing machine learning technique to detect credit card frauds in wireless communications, *Wirel. Commun. Mob. Comput.*, vol. 2022, p. 2439205, 2022.

[51] P. Verma and P. Tyagi, Analysis of supervised machine learning algorithms in the context of fraud detection, *ECS Trans.*, vol. 107, no. 1, pp. 7189–7200, 2022.

[52] A. Baishya and S. Kakoty, A review on web content filtering, its technique and prospects, *Int. J. Comput. Sci. Trends Technol.*, vol. 7, no. 3, pp. 37–40, 2019.

[53] E. Ileberi, Y. Sun, and Z. Wang, Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost, *IEEE Access*, vol. 9, pp. 165286–165294, 2021.

[54] N. Prabha and S. Manimekalai, Imbalanced data classification in credit card fraudulent activities detection using multi-class neural network, in *Proc. 2nd Int. Conf. Artificial Intelligence and Smart Energy*, Coimbatore, India, 2022, pp. 131–138.

[55] P. S. Lokhande and B. B. Meshram, E-commerce applications: Vulnerabilities, attacks and countermeasures, https://www.researchgate.net/publication/235697382_E-Commerce_Applications_Vulnerabilities_Attacks_and_CountermeasUres, 2022.

[56] T. Mauritsius, S. Alatas, F. Binsar, R. Jayadi, and N. Legowo, Promo abuse modeling in e-commerce using machine learning approach, in *Proc. 8th Int. Conf. Orange Technology*, Daegu, Republic of Korea, 2020, pp. 1–6.

[57] K. Kim, Y. Choi, and J. Park, Pricing fraud detection in online shopping malls using a finite mixture model, *Electron. Commer. Res. Appl.*, vol. 12, no. 3, pp. 195–207, 2013.

[58] A. G. Marakhtanov, E. O. Parenchenkov, and N. V. Smirnov, Detection of fictitious accounts registration, in *Proc. Int. Russian Automation Conf.*, Sochi, Russia, 2021, pp. 226–230.

[59] I. Saha, D. Sarma, R. J. Chakma, M. N. Alam, A. Sultana, and S. Hossain, Phishing attacks detection using deep learning approach, in *Proc. 3rd Int. Conf. Smart Systems and Inventive Technology*, Tirunelveli, India, 2020, pp. 1180–1185.

[60] A. Zamir, H. U. Khan, T. Iqbal, N. Yousaf, F. Aslam, A. Anjum, and M. Hamdani, Phishing web site detection using diverse machine learning algorithms, *Electronic Library*, vol. 38, no. 1, pp. 65–80, 2020.

[61] F. Hasan, S. K. Mondal, M. R. Kabir, M. A. Al Mamun, N. S. Rahman, and M. S. Hossen, E-commerce merchant fraud detection using machine learning approach, in *Proc. 7th Int. Conf. Communication and Electronics Systems*, Coimbatore, India, 2022, pp. 1123–1127.

[62] S. Carta, G. Fenu, D. R. Recupero, and R. Saia, Fraud detection for E-commerce transactions by employing a prudential multiple consensus model, *J. Inform. Secur.*

Appl., vol. 46, pp. 13–22, 2019.
[63] L. Beltzung, A. Lindley, O. Dinica, N. Hermann, and R. Lindner, Real-time detection of fake-shops through machine learning, in *Proc. IEEE Int. Conf. Big Data*, Atlanta, GA, USA, 2020, pp. 2254–2263.
[64] A. Abbasi, Z. Zhang, D. Zimbra, H. Chen, and J. F. N. Jr, Detecting fake websites: The contribution of statistical learning theory, *MIS Quart.*, vol. 34, no. 3, pp. 435–461, 2010.
[65] Q. Sun, T. Tang, H. Chai, J. Wu, and Y. Chen, Boosting fraud detection in mobile payment with prior knowledge, *Appl. Sci.*, vol. 11, no. 10, p. 4347, 2021.
[66] Y. Guo, J. Shi, Z. Cao, C. Kang, G. Xiong, and Z. Li, Machine learning based cloudbot detection using multi-layer traffic statistics, in *Proc. IEEE 21st Int. Conf. High Performance Computing and Communications*, *IEEE 17th Int. Conf. Smart City*, *IEEE 5th Int. Conf. Data Science and Systems*, Zhangjiajie, China, 2019, pp. 2428–2435.
[67] J. C. Mathew, B. Nithya, C. R. Vishwanatha, P. Shetty, H. Priya, and G. Kavya, An analysis on fraud detection in credit card transactions using machine learning techniques, in *Proc. 2nd Int. Conf. Artificial Intelligence and Smart Energy*, Coimbatore, India, 2022, pp. 265–272.
[68] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, Developing a credit card fraud detection model using machine learning approaches, *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, pp. 411–418, 2022.
[69] K. Abhirami, A. K. Pani, M. Manohar, and P. Kumar, An approach for detecting frauds in E-commerce transactions using machine learning techniques, in *Proc. 2nd Int. Conf. Smart Electronics and Communication*, Trichy, India, 2021, pp. 826–831.
[70] A. S, N. Sethumadhavan, and H. N. AG, Credit card fraud detection using apache spark analysis, in *Proc. 5th Int. Conf. Trends in Electronics and Informatics*, Tirunelveli, India, 2021, pp. 998–1002.
[71] K. N. Mishra and S. C. Pandey, Fraud prediction in smart societies using logistic regression and K-fold machine learning techniques, *Wirel. Pers. Commun.*, vol. 119, no. 2, pp. 1341–1367, 2021.
[72] S. V. J. B. Gracia, J. G. Ponsam, S. Preetha, and J. G. K. Subhiksha, Payment fraud detection using machine learning techniques, in *Proc. 4th Int. Conf. Computing and Communications Technologies*, Chennai, India, 2021, pp. 623–626.
[73] S. Patil, V. Nemade, and P. K. Soni, Predictive modelling for credit card fraud detection using data analytics, *Procedia Comput. Sci.*, vol. 132, pp. 385–395, 2018.
[74] R. F. Lima and A. C. M. Pereira, A fraud detection model based on feature selection and undersampling applied to web payment systems, in *Proc. IEEE/WIC/ACM Int. Joint Conf. Web Intelligence and Intelligent Agent Technology*, Singapore, 2015, pp. 219–222.
[75] G. K. Nune and P. V. Sena, Novel artificial neural networks and logistic approach for detecting credit card deceit, *Int. J. Comput. Sci. Netw. Secur.*, vol. 15, no. 9, pp. 21–27, 2015.
[76] H. Zhou, G. Sun, S. Fu, W. Jiang, and J. Xue, A scalable approach for fraud detection in online e-commerce transactions with big data analytics, *Computers, Materials and Continua*, vol. 60, no. 1, pp. 179–192, 2019.
[77] P. Tomar, S. Shrivastava, and U. Thakar, Ensemble learning based credit card fraud detection system, in *Proc. 5th Conf. Information and Communication Technology*, Kurnool, India, 2021, pp. 1–5.
[78] K. AbdulSattar and M. Hammad, Fraudulent transaction detection in FinTech using machine learning algorithms, in *Proc. Int. Conf. Innovation and Intelligence for Informatics, Computing and Technologies* (*3ICT*), Sakheer, Bahrain, 2020, pp. 1–6.
[79] H. Zhou, G. Sun, S. Fu, W. Jiang, and J. Xue, A scalable approach for fraud detection in online e-commerce transactions with big data analytics, *Comput. Mater. Contin.*, vol. 60, no. 1, pp. 179–192, 2019.
[80] A. Roshan, A. Vyas, and U. Singh, Credit card fraud detection using choice tree technology, in *Proc. 2nd Int. Conf. Electronics, Communication and Aerospace Technology*, Coimbatore, India, 2018, pp. 1613–1619.
[81] F. Vanhoenshoven, G. Napoles, R. Falcon, K. Vanhoof, and M. Koppen, Detecting malicious URLs using machine learning techniques, in *Proc. IEEE Symp. Series on Computational Intelligence*, Athens, Greece, 2016, pp. 1–8.
[82] A. Barahim, A. Alhajri, N. Alasaibia, N. Altamimi, N. Aslam, and I. U. Khan, Enhancing the credit card fraud detection through ensemble techniques, *J. Comput. Theor. Nanosci.*, vol. 16, no. 11, pp. 4461–4468, 2019.
[83] A. S. Saputra and S. Suharjito, Fraud detection using machine learning in e-commerce, *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 332–339, 2019.
[84] W. Mostard, B. Zijlema, and M. Wiering, Combining visual and contextual information for fraudulent online store classification, in *Proceedings IEEE/WIC/ACM International Conference on Web Intelligence*, doi: 10.1145/3350546.3352504.
[85] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, Credit card fraud detection using machine learning, in *Proc. 4th Int. Conf. Intelligent Computing and Control Systems*, Madurai, India, 2020, pp. 1264–1270.
[86] W. Mostard, B. Zijlema, and M. Wiering, Combining visual and contextual information for fraudulent online store classification, in *Proc. IEEE/WIC/ACM Int. Conf. Web Intelligence*, Thessaloniki, Greece, 2019, pp. 84–90.
[87] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, Random forest for credit card fraud detection, in *Proc. IEEE 15th Int. Conf. Networking, Sensing and Control*, Zhuhai, China, 2018, pp. 1–6.
[88] S. K. Kalhotra, S. V. Dongare, A. Kasthuri, and D. Kaur, Data mining and machine learning techniques for credit card fraud detection, *ECS Trans.*, vol. 107, no. 1, pp. 4977–4985, 2022.
[89] T. Vairam, S. Sarathambekai, S. Bhavadharani, A. Kavi Dharshini, N. Nithya Sri, and T. Sen, Evaluation of Naïve bayes and voting classifier algorithm for credit card fraud

detection, in *Proc. 8th Int. Conf. Advanced Computing and Communication Systems*, Coimbatore, India, 2022, pp. 602–608.

[90] I. Ali, K. Aurangzeb, M. Awais, R. J. u. H. Khan, and S. Aslam, An efficient credit card fraud detection system using deep-learning based approaches, in *Proc. IEEE 23rd Int. Multi-Topic Conf.*, Bahawalpur, Pakistan, 2020, pp. 1–6.

[91] K. Shin, T. Ishikawa, Y. L. Liu, and D. L. Shepard, Learning DOM trees of web pages by subpath kernel and detecting fake e-commerce sites, *Mach. Learn. Knowl. Extr.*, vol. 3, no. 1, pp. 95–122, 2021.

[92] Y. Dong, Z. Jiang, A. Mamoun, and P. M. Kumar, Real-time fraud detection in e-market using machine learning algorithms, *J. Mult.-Valued Log. Soft Comput.*, vol. 36, nos. 1–3, pp. 191–209, 2021.

[93] V. Mareeswari and G. Gunasekaran, Prevention of credit card fraud detection based on HSVM, in *Proc. Int. Conf. Information Communication and Embedded Systems*, Chennai, India, 2016, pp. 1–4.

[94] G. P. Santiago, A. C. M. Pereira, and R. Hirata, A modeling approach for credit card fraud detection in electronic payment services, in *Proc. 30th Annu. ACM Symp. Applied Computing*, Salamanca, Spain, 2015, pp. 2328–2331.

[95] A. Mitra and M. Siddhant, Credit card fraud detection using autoencoders, *YMER*, vol. 21, no. 6, pp. 337–342, 2022.

[96] G. M. Rao and K. Srinivas, RNN-BD: An approach for fraud visualisation and detection using deep learning, *Int. J. Comput. Sci. Eng.*, vol. 25, no. 2, pp. 166–173, 2022.

[97] H. Huang, B. Liu, X. Xue, J. Cao, and X. Chen, Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique, *Applied Soft Computing*, vol. 154, p. 111368, 2024.

[98] J. Forough and S. Momtazi, Ensemble of deep sequential models for credit card fraud detection, *Appl. Soft Comput.*, vol. 99, p. 106883, 2021.

[99] N. T. N. Anh, T. Q. Khanh, N. Q. Dat, E. Amouroux, and V. K. Solanki, Fraud detection via deep neural variational autoencoder oblique random forest, in *Proceedings of 2020 IEEE-HYDCON International Conference on Engineering in the 4th Industrial Revolution, HYDCON 2020*, doi: 10.1109/HYDCON48903.2020.9242753.

[100] A. K. Rai and R. K. Dwivedi, Fraud detection in credit card data using machine learning techniques, in *Proc. 2nd Int. Conf. Machine Learning, Image Processing, Network Security and Data Sciences*, Silchar, India, 2020, pp. 369–382.

[101] N. T. N. Anh, T. Q. Khanh, N. Q. Dat, E. Amouroux, and V. K. Solanki, Fraud detection via deep neural variational autoencoder oblique random forest, in *Proc. IEEE-HYDCON*, Hyderabad, India, 2020, pp. 1–6.

[102] J. Wang and C. Wu, Camouflage is NOT easy: Uncovering adversarial fraudsters in large online app review platform, *Measurement and Control*, vol. 53, nos. 9&10, pp. 2137–2145, 2020.

[103] X. Liu, K. Yan, L. Burak Kara, and Z. Nie, CCFD-Net: A novel deep learning model for credit card fraud detection, in *Proceedings IEEE 22nd International Conference on Information Reuse and Integration for Data Science*, doi: 10.1109/IRI51335.2021.00008.

[104] M. Zamini and G. Montazer, Credit card fraud detection using autoencoder based clustering, in *Proc. 9th Int. Symp. Telecommunications*, Tehran, Iran, 2018, pp. 486–491.

[105] X. Liu, K. Yan, L. Burak Kara, and Z. Nie, CCFD-Net: A novel deep learning model for credit card fraud detection, in *Proc. IEEE 22nd Int. Conf. Information Reuse and Integration for Data Science*, Las Vegas, NV, USA, 2021, pp. 9–16.

[106] J. A. Smiles and T. Kamalakannan, Data mining based hybrid latent representation induced ensemble model towards fraud prediction, in *Proc. 3rd Int. Conf. Intelligent Sustainable Systems*, Thoothukudi, India, 2020, pp. 376–382.

[107] M. Zhao, Z. Li, B. An, H. Lu, Y. Yang, and C. Chu, Impression allocation for combating fraud in E-commerce via deep reinforcement learning with action norm penalty, in *Proc. 27th Int. Joint Conf. Artificial Intelligence*, doi:10.24963/ijcai.2018/548.

[108] A. Srivastava, M. Yadav, S. Basu, S. Salunkhe, and M. Shabad, Credit card fraud detection at merchant side using neural networks, in *Proc. 3rd Int. Conf. Computing for Sustainable Global Development*, New Delhi, India, 2016, pp. 667–670.

[109] T. K. Behera and S. Panigrahi, Credit card fraud detection: A hybrid approach using fuzzy clustering & neural network, in *Proc. 2nd Int. Conf. Advances in Computing and Communication Engineering*, doi:10.1109/ICACCE.2015.33.

[110] B. J. Ford, H. Xu, and I. Valova, A real-time self-adaptive classifier for identifying suspicious bidders in online auctions, *Comput. J.*, vol. 56, no. 5, pp. 646–663, 2013.

[111] C. Liu, Q. W. Zhong, X. Ao, L. Sun, W. L. Lin, J. H. Feng, Q. He, and J. Y. Tang, Fraud transactions detection via behavior tree with local intention calibration, in *Proc. 26th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, Virtual Event, 2020, pp. 3035–3043.

[112] S. Alqethami, B. Almutanni, and M. Alghamdi, Fraud detection in E-commerce, *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 6, pp. 200–206, 2021.

[113] A. Maurya and A. Kumar, Credit card fraud detection system using machine learning technique, in *Proc. IEEE Int. Conf. Cybernetics and Computational Intelligence*, Malang, Indonesia, 2022, pp. 500–504.

[114] V. H. Khang, C. T. Anh, N. D. Thuan, and H. C. M. City, Detecting fraud transaction using ripper algorithm combines with ensemble learning model, *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, p. 2023, 2023.

[115] Z. Li, M. Huang, G. Liu, and C. Jiang, A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud

detection, *Expert Systems with Applications*, vol. 175, pp. 114750, 2021.

[116] V. H. Khang, C. T. Anh, and N. D. Thuan, Detecting fraud transaction using ripper algorithm combines with ensemble learning model, *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 336–345, 2023.

[117] L. Zheng, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, Improved TrAdaBoost and its application to transaction fraud detection, *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 5, pp. 1304–1316, 2020.

[118] B. B. Jayasingh and G. B. Sri, Online transaction anomaly detection model for credit card usage using machine learning classifiers, in *Proc. Int. Conf. Emerging Smart Computing and Informatics*, Pune, India, 2023, pp. 1–5.

[119] R. Raja, K. K. Nagwanshi, S. Kumar, and K. R. Laxmi, *Data Mining and Machine Learning Applications*. Beverly, MA, USA: Scrivener Publishing, 2022.

[120] Y. J. Lee, Y. R. Yeh, and Y. C. F. Wang, Anomaly detection via online oversampling principal component analysis, *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1460–1470, 2013.

[121] R. Saia, L. Boratto, and S. Carta, Multiple behavioral models: A divide and conquer strategy to fraud detection in financial data streams, in *Proc. 7th Int. Joint Conf. Knowledge Discovery, Knowledge Engineering and Knowledge Management*, Lisbon, Portugal, 2015, pp. 496–503.

[122] G. A. Montazer and S. ArabYarmohammadi, Detection of phishing attacks in Iranian e-banking using a fuzzy-rough hybrid system, *Appl. Soft Comput.*, vol. 35, pp. 482–492, 2015.

[123] D. Trisanto, N. Rismawati, M. F. Mulya, and F. I. Kurniadi, Effectiveness undersampling method and feature reduction in credit card fraud detection, *Int. J. Intell. Eng. Syst.*, vol. 13, no. 2, pp. 173–181, 2020.

[124] M. Shao, N. Gu, and X. Zhang, Credit card transactions data adversarial augmentation in the frequency domain, in *Proc. 5th IEEE Int. Conf. Big Data Analytics*, Xiamen, China, 2020, pp. 238–245.

[125] Z. Li, H. Wang, P. Zhang, P. Hui, J. Huang, J. Liao, J. Zhang, and J. Bu, Live-streaming fraud detection: A heterogeneous graph neural network approach, in *Proc. 27th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, Singapore, 2021, pp. 3670–3678.

[126] S. Subbulakshmi and D. J. Evanjaline, An efficient analytics in credit card fraud detection using resolution classification (Rc) technique, *Int. J. Sci. Technol. Res.*, vol. 9, no. 2, pp. 3284–3289, 2020.

[127] H. Chi, Y. Lu, B. Liao, L. Xu, and Y. Liu, An optimized quantitative argumentation debate model for fraud detection in E-commerce transactions, *IEEE Intell. Syst.*, vol. 36, no. 2, pp. 52–63, 2021.

[128] K. N. Mishra, V. P. Mishra, S. Saket, and S. P. Mishra, Hybrid approach for deception tracing in smart cities using LR and *n*-fold intelligent machine learning techniques, *Int. J. Manag. Pract.*, vol. 15, no. 4, pp. 460–487, 2022.

[129] B. Lebichot, T. Verhelst, Y. A. Le Borgne, L. He-Guelton, F. Oble, and G. Bontempi, Transfer learning strategies for credit card fraud detection, *IEEE Access*, vol. 9, pp. 114754–114766, 2021.

[130] K. Huang, An optimized LightGBM model for fraud detection, *J. Phys.: Conf. Ser.*, vol. 1651, no. 1, p. 012111, 2020.

[131] P. Mrozek, J. Panneerselvam, and O. Bagdasar, Efficient resampling for fraud detection during anonymised credit card transactions with unbalanced datasets, in *Proc. IEEE/ACM 13th Int. Conf. Utility and Cloud Computing*, Leicester, UK, 2020, pp. 426–433.

[132] A. K. Rai and R. K. Dwivedi, Fraud detection in credit card data using unsupervised machine learning based scheme, in *Proc. Int. Conf. Electronics and Sustainable Communication Systems*, Coimbatore, India, 2020, pp. 421–426.

[133] Y. Lucas, P. E. Portier, L. Laporte, L. He-Guelton, O. Caelen, M. Granitzer, and S. Calabretto, Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs, *Future Gener. Comput. Syst.*, vol. 102, pp. 393–402, 2020.

[134] Y. Fang, Y. Zhang, and C. Huang, Credit card fraud detection based on machine learning, *Comput. Mater. Contin.*, vol. 61, no. 1, pp. 185–195, 2019.

[135] R. Abiramy, K. Narayanan, R. Anandan, and C. S. Paul, Fraud detection for online retail using random forest, *Int. J. Eng. Adv. Technol.*, vol. 8, no. 3S, pp. 1–6, 2019.

[136] R. Jhangiani, D. Bein, and A. Verma, Machine learning pipeline for fraud detection and prevention in E-commerce transactions, in *Proc. IEEE 10th Annu. Ubiquitous Computing, Electronics and Mobile Communication Conf.*, New York, NY, USA, 2019, pp. 135–140.

[137] U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, Using generative adversarial networks for improving classification effectiveness in credit card fraud detection, *Inf. Sci.*, vol. 479, pp. 448–455, 2019.

[138] R. Saia and S. Carta, A frequency-domain-based pattern mining for credit card fraud detection, in *Proc. of 2nd International Conference on Internet of Things, Big Data and Security* (*IoTBDS-2017*), doi:10.13140/RG.2.2.36578.

[139] A. Shaji, S. Binu, A. M. Nair, and J. George, Fraud detection in credit card transaction using ANN and SVM, doi: 10.1007/978-3-030-79276-3_14.

[140] R. Saia, Unbalanced data classification in fraud detection by introducing a multidimensional space analysis, in *Proc. 3rd Int. Conf. Internet of Things, Big Data and Security*, Funchal, Portugal, 2018, pp. 29–40.

[141] A. Shaji, S. Binu, A. M. Nair, and J. George, Fraud detection in credit card transaction using ANN and SVM, in *Proc. 4th EAI Int. Conf. Ubiquitous Communications and Network Computing*, Virtual Event, 2021, pp. 187–197.

[142] M. A. Jawed, D. K. Sasmal, and M. U. Khan, Credit card fraud detection, http://localhost:8080/xmlui/handle/123456789/14658, 2022.

[143] J. Lee, Y. C. Lee, and J. T. Kim, Fault detection based on

one-class deep learning for manufacturing applications limited to an imbalanced database, *J. Manuf. Syst.*, vol. 57, pp. 357–366, 2020.

[144] M. A. Jawed, D. K. Sasmal, and M. U. Khan, Credit card fraud detection, http://localhost:8080/xmlui/handle/123456789/14658, 2021.

[145] L. Zhinin-Vera, Credit card fraud detection using artificial intelligence, doi:10.13140/RG.2.2.13642.18885.

[146] S. B. E. Raj and A. A. Portia, Analysis on credit card fraud detection methods in *Proc. Int. Conf. Computer, Communication and Electrical Technology*, Tirunelveli, India, 2011, pp. 152–156.

[147] L. Moumeni, M. Saber, I. Slimani, I. Elfarissi, and Z. Bougroun, Machine learning for credit card fraud detection, in *Proc. 6th Int. Conf. Wireless Technologies, Embedded, and Intelligent Systems*, Singapore, 2022, pp. 211–221.

[148] A. S. Muttipati, S. Viswanadham, R. Dharavathu, and J. Nema, LightGBM model for credit card fraud discovery, in *Proc. 6th Int. Conf. Microelectronics, Electromagnetics and Telecommunications*, Singapore, 2022, pp. 51–58.

[149] A. Mohari, J. Dowerah, K. Das, F. Koucher, and D. J. Bora, Credit card fraud detection techniques: A review, in *Soft Computing for Intelligent Systems*, N. Marriwala, C. C. Tripathi, S. Jain, and S. Mathapathi, eds. Singapore: Springer, 2022, pp. 157–166.

[150] V. N. Dornadula and S. Geetha, Credit card fraud detection using machine learning algorithms, *Procedia Computer Science*, doi: 10.1016/j.procs.2020.01.057.

[151] B. Al-Smadi, Credit card security system and fraud detection algorithm, PhD dissertation, Louisiana Tech University, Ruston, LA, USA, 2021.

[152] V. N. Dornadula and S. Geetha, Credit card fraud detection using machine learning algorithms, *Procedia Comput. Sci.*, vol. 165, pp. 631–641, 2019.

[153] Y. Sahin and E. Duman, Detecting credit card fraud by ANN and logistic regression, in *Proc. Int. Symp. Innovations in Intelligent Systems and Applications*, Istanbul, Turkey, 2011, pp. 315–319.

[154] S. L. Marie-Sainte, M. B. Alamir, D. Alsaleh, G. Albakri, and J. Zouhair, Enhancing credit card fraud detection using deep neural network, in *Proc. 2020 Computing Conf. Intelligent Computing*, Switzerland, 2020, pp. 301–313.

[155] M. Puh and L. Brkic, Detecting credit card fraud using selected machine learning algorithms, in *Proc. 42nd Int. Convention on Information and Communication Technology, Electronics and Microelectronics*, Opatija, Croatia, 2019, pp. 1250–1255.

[156] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, Fraud detection in banking data by machine learning techniques, *IEEE Access*, vol. 11, pp. 3034–3043, 2023.

[157] B. Chugh and N. Malik, Machine learning classifiers for detecting credit card fraudulent transactions, in *Information and Communication Technology for Competitive Strategies*, A. Joshi, M. Mahmud, and R. G. Ragel, eds. Singapore: Springer, 2023, pp. 223–231.

[158] U. L. Chilaka, G. A. Chukwudebe, and A. Bashiru, A review of credit card fraud detection techniques in electronic finance and banking, *Iconic Research and Engineering Journals*, vol. 3, no. 2, pp. 456–467, 2019.

[159] J. Liu, X. Gu, and C. Shang, Quantitative detection of financial fraud based on deep learning with combination of E-commerce big data, *Complexity*, vol. 2020, p. 6685888, 2020.

[160] F. S. Nezhad and H. R. Shahriari, Fuzzy logic and Takagi-Sugeno Neural-Fuzzy to Deutsche bank fraud transactions, in *Proc. 7th Int. Conf. e-Commerce in Developing Countries*: *With Focus on e-Security*, Kish Island, Iran, 2013, pp. 1–15.

[161] M. K. Khormuji, M. Bazrafkan, M. Sharifian, S. J. Mirabedini, and A. Harounabadi, Credit card fraud detection with a cascade artificial neural network and imperialist competitive algorithm, *International Journal of Computer Applications*, vol. 96, no. 25, pp. 1–9, 2014.

[162] L. Zhou, J. Dang, and Z. Zhang, Research on fault diagnosis for on-board equipment of train control system based on imbalanced text classification, *J. Appl. Sci. Eng.*, vol. 24, no. 2, pp. 167–175, 2021.

[163] J. Wang, R. Wen, C. Wu, Y. Huang, and J. Xiong, FDGars: Fraudster detection via graph convolutional networks in online app review system, in *Proc. Web Conference 2019 - Companion of the World Wide Web Conference, WWW 2019*, doi: 10.1145/3308560.3316586.

[164] J. Wang, R. Wen, C. Wu, Y. Huang, and J. Xiong, FdGars: Fraudster detection via graph convolutional networks in online app review system, in *Proc. World Wide Web Conf.*, San Francisco, CA, USA, 2019, pp. 310–316.

[165] R. Kawase, F. Diana, M. Czeladka, M. Schüler, and M. Faust, Internet fraud: The case of account takeover in online marketplace, in *Proc. 30th ACM Conf. Hypertext and Social Media*, Hof, Germany, 2019, pp. 181–190.

[166] P. Pant, P. Srivastava, and A. Gupta, Provisional research on ensemble learning techniques for card fraud detection, *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6S, pp. 13–17, 2019.

[167] W. H. Chang and J. S. Chang, A novel two-stage phased modeling framework for early fraud detection in online auctions, *Expert Syst. Appl.*, vol. 38, no. 9, pp. 11244–11260, 2011.

[168] J. S. Chang and W. H. Chang, Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters, *Electron. Commer. Res. Appl.*, vol. 13, no. 2, pp. 79–97, 2014.

[169] S. S. Bhakta, S. Ghosh, and B. Sadhukhan, Credit card fraud detection using machine learning: A comparative study of ensemble learning algorithms, in *Proc. 9th Int. Conf. Smart Computing and Communications* (*ICSCC*), Kochi, India, 2023, pp. 296–301.

[170] Z. Faraji, A review of machine learning applications for credit card fraud detection with a case study, *SEISENSE Journal of Management*, vol. 5, no. 1, pp. 49–59, 2022.

[171] G. Douzas and F. Bacao, Effective data generation for

imbalanced learning using conditional generative adversarial networks, *Expert Syst. Appl.*, vol. 91, pp. 464–471, 2018.

[172] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, SMOTE: Synthetic minority over-sampling technique, *J. Artif. Intell. Res*., vol. 16, pp. 321–357, 2002.

[173] V. F. Rodrigues, L. M. Policarpo, D. E. da Silveira, R. da Rosa Righi, C. A. da Costa, J. L. V. Barbosa, R. S. Antunes, R. Scorsatto, and T. Arcot, Fraud detection and prevention in e-commerce: A systematic literature review, *Electron. Commer. Res. Appl*., vol. 56, p. 101207, 2022.

[174] C. Ludl, S. McAllister, E. Kirda, and C. Kruegel, On the effectiveness of techniques to detect phishing sites, in *Proc. 4th Int. Conf. Detection of Intrusions and Malware, and Vulnerability Assessment*, Lucerne, Switzerland, 2007, pp. 20–39.

[175] C. E. H. Chua and J. Wareham, Fighting internet auction fraud: An assessment and proposal, *Computer*, vol. 37, no. 10, pp. 31–37, 2004.

Fernando Bacao is a full professor at NOVA Information Management School, Universidade Nova de Lisboa, Portugal, where he is also the director of the master in information management. He holds the PhD degree in information management and his research interests include machine learning and data science, with particular emphasis on geospatial applications, text mining, and imbalanced learning. His research work has appeared in journals, such as *Information Sciences*, *Expert Systems with Applications*, *International Journal of Intelligent Systems*, *Information & Management*, *International Journal of Wildland Fire*, *International Journal of Geographical Information Science*, among other. Additional details can be found in https://www.novaims.unl.pt/fbacao/.

Abed Mutemi is a senior lead data scientist at Meta (control risks), and is affiliated with NOVA Information Management School, Universidade Nova de Lisboa, Campus de Campolide, Lisboa, Portugal, where he is doing academic research in information management systems. His areas of interest include fraud detection systems for digital marketplaces, threat intelligence and management systems, product security systems, payments and financial services systems, imbalanced learning, machine learning design, deep learning, and generative AI. His research work has appeared in Nature, among other peer reviewed journals.