6-18-2022

A TAXONOMY OF MACHINE LEARNING-BASED FRAUD DETECTION SYSTEMS

Tizian Matschak
University of Goettingen, tizian.matschak@uni-goettingen.de

Simon Trang
University of Göttingen, simon.trang@wiwi.uni-goettingen.de

Christoph Prinz
University of Goettingen, christoph.prinz@uni-goettingen.de

A TAXONOMY OF MACHINE LEARNING-BASED FRAUD DETECTION SYSTEMS

Research Paper

Tizian Matschak, University of Goettingen, Goettingen, Germany, tizian.matschak@uni-goettingen.de

Christoph Prinz, University of Goettingen, Goettingen, Germany, christoph.prinz@uni-goettingen.de

Simon Trang, University of Goettingen, Goettingen, Germany, strang@uni-goettingen.de

Abstract

As fundamental changes in information systems drive digitalization, the heavy reliance on computers today significantly increases the risk of fraud. Existing literature promotes machine learning as a potential solution approach for the problem of fraud detection as it is able able to detect patterns in large datasets efficiently. However, there is a lack of clarity and awareness on which components and functionalities of machine learning-based fraud detection systems exist and how these systems can be classified consistently. We draw on 54 identified relevant machine learning-based fraud detection systems to address this research gap and develop a taxonomic scheme. By deriving three archetypes of machine learning-based fraud detection systems, the taxonomy paves the way for research and practice to understand and advance fraud detection knowledge to combat fraud and abuse.

Keywords: Fraud Detection, Machine Learning, Anomaly Detection, Taxonomy.

1 Introduction

Every second organization has already been a victim of fraud at least once in 2020 (PwC, 2020). They lose an estimated 5% of revenue to fraud every year (ACFE, 2020). Projected against the 2019 GDP ($87,345.3 billion) that's more than $4.3 trillion lost to fraud globally each year. Besides the direct financial losses, organizations can face loss of reputation and trust and, thus, customer loyalty as well (Akgul, 2021a). Therefore, effectively combating fraud can provide a strategic business advantage. Based on the British Fraud Act (2006), we define fraud as the *misuse of a system by obtaining financial advantage or causing loss by implicit or explicit deception*.

Fraud is not a phenomenon of a single industry but can be observed across industries and the entire value chain. Exemplary fraud types are financial (bank and insurance) fraud, telecommunication fraud, healthcare fraud, and e-commerce fraud. In practice, such fraud types could be operationalized as follows (Baesens *et al.*, 2015): Opening a new bank account by using a victim's information without his knowledge and permission (banking), invoicing for the services not performed (healthcare), selling services that do not exist (insurance). Based on this macroeconomic relevance, various ways to combat fraud have been researched and implemented in real-world use cases in recent years.

Besides statistical and rule-based approaches, machine learning (ML) in particular is suitable for the problem of fraud detection as it is able to efficiently detect patterns in large datasets, which promotes further automation of the fraud detection process, thus helping to make the process more economical (Matschak *et al.*, 2021). Facing increasing numbers of transactions annually (Jhangiani *et al.*, 2019), ML-based approaches have proven their superiority and future potentials over classic (rule-based) methods in several research papers and case studies (e.g., Samakovitis and Stelios Kapetanakis (2013), Matschak et al. (2021), Akgul (2021b)). Here, researchers focused not only on designing and analyzing fraud detection systems (FDSs) themselves and their integration in real-world use cases but also dealt

with the optimization of single system components. As ML and its integration in FDSs is a relatively new discipline in IS research, the body of literature regarding technological ML-based fraud detection components, their configuration, and processual integration increases constantly.

Researchers not only use several ML algorithm types such as supervised, unsupervised, and semi-supervised (Bhattacharya and Lindgreen, 2020) standalone, but tackle fraud detection specific problems, namely strong class imbalance, a limited amount of training data, and changing fraud patterns (Debener *et al.*, 2021; Jurgovsky *et al.*, 2018) by additional system components and functionalities. Current research has demonstrated that developed concepts and designs can improve fraud detection performance. However, the emerging literature stream on ML-based FDSs reveals different perceptions towards these components and their combination with each other. In this context, we identify three challenges in the current fraud detection literature.

Firstly, the level of abstraction varies across research articles. While in one extreme, authors deal with ML-based FDSs implemented in real-world scenarios, in the other extreme authors, focus on just one aspect of a component designed and tested in a laboratory environment. Consequently, there is uncertainty on which component harmonizes with which component or system setup.

Secondly, by revisiting current literature, we observed many manifestations of the components that present authors with at least two subsequent problems. On the one hand, authors need to know all possible expressions to base their design decisions on these options and yield the best possible performance for their specific use case. On the other hand, as a consequence of uncertainty and a lack of components overview, research produces duplications when two authors claim the same configuration of an ML-based fraud detection system. This hinders research progress and costs unnecessary resources.

Thirdly, we discover differences between those components studied in theory and those applied in actual real-world FDSs. Many authors test their designs in a laboratory setup or on artificial data, leaving the question of practicality unanswered. This indicates a gap between practical evaluation and theoretical analysis. Therefore, an underlying need exists in recent literature to determine which component setups are used in practice and provide value to practitioners. Conversely, this enables a subsequent review of these applied just in academia.

Our review highlights a need for a systematic classification of actual ML-based FDSs to investigate the combination and configuration of associated components in two aspects. We observe different research levels (system vs. component) in current literature that may severely impact the applicability of research findings. Moreover, we identify a lack of awareness of FDS component combination possibilities and their practicability. Due to a large production of FDS studies published in different fields, many authors are not aware of other's works which leads to duplicates. Building on existing ML-based FDS and deriving archetypes from them offers the possibility to either adopt one of these common compositions of FDS characteristics/components or to adapt it to the specific use case. Thus, providing researchers and practitioners with general types of ML-based FDS that can be used as a blueprint for rapid prototyping could help bridge the gap betweed FDS and fraudsters strategies more efficiently.

Against this background, our paper aims to develop an overarching ML-based fraud detection taxonomic scheme guided by the following research questions:

RQ1: How can ML-based fraud detection systems be classified?

RQ2: What archetypal ML-based fraud detection systems exist?

To do so, we follow a three-phase taxonomy building method. First, we enrich our understanding of the current ML-based fraud detection landscape by identifying a dataset of 54 scientific studies (phase 1). Secondly, we utilize the concepts and characteristics gathered in the database to develop a taxonomy following the approach of Nickerson et al. (2013). Thirdly, we apply the resulting taxonomy and composed dataset to derive archetypal ML-based FDSs using k-means cluster analysis (phase 3).

With our research, we contribute to the discussion of innovative fraud detection approaches in at least three ways. First, we provide a taxonomy to classify FDSs to enable users, researchers, and developers to know if a new FDS approach is something entirely new and unique, a significant variation of an existing approach, or just a reflection of what is already known. Second, the structured composition of

the current knowledge base of ML-based fraud detection identifies characteristics and research gaps to lead and accelerate future research in this dynamic domain. The derived archetypes provide a baseline for a practical application of the taxonomy and pave the way for developing guidelines for FDS design. Third, our taxonomy and identified dimensions provide a methodological blueprint to further studies of taxonomy development to build on.

The paper is structured as follows. We first provide an overview of previous research works dealing with ML-based FDSs and their components. Subsequently, we present the 3-phase methodological approach and give an outline of our obtained results. Finally, the implications and limitations of this study are discussed, and a conclusion is drawn.

2 Research Background

As introduced, we define fraud as the misuse of a system by obtaining financial advantage or causing loss by implicit or explicit deception. Reviewing the literature and in consensus with Cressey (1953), we conclude that fraud potentials arise when there is an incentive to commit fraud, a rationalization for justifying fraudulent behavior, and an opportunity to commit fraud. As fundamental changes in information systems drive digitalization, the heavy reliance on computers today significantly increases the risk of fraud. Electronic variations of traditional frauds are carried out with greater efficiency and effectiveness and, thus, could have potentially greater impact and will be more difficult to investigate (Wardlaw, 1999). As a result, fraud places a significant financial burden on organizations, customers, and other stakeholders (Vaisu *et al.*, 2003). In addition to the financial impact, fraud can also affect the reputation in the eyes of customers and customer trust (Akgul, 2021b).

Based on that, especially transaction-based businesses such as banking, insurance, e-commerce, and healthcare emerge as affected business domains. These industries have in common that they are characterized by an extensive quantity of transactions on the one hand and, on the other hand, by a high value per transaction. Thereby, the large number of transactions means both that not all transactions can be thorouhly checked manually, which in turn leads to fraud cases being uncovered and making fraud worthwhile, and on the contrary, that, based on the amount of available data, this is a potentially suitable use case for ML. For comparability and the research goal of developing a taxonomy for ML-based fraud detection, therefore, we will devote the remainder of the paper to these relevant industries, namely e-commerce, banking, insurance, and in particular, healthcare. We will outline typical fraud types assigned to these industries in the following.

The growth of electronic commerce has been accompanied by an increase in fraudulent practices since the first e-commerce transaction in 1995 (Lek *et al.*, 2001; Sharma *et al.*, 2016). While fraud patterns may occur, detecting, managing, and controlling these patterns is difficult due to the increasing number of online transactions currently handled by e-commerce systems (Lek *et al.*, 2001). As e-commerce provides a 24/7 unlimited shopping platform, the potential for fraud also exists around the clock. There are many potential *e-commerce fraud* cases: Merchant has no authorization, authorization canceled, charged my expired card, goods returned but not money, service not rendered, etc. (Alanezi and Brooks, 2014).

Financial fraud is one of the main problems in the financial industry, not just because of potential financial loss but also for customer thrust (Akgul, 2021b). Criminals and criminal organizations often make use of companies and other corporate entities in order to, e.g., hide their identity, conceal illicit flows of money, launder funds, finance terrorist organizations, evade taxes, create and hide slash funds, commit bribery, corruption, and accounting frauds (Bellini, 2014). We summarize these financial crimes under the term *financial fraud.* In addition, all these frauds are inter-connected as the illegal profits need to be re-integrated into the financial system, aka ‘laundered’ (Bellini, 2014).

Information asymmetries are a key characteristic of many interactions in insurance services, e.g., automobile insurance (Derring, 2002; Dionne *et al.*, 2009). Exploiting one of these information asymmetries by policyholders or other parties is defined as *insurance claim fraud* (Debener *et al.*, 2021).

A special subcategory of insurance fraud is *healthcare fraud* (health insurance fraud). Healthcare has become a major expenditure for the society and financial systems, while annually increasing global spending in health is expected to reach $18.28 trillion by 2040 (Bauder *et al.*, 2018; Dieleman *et al.*, 2016). In parallel, healthcare emerged as an attractive fraud target due to its complexity, analogous processes, and transactional value (Bauder *et al.*, 2016; Dora and Sekharan, 2015; Waghade and Karandikar, 2018). Consequently, the healthcare domain faces an increasing number of fraud incidents every year from dishonest providers, organized criminals, colluding patients, and patients who misrepresent their eligibility for health insurance coverage (Dora and Sekharan, 2015; Thornton *et al.*, 2015). Consequently, fraud is driving up costs for insurers, premiums for policyholders, expenses for providers, and thus, is weakening the backbone of the healthcare system (Rawte and Anuradha, 2015).

Based on the relevant literature and these fraud cases, we derived characteristics of the fraud detection problem that must be considered when designing an ML-based approach to detect fraud:

- *Strong Class Imbalance*
  Fraud detection typically deals with the problem of identifying a few fraudulent cases in a vast number of normal cases (Yang and Xu, 2019), in other words: the search for the needle in the haystack. Accordingly, ML algorithms may face degradation of classification performance caused by the class imbalance, minority class decomposition into sub-parts, and overlapping classes (Dal Pozzolo *et al.*, 2015). Considering a binary classification task since it is anomaly detection and a minority class partition of 0.6%, an algorithm can trivially gain 99.4% accuracy by simply learning the rule *f(x)=normal* (always classify as normal; Murphy, 2012). This makes the learning of a classifier quite challenging (Chandola *et al.*, 2009).
- *Processing of Sensitive Data*
  Where machine learning appears to be an appropriate technology for fraud detection due to the volume of transnational data, this data is often tagged with personal (customer) attributes such as gender, banking data, address, health data, etc. This data is protected both by various generic data protection regulations (for example, the European GDPR) and, in some cases, again by specific industry-related guidelines. In addition, besides customer privacy, the data may have importance as a source of proprietary information for the organization itself (Wang *et al.*, 2018). Implications for ML are twofold; on the one hand, ML can identify (customers') patterns that may themselves be treated as private data; on the other hand, barriers to data sharing make it difficult to coordinate large-scale collaborative studies (Wang *et al.*, 2018).
- *Limited Amount of Labelled Data*
  As manually identifying fraud is highly time and cost-sensitive, only a few fraudulent cases get detected as fraud (Viaene *et al.*, 2007). This leads to a limited amount of labeled data available for processing in the development and evaluation process of an ML-based fraud detection system. In addition, even though researchers demonstrated that data sharing improves fraud detection performance (Power and Power, 2015), organizations are reluctant to share their data with third parties. The fear of potential regulatory problems, data security, privacy concerns, and own corporate interests are also present (Bauder and Khoshgoftaar 2017b; Chandola et al. 2013). Consequently, fraud detection approaches must deal with learning from relatively few labeled cases while mitigating the risk of overfitting (Debener *et al.*, 2021).
- *Dynamic Fraud and Patterns (Concept Drift)*
  Even if labeled fraud data may become available, fraud patterns are dynamic and evolve over time; thus, they are difficult to detect (Debener *et al.*, 2021; Jurgovsky *et al.*, 2018). Due to fraudsters changing their fraud behavior as time evolves, there is no obvious pattern of fraud that can be applied as a one-fits-all solution (Sun *et al.*, 2019). This is contrary to most other classification problems ML is currently applied for (e.g., image classification) and raises the need for alternative solution approaches.

3 Research Approach to Taxonomy Development

In consensus with other relevant literature in IS research (e.g., Rau et al. (2020), Remane et al. (2016)), we adapted a three-phase research design approach (see Table 1) to answer the two research questions at the core of this study. Phase 1 involves the preliminary work of setting up the taxonomy research database through a literature search. Phase 2 utilizes the concepts and characteristics gathered in the database to develop a taxonomy following the approach of Nickerson et al. (2013). This addresses the first research question (RQ1), which calls for an overview of the most prevalent ML-based FDS characteristics. Phase 3 concludes with publication analysis using the developed taxonomy to answer the second research question (RQ2), which calls for an overview of existing archetypes of ML-based FDSs.

	Phase 1: **Set Up the Database**	**Phase 2:** **Taxonomy Development**	**Phase 1:** **Conduct Cluster Analysis and Derive Archetypes**
Steps	▪ Create search string for keyword search ▪ Perform backward and forward search ▪ Add relevant literature to the database	▪ Define meta-characteristic for the taxonomy ▪ Iterate through taxonomy development until ending conditions are met	▪ Determine appropriate number of clusters ▪ Specify the FDSs belonging to each cluster
Method	Literature review	Taxonomy development	Clustering Analysis
Source	Literature on ML-based FDSs in finance, insurance and e-commerce	Literature on ML-based FDSs	Taxonomy of ML-based FDSs with empirical data
Results	Database with 54 FDSs	Taxonomy of ML-based FDSs with 10 dimensions	Three identified archetypes of ML-based FDSs

Table 1: Three-Phase Research Approach

3.1 Phase 1: Set Up the Database

The objective of the first phase was to generate a research database including all relevant publications to be considered in the taxonomy building process. We required publications to include the development and/or testing of ML-based FDSs to be considered in the database. To build our research database, we applied the following procedure. Firstly, we analyzed recent literature reviews (Minastireanu & Mesnita (2019), Ngai et al. (2011), Omar et al. (2018), Paruchuri (2017), and Pourhabibi et al. (2020)), and identified publications regarding ML-based FDSs in relevant domains. Next, we performed a structured literature review following the framework introduced by Webster and Watson (2002) until 28th of October 2021. Therefore, we added publications via keyword search in the most relevant publication databases (ScienceDirect, EbscoHost, AIS electronic library, Springer Link and IEEE Xplore) using the query:

(“fraud detection” OR “anomaly detection”) AND (“insurance” OR “finance” OR “banking” OR “healthcare” OR “e-commerce) AND “machine learning”

We conducted a forward and backward search to complete the database, resulting in additional publications (Webster and Watson, 2002). In total, we gathered 54 publications to be included in our research database. Although we strive for high-quality research publications to be the basis of our review, we did not limit our literature search to high-ranking journals, opting to include lower-ranking journals and conferences to obtain an extensive research overview of a practical problem.

3.2 Phase 2: Taxonomy Development

The goal of the second phase was to systematically develop a taxonomy for ML-based FDSs that incorporates the most relevant dimensions. We applied the taxonomy-development method suggested by Nickerson et al. (2013), which provides a structured process for developing taxonomies based on existing theoretical foundations (deduction), as well as empirical evidence (induction) in an iterative manner (Eickhoff *et al.*, 2017). Therefore, we conceptually develop the taxonomy and derive associated dimensions by building upon the previously gathered publications regarding ML-based FDSs (conceptual-to-empirical). Subsequently, related characteristics are drawn from empirically examining ML-based FDSs and associated components (empirical-to-conceptual). The applied taxonomy development approach has been applied by several other studies in the IS field, such as Tan et al. (2016) or Eickhoff et al. (2017), and has been shown to be useful. Moreover, this approach suits our research and assists us in addressing the research problem as follows: First, we can verify that specific FDS components are applied in practice and provide practicality by reviewing implementations and their evaluation in literature. Secondly, the methodology enables us to identify common characteristics of components and configurations in practice that have not been previously explored in the literature. The method consists of the following steps (see Figure 1):

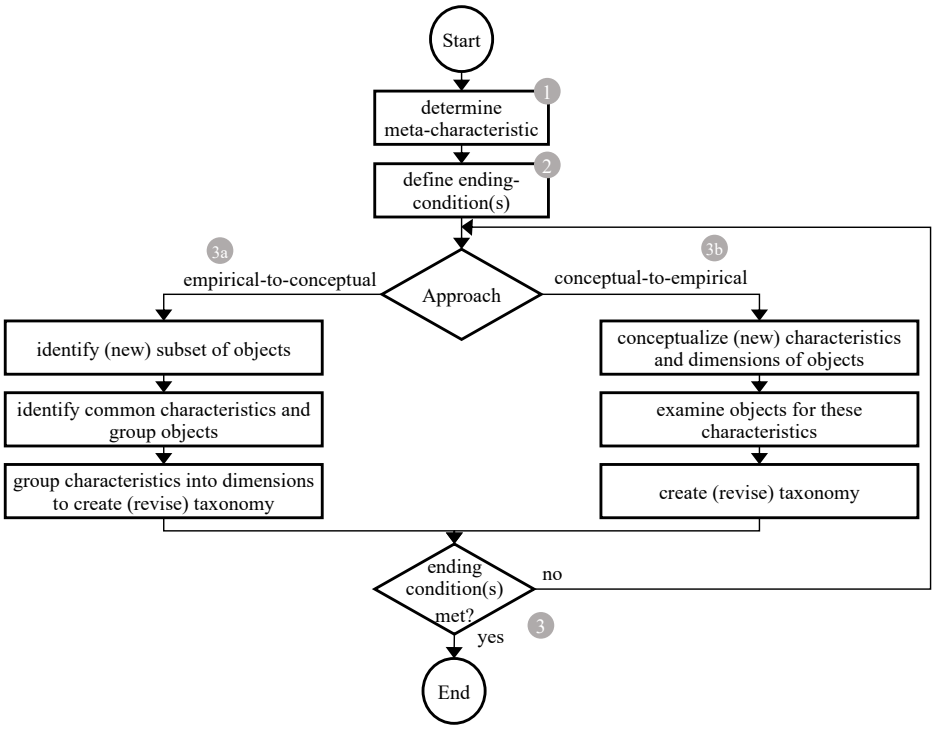

Figure 1: Taxonomy development process (Nickerson et al.*, 2013)*

Following this process, we defined the meta-characteristic first. It highly influences the outcome of the emerging taxonomy and indicates the utilization scope of a taxonomy (Nickerson *et al.*, 2013). Since the taxonomy contains characteristics of ML-based FDSs, particularly with a focus on components and their configuration, we define the meta-characteristic as *components of ML-based FDSs*. All derived dimensions must be a consequence of this meta-characteristic and should describe a conceptual difference of analyzed ML-based FDSs (Nickerson *et al.*, 2013).

Furthermore, we applied seven of the eight objectives and all five subjective ending conditions from Nickerson et al. (2013). We omitted the objective condition of "At least one object is classified under every characteristic of every dimension" (Nickerson *et al.*, 2013) since we aim to include un-operationalized characteristics of ML-based FDSs to obtain a complete view of the status-quo of the theoretical background and its practice implementation. In addition, this approach allows us to identify research gaps that can then be addressed in future research. Hence, we altered the rule as follows:

At least one object is classified under every characteristic of every dimension, or the characteristic must be the logical and feasible opposite, combination, or component of previously identified characteristics.

All these ending conditions are checked during taxonomy development and after each iteration of revising the taxonomy's dimensions and/or characteristics. Only in the case of all conditions being satisfied, the taxonomy can be seen as mature, and the development process terminates. During each iteration, the revision of dimensions and/or characteristics of the taxonomy is done based on either deductive (conceptual- to-empirical) or inductive (empirical-to-conceptual) reasoning.

We ran through four iterations, each with a subset of the previousls identified FDS studies, until all publications from the research database were satisfactorily classified (see Figure 2). Our first cycle was conceptual-to-empirical. Subsequently, three empirical-to-conceptual cycles were performed to obtain a final taxonomy fulfilling the objective and subjective ending conditions. Thereby, the taxonomy building process stops by meeting the ending conditions in the fourth iteration.

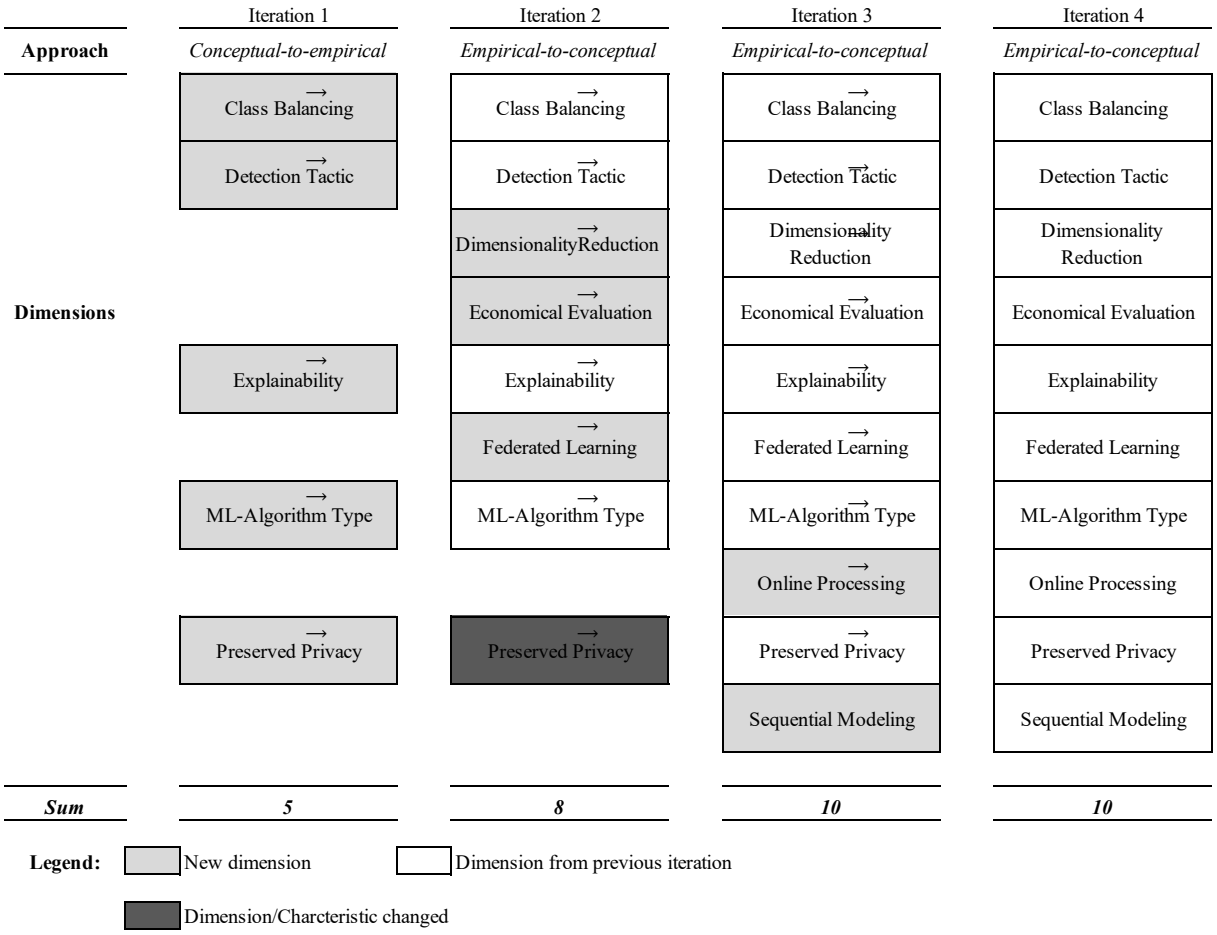

Figure 2: Taxonomy Development Iterations

3.3 Phase 3: Cluster Analysis

Taxonomies are often validated through their application to identify patterns within data that highlight structural differences of the analyzed objects. Thus, the third phase applied a clustering analysis to empirically identify archetypes of ML-based FDSs from the taxonomy. The goal of a clustering analysis is to define groups of objects whereby objects in the same group are as similar as possible and objects in different groups are as dissimilar as possible (Kaufman and Rousseeuw, 2009). Based on the findings of Remane et al. (2016) and Punj and Steward (1983), we decided to perform a two-step clustering analysis as it proved to deliver superior results compared to simple cluster analysis. First, we used

Ward's method (agglomerative clustering) to specify the number of clusters. Then we applied k-means (centroids-based clustering) to further specify the clusters by iterative partitioning.

Following this concept, we first perform Ward's method. This method is an agglomerative clustering approach that iteratively combines the two closest objects into one group until, at a final stage, all objects belong to the same group (cluster) (Landau and Everitt, 2004). Here, the similarity between objects is calculated by their number of identical characteristics along the taxonomy dimensions using the squared Euclidean distance. We are aware of the possibility of using alternative distances. However, Euclidean distance has proven to provide suitable results in previous studies (e.g., Remane et al. (2016)). Subsequently, the appropriate number of clusters (k) must be determined. To do so, we use the scree plot to apply the elbow rule (Yuan and Yang, 2019) (see Figure 3). These statistics indicated that three clusters would be most useful in our context.

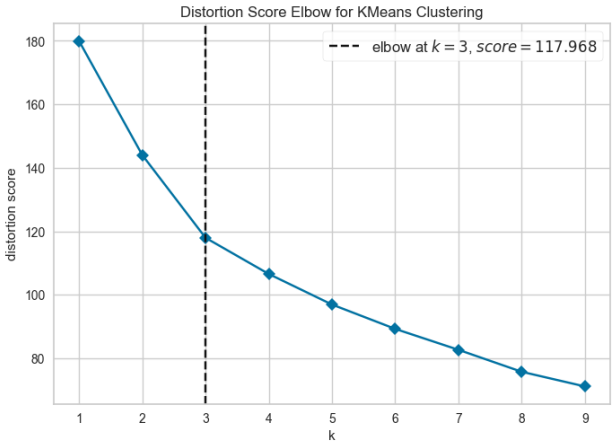

Figure 3: Elbow Method - Scree Plot

Second, we applied the k-means algorithm using the previously defined number of clusters k = 3. The k-means algorithm is a clustering method based on an iterative partition of a set of objects. The algorithm goes through several rounds of optimization for an a priori defined number of clusters k until each object is closer to the mean vector of its group than that of any other group (Landau and Everitt, 2004). Finally, we manually analyzed and evaluated the resulting clusters and derived archetypes. We further elaborate on each archetype in the results section.

4 Results

4.1 ML-based Fraud Detection Systems Taxonomy

The final taxonomy contains ten dimensions, each with two to four different characteristics (see Figure 4). Our taxonomy fulfills quality criteria since each of the 54 FDS in our database can be described by exactly one characteristic per dimension (mutually exclusive, collectively exhaustive).

Dimension	Characteristic			
Class Balancing	Random Undersampling	Random Oversampling	Hybrid	None
Detection Tactic	Misuse Detection		Anomaly Detection	
Dimensionality Reduction	Feature Selection	Feature Extraction	None	
Economical Evaluation	Evaluation Integrated		No Evaluation Integrated	
Explainability	Results Explainable		Results Not Explainable	
Federated Learning	Federated Learning Used		Federated Learning Not Used	
ML-Algorithm Type	Supervised Learning	Semi-Supervised Learning	Unsupervised Learning	
Online Processing	Online Processing Implemented		Online Processing Not Implemented	
Preserved Privacy	Data Privacy Preserved		Data Privacy Not Preserved	
Sequential Modeling	Sequential Modeling Used		Sequential Modeling Not Used	

Figure 4: ML-based Fraud Detection Systems Taxonomy

Class Balancing

The dimension *Class Balancing* indicates whether the FDS implements some kind of class balancing methods such as *random undersampling* or *random oversampling*. Class imbalance is one of the main challenges of fraud detection since, especially in the context of machine learning, it makes the learning and evaluation of a classifier quite challenging (Chandola *et al.*, 2009; Murphy, 2012). Thus, researchers integrate class balancing techniques into their FDSs to increase detection performance (Herland *et al.*, 2017). For example, Matschak et al. (2021) applied syntenic random oversampling (SMOTE) to create new synthetic fraud cases for machine learning model training.

Detection Tactic

Currently, the tactics used for ML-based fraud detection can be classified into the two following categories *misuse detection* and *anomaly detection* (Mittal and Tyagi, 2020). While misuse detection is mainly focused on using supervised ML-learning for fraud analysis, *anomaly detection* deals with unsupervised ML-learning to detect abnormal user behavior and outliers (e.g., abnormal amounts of credit card payments).

Dimensionality Reduction

The dimension *Dimensionality Reduction* was added concerning some ML-based fraud detection systems that explicitly use dimensionality techniques like *feature selection* or *feature reduction* (also called feature projection) to reduce the dimensional complexity of extensive fraud detection problems. For example, Herland et al. (2017) use feature selection to limit the number of features fed forward to the detection method to the most meaningful ones.

Economic Evaluation

Generally, machine learning algorithms do not consider fraud detection's associated costs (Akgul, 2021b). Only a few ML-based fraud detection approaches that consider the costs of investigation detected fraud in their classification decision (e.g., Akgul (2021b)). We believe that including costs

enables organizations to decrease their fraud detection costs significantly and thus increases ML-based fraud detection practicality.

Explainability

Explainability indicates whether a fraud detection system, based on the used fraud detection technique, is able to provide information on the how and why of its decision-making. This enables users and regulatory entities to review and interpret fraud detection decisions to ensure compliance. Fraud detection problems specifically belong to the group of domains where the explanation in the classification decision is important. For example, supervised algorithms of the type of neural network are often considered 'black boxes' since they provide limited information regarding their internal training and decision making and, consequently, are less explainable than, e.g., rule-based decision trees.

Federated Learning

Regarding the characteristics of the fraud detection problem (see chapter **Error! Reference source not found.**), the amount of labeled (training-) data is limited. Furthermore, due to data security and privacy, different organizations are usually not allowed or willing to share their transaction datasets (Yang *et al.*, 2019). These problems make it difficult for FDSs to learn the patterns of fraud and to detect them (Yang *et al.*, 2019). Federated learning enables organizations to train ML models with data distributed on their own local database; thus, they can collectively reap the benefits of a shared (collectively trained) model without sharing the dataset itself and protecting sensitive information. Examples of ML-based FDSs implementing federated learning are provided by Wang et al. (2018) and Zheng et al. (2020).

ML Algorithm-Type

Since machine learning-based approaches and the existence of diverse machine learning algorithms have gained in popularity in recent years, we decided to further specify this detection type. While the boundaries between fraud detection and anomaly detection are blurred in the literature, three main research directions are emerging in the context of ML-based approaches. Consistent with relevant literature on machine learning algorithms (e.g., Travaille (2011)), we classify ML-algorithm types into unsupervised, supervised, and semi-supervised machine-learning. For example, Kirlidog and Asuk (2012) present a supervise fraud detection approach based on a Suppport-Vector-Machine. In addition, Debener (2021) uses the unsupervised Isolation-Forest for his study. A semi-supervised autoencoder was applied by Abakarim et al. (2018) for fraud detection.

Online Processing

Online Processing refers to the ability of an FDS to process and perform fraud detection *online* (data stream) or *offline* (batch-wise). The analyzed publications unveil that this characteristic can be primarily found in the financial sector (e.g., Patil et al. (2018), Abakarim et al. (2018), and Thennakoon et al. (2019)). But this technology is also used in the healthcare industry. For example, Rawte and Anuradha (2015) dealt with a fraud detection approach that can cope with streamed data using an evolving clustering approach. Streaming Analysis, Spark Streaming and Time Data Analytics are typical technologies for online processing (Mittal and Tyagi, 2020). This characteristic could be of value when dealing with time-critical detection tasks as they are imageable, for example, in the context of live validation of upcoming e-prescriptions in healthcare or credit card validation in e-commerce.

Preserved Privacy

The dimension *Preserved Privacy* refers to the ability of the detection method to *preserve privacy* of personal data. Since especially health and financial data are very worthy of protection, researchers highlight the need for privacy-preserving fraud detection approaches to meet regulations and gain practical acceptance of the technology (Bauder and Khoshgoftaar, 2017b; Chandola *et al.*, 2013; Zerka *et al.*, 2020). However, privacy-preserving fraud detection approaches in research and practice are rare.

Sequential Modeling

Besides considering data instances as snapshots, thus analyzing data without considering previous values, some ML-based FDSs use sequential modeling to investigate data for sequential patterns over time (Kirlidog and Asuk, 2012). In particular, these approaches build on sequential modeling to capture

the sequential patterns of each data instance and leverage, e.g., memory networks, to improve performance and interpretability (Yang and Xu, 2019).

4.2 ML-based Fraud Detection System Archetypes

Finally, we performed a cluster analysis to identify archetypes of ML-based FDSs. The results of the cluster analysis conducted can be seen in Figure 5. Due to the results of the applied method and associated ending conditions by Nickerson et al. (2013), the shown characteristics are mutually exclusive and collectively exhaustive. The color shade is supposed to support the interpretation of the results. The individual clusters describe the interrelationship of characteristics identified in the taxonomy development process. As a result, they represent archetypal ML-based FDSs. By giving an overview of characteristic combinations, these archetypes provide guidance toward design patterns of developed and evaluated ML-based FDSs.

Dimension	Characteristic	Archetype 0	Archetype 1	Archetype 2
Number of Fraud Detection Systems in Cluster		*20*	*23*	*11*
Class Balancing	Random Undersampling	0,00%	30,43%	0,00%
	Random Oversampling	15,00%	21,74%	0,00%
	Hybrid	10,00%	0,00%	0,00%
	None	75,00%	47,83%	100,00%
Detection Tactic	Misuse Detection	100,00%	100,00%	0,00%
	Anomaly Detection	0,00%	0,00%	100,00%
Dimensionality Reduction	Feature Selection	15,00%	4,35%	18,18%
	Feature Extraction	20,00%	8,70%	0,00%
	None	65,00%	86,96%	81,82%
Economical Evaluation	Evaluation Integrated	5,00%	0,00%	0,00%
	Evaluation Not Integrated	95,00%	100,00%	100,00%
Explainability	Results Explainable	0,00%	95,65%	81,82%
	Results Not Explainable	100,00%	4,35%	18,18%
Federated Learning	Federated Learning Used	10,00%	0,00%	0,00%
	Federated Learning Not Used	90,00%	100,00%	100,00%
ML-Algorithm Type	Supervised Learning	75,00%	82,61%	9,09%
	Semi-Supervised Learning	25,00%	8,70%	9,09%
	Unsupervised Learning	0,00%	8,70%	81,82%
Online Processing	Online Processing Implemented	25,00%	0,00%	0,00%
	Online Processing Not Implemented	75,00%	100,00%	100,00%
Preserved Privacy	Data Privacy Preserved	15,00%	0,00%	0,00%
	Data Privacy Not Preserved	85,00%	100,00%	100,00%
Sequential Modeling	Sequential Modeling Used	10,00%	4,35%	0,00%
	Sequential Modeling Not Used	90,00%	95,65%	100,00%

Figure 5: Cluster Analysis Results

We briefly describe each archetype and assign a representative label in the following.

The first archetype includes only ML-based FDSs dealing with m*isuse extraction* mainly based on supervised learning. Consequently, FDS of this archetype need labeled data with enough instances of identified fraud. In addition, it is noticeable that this archetype is technologically advanced overall, as much of the available functionality and components are applied here. However, the explainability of the decisions made by the system suffers from this complexity. Against this background, we name this archetype *Advanced Misuse Detection*.

In contrast, the second archetype is named *Simple Misuse Detection.* This archetype also focuses on misuse detection but uses a simpler setup of technologies (e.g., less dimensionality reduction and data security and privacy mechanisms). Although, the classification of FDSs of this archetype is, in general, more explainable. Analogous to FDS of the first archetype, FDS of the second archetype also require labeled data with a sufficient number of identified fraud instances to exploit their detection potential.

Finally, the third archetype is dominated by anomaly detection approaches based on unsupervised learning. Since the type of ML algorithm itself already limits a part of the possible technical possibilities, this archetype is also regarded as technologically simpler. However, unsupervised ML has advantages over supervised ML regarding detecting new fraud patterns and no need for labeled training data. Therefore, FDSs of the third archetype are particularly useful in areas where there is limited access to labeled data or where new types of fraud emerge very regularly. In addition, the FDSs of this archetype provide advanced explainability.

In summary, it should also be mentioned that the archetypes named here can be used alone or in combination with other FDS, e.g. to compensate for potential weaknesses of the other type.

5 Discussion

5.1 Contributions to Literature

The contributions of this study to the literature are manifold. As ML and its integration in FDSs is a relatively new discipline in IS research, the body of literature regarding ML-based fraud detection constantly increases, presenting scientists with the challenge of keeping track of relevant topics. Against this background, first, we were able to draw the diversity of FDSs setups by analyzing literature on ML-based FDSs. By doing so, we provided an overview of the state-of-the-art of FDS-designs and derived relevant FDS characteristics, which are subsequently used to develop a taxonomy of ML-based FDSs.

Second, for the first time, an ML-based FDSs taxonomy was developed that extends the existing, basic classification of ML-based FDSs (anomaly detection vs. misuse detection (Mittal and Tyagi, 2020)) by adding further dimensions. These dimensions describe FDSs in greater detail than the existing classifications.

Third, in addition to the classification of FDSs, these dimensions can be used in future design-oriented research on FDSs. Thus, in the context of design-oriented research, this study contributes to the growing knowledge base on FDS and can increase the comparability and transferability of research results. Moreover, by creating awareness towards FDSs characteristics, we mitigate the risk of research producing duplications, and thus, support research progress and help to avoid waste of resources.

Finally, we offer future researchers a guiding scope for investigating FDSs and providing them with plenty of opportunities for further exploration.

5.2 Contributions to Practice

In addition to the aforementioned contributions to literature, our study also provides contributions to practitioners. First, by highlighting potential characteristics, components, and combination, the developed taxonomy allows companies to explore potential ways of designing an FDS. Consequently, this enables them to design and tailor their own FDS based on their specific use case characteristics. This migh improve the design process ans accelerate the development of new effective FDS keeping up in the race between fraudsters and fraud detection.

Secondly, the structured set of characteristics and the derived archetypes enable practitioners to formulate specific requirements for internal developers or when engaging with a vendor. This could lead to improved evaluation and selection of FDS offered on the market.

Third, the identified FDS archetypes provide practitioners with a blueprint for FDS design, while the derived archetypes can be used as maturity scales. Thus, practitioners can analyze competitors' FDS or FDS available on the market and compare their own implementations against them. In general, each step towards less fraud means saving resources, thus supporting economic progress.

5.3 Limitations and Future Research Opportunities

Our paper also holds limitations that offer opportunities for future research. First, it cannot be guaranteed that all relevant literature and thus relevant FDS have been identified and, thus, are taken into account in the taxonomy development process. This limitation is based on either the selected databases or our applied search string.

Secondly, the taxonomy developed from existing FDS literature cannot be considered comprehensive in terms of explaining platforms in detail but can be helpful for understanding and classification.

Thirdly, as Nickerson et al. (2013) highlight that a taxonomy can never be perfect but can develop dynamically, there may be other relevant dimensions that should be integrated into the taxonomy in the future. Especially in an agile research domain such as FDS research, our taxonomy may be outdated one day. Therefore, we call on other scientists to build on our work to validate and expand it in future studies.

Fourthly, a methodological limitation arises when there are FDS that are not published. Since we use publicly accessible literature, the characteristics of these FDS might not be recognized by our developed taxonomy.

Future research should investigate further how different FDS characteristics influence their ability to detect fraud and abuse effectively and efficiently. Moreover, we were able to highlight FDS characteristics that may support the design of new FDS, though future research should deal with adoption enablers and success factors influencing the success of FDS implementations in the long run. Here, based on regulations, among other things, it is relevant to create new approaches to combine technological complexity and performance of fraud detection with explainability of the classification results. The same applies to ML robustness and information security and privacy because these topics are still given very little consideration in current FDS.

6 Conclusion

Fraud is a significant burden on the economy and society. Nevertheless, research on FDSs is limited, and, particularly, a structured classification method of ML-based FDSs is missing in previous research. To address this research gap, we analyzed 54 FDSs identified in the literature and used this database to develop a contextualized taxonomy for ML-based FDSs. This taxonomy can be used to classify ML-based FDS based on 10 dimensions in a structured way, thus extending the existing, basic classification of ML-based FDSs (RQ1). Moreover, we were also able to derive three archetypes that, in combination with identified characteristics, can serve as a guideline for future research (RQ2).

References

Abakarim, Y., Lahby, M. and Attioui, A. (2018), "An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning", *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications*, presented at the SITA'18: THEORIES AND APPLICATIONS, ACM, Rabat Morocco, pp. 1–7.

ACFE. (2020), *Report to the Nations*, No. 11, available at: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf.

Akgul, M. (2021a), "Fraud Detection System Adoption: Success Factors", *ECIS 2021 Research-in-Progress Papers*, presented at the European Conference on Information Systems (ECIS), p. 12.

Akgul, M. (2021b), "A Cost-Based Fraud Detection System for Financial Sector", *AMCIS 2021 Proceedings*, presented at the AMCIS 2021.

Alanezi, F. and Brooks, L. (2014), "Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT)", *AMCIS 2014 Proceedings*, presented at the Americas Conference on Information Systems (AMCIS), p. 13.

Baesens, B., Van Vlasselaer, V. and Verbeke, W. (2015), *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*, John Wiley & Sons.

Bauder, R., da Rosa, R. and Khoshgoftaar, T. (2018), "Identifying Medicare Provider Fraud with Unsupervised Machine Learning", *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, presented at the 2018 IEEE International Conference on Information Reuse and Integration for Data Science (IRI), IEEE, Salt Lake City, UT, pp. 285–292.

Bauder, R.A. and Khoshgoftaar, T.M. (2017b), "Medicare Fraud Detection Using Machine Learning Methods", *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, presented at the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, Cancun, Mexico, pp. 858–865.

Bauder, R.A., Khoshgoftaar, T.M., Richter, A. and Herland, M. (2016), "Predicting Medical Provider Specialties to Detect Anomalous Insurance Claims", *2016 IEEE 28th International Conference on Tools with Artificial Intelligence (ICTAI)*, presented at the 2016 IEEE 28th International Conference on Tools with Artificial Intelligence (ICTAI), IEEE, San Jose, CA, USA, pp. 784–790.

Bellini, F. (2014), "BIG DATA ANALYTICS FOR FINANCIAL FRAUDS DETECTION", *Proceedings of the 8th Mediterranean Conference on Information Systems*, presented at the Mediterranean Conference on Information Systems (MCIS), p. 11.

Bhattacharya, I. and Lindgreen, E.R. (2020), "A SEMI-SUPERVISED MACHINE LEARNING APPROACH TO DETECT ANOMALIES IN BIG ACCOUNTING DATA", *Proceedings of the 28th European Conference on Information Systems (ECIS)*, presented at the European Conference on Information Systems (ECIS), An Online AIS Conference, p. 15.

Chandola, V., Banerjee, A. and Kumar, V. (2009), "Anomaly detection: A survey", *ACM Computing Surveys*, Vol. 41 No. 3, pp. 1–58.

Chandola, V., Sukumar, S.R. and Schryver, J.C. (2013), "Knowledge discovery from massive healthcare claims data", *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, presented at the KDD' 13: The 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, Chicago Illinois USA, pp. 1312–1320.

Cressey, D.R. (1953), *Other People's Money; a Study of the Social Psychology of Embezzlement.*, Free Press.

Dal Pozzolo, A., Caelen, O. and Bontempi, G. (2015), "When is Undersampling Effective in Unbalanced Classification Tasks?", in Appice, A., Rodrigues, P.P., Santos Costa, V., Soares, C., Gama, J. and Jorge, A. (Eds.), *Machine Learning and Knowledge Discovery in Databases*, Vol. 9284, Springer International Publishing, Cham, pp. 200–215.

Debener, J., Heinke, V. and Kriebel, J. (2021), "Insurance Fraud and Isolation Forests", *ICIS 2021 Proceedings*, presented at the ICIS 2021, p. 10.

Derring, R.A. (2002), "Insurance Fraud", *Ournal of Risk and Insurance*, Vol. 69 No. 3, pp. 271–287.

Dieleman, J.L., Templin, T., Sadat, N., Reidy, P., Chapin, A., Foreman, K., Haakenstad, A., *et al.* (2016), "National spending on health by source for 184 countries between 2013 and 2040", *The Lancet*, Vol. 387 No. 10037, pp. 2521–2535.

Dionne, G., Giuliano, F. and Picard, P. (2009), "Optimal Auditing with Scoring: Theory and Application to Insurance Fraud", *Management Science*, Vol. 55 No. 1, pp. 58–70.

Dora, P. and Sekharan, D.G.H. (2015), "Healthcare Insurance Fraud Detection Leveraging Big Data Analytics", *IJSR*, Vol. 4 No. 4, pp. 2073–2076.

Eickhoff, M., Muntermann, J. and Weinrich, T. (2017), "What do FinTechs actually do? A Taxonomy of FinTech Business Models", *Proceedings of the Thirty Eighth International Conference on Information Systems*, presented at the International Conference on Information Systems, South Korea, p. 20.

"Fraud Act 2006". (2006), available at: https://www.legislation.gov.uk/ukpga/2006/35/contents (accessed 13 October 2021).

Herland, M., Bauder, R.A. and Khoshgoftaar, T.M. (2017), "Medical Provider Specialty Predictions for the Detection of Anomalous Medicare Insurance Claims", *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, presented at the 2017 IEEE International Conference on Information Reuse and Integration (IRI), IEEE, San Diego, CA, pp. 579–588.

Jhangiani, R., Bein, D. and Verma, A. (2019), "Machine Learning Pipeline for Fraud Detection and Prevention in E-Commerce Transactions", presented at the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0135–0140.

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L. and Caelen, O. (2018), "Sequence classification for credit-card fraud detection", *Expert Systems with Applications*, Vol. 100, pp. 234–245.

Kaufman, L. and Rousseeuw, P.J. (2009), *Finding Groups in Data: An Introduction to Cluster Analysis*, Vol. 344, John Wiley & Sons.

Kirlidog, M. and Asuk, C. (2012), "A Fraud Detection Approach with Data Mining in Health Insurance", *Procedia - Social and Behavioral Sciences*, Vol. 62, pp. 989–994.

Landau, S. and Everitt, B. (2004), *A Handbook of Statistical Analyses Using SPSS*, Chapman & Hall/CRC, Boca Raton.

Lek, M., Anandarajah, B., Cerpa, N. and Jamieson, R. (2001), "Data Mining Prototype for Detecting E-Commerce Fraud", *ECIS 2001 Proceedings*, presented at the European Conference on Information Systems (ECIS), p. 6.

Matschak, T., Prinz, C., Masuch, C. and Trang, S. (2021), "Healthcare in Fraudster's Crosshairs: Designing, Implementing and Evaluating a Machine Learning Approach for Anomaly Detection on Medical Prescription Claim Data", presented at the Twenty-fifth Pacific Asia Conference on Information Systems, Dubai, UAE, pp. 1–14.

Minastireanu, E.-A. and Mesnita, G. (2019), "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection", *Informatica Economica*, Vol. 23 No. 1/2019, pp. 5–16.

Mittal, S. and Tyagi, S. (2020), "Computational Techniques for Real-Time Credit Card Fraud Detection", in Gupta, B.B., Perez, G.M., Agrawal, D.P. and Gupta, D. (Eds.), *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Springer International Publishing, Cham, available at:https://doi.org/10.1007/978-3-030-22277-2.

Murphy, K.P. (2012), *Machine Learning: A Probabilistic Perspective*, MIT Press, Cambridge, MA.

Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y. and Sun, X. (2011), "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature", *Decision Support Systems*, Vol. 50 No. 3, pp. 559–569.

Nickerson, R.C., Varshney, U. and Muntermann, J. (2013), "A method for taxonomy development and its application in information systems", *European Journal of Information Systems*, Vol. 22 No. 3, pp. 336–359.

Omar, S.J., Fred, K. and Swaib, K.K. (2018), "A state-of-the-art review of machine learning techniques for fraud detection research", *Proceedings of the 2018 International Conference on Software*

Engineering in Africa - SEiA '18, presented at the the 2018 International Conference, ACM Press, Gothenburg, Sweden, pp. 11–19.

Paruchuri, H. (2017), "Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review", *ABC Journal of Advanced Research*, Vol. 6 No. 2, pp. 113–120.

Patil, S., Nemade, V. and Soni, P.K. (2018), "Predictive Modelling For Credit Card Fraud Detection Using Data Analytics", *Procedia Computer Science*, Vol. 132, pp. 385–395.

Pourhabibi, T., Ong, K.-L., Kam, B.H. and Boo, Y.L. (2020), "Fraud detection: A systematic literature review of graph-based anomaly detection approaches", *Decision Support Systems*, Vol. 133, p. 113303.

Power, D.J. and Power, M.L. (2015), "Sharing and Analyzing Data to Reduce Insurance Fraud", *Proceedings of the Tenth Midwest Association for Information Systems Conference*, Pittsburg, Kansas, pp. 1–6.

Punj, G. and Stewart, D.W. (1983), "Cluster Analysis in Marketing Research: Review and Suggestions for Application", *Journal of Marketing Research*, Vol. 20 No. 2, pp. 134–148.

PwC. (2020), *PwC's Global Economic Crime and Fraud Survey*, available at: https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf.

Rau, D., Perlitt, L.-H., Röglinger, M. and Wenninger, A. (2020), "Pushing the Frontiers of Service Research – A Taxonomy of Proactive Services", *ICIS 2020 Proceedings*, presented at the International Conference on Information Systems (ICIS), p. 18.

Rawte, V. and Anuradha, G. (2015), "Fraud detection in health insurance using data mining techniques", *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, presented at the 2015 International Conference on Communication, Information & Computing Technology (ICCICT), IEEE, Mumbai, India, pp. 1–5.

Remane, G., Nickerson, R.C., Hanelt, A., Tesch, J.F. and Kolbe, L.M. (2016), "A Taxonomy of Carsharing Business Models", *Proceedings of the Thirty Seventh International Conference on Information Systems*, presented at the International Conference on Information Systems, Dublin, p. 20.

Samakovitis, G. and Kapetanakis, S. (2013), "Computer-aided Financial Fraud Detection: Promise and Applicability in Monitoring Financial Transaction Fraud", *Proceedings of the 2013 International Conference on Business Management & Information Systems*, presented at the International Conference on Business Management & Information Systems, pp. 135–144.

Sharma, S., Ku, C.-Y. and Chuang, Y.-T. (2016), "AN APPROACH TO RISK MANAGEMENT FOR E-COMMERCE", *PACIS 2016 Proceedings*, presented at the Pacific Asia Conference on Information Systems (PACIS), p. 9.

Sun, C., Li, Q., Li, H., Shi, Y., Zhang, S. and Guo, W. (2019), "Patient Cluster Divergence Based Healthcare Insurance Fraudster Detection", *IEEE Access*, Vol. 7, pp. 14162–14170.

Tan, C.-W., Benbasat, I. and Cenfetelli, R.T. (2016), "An Exploratory Study of the Formation and Impact of Electronic Service Failures", *MIS Quarterly*, Vol. 40 No. 1, pp. 1–29.

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. and Kuruwitaarachchi, N. (2019), "Real-time Credit Card Fraud Detection Using Machine Learning", *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, presented at the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, Noida, India, pp. 488–493.

Thornton, D., Brinkhuis, M., Amrit, C. and Aly, R. (2015), "Categorizing and Describing the Types of Fraud in Healthcare", *Procedia Computer Science*, Vol. 64, pp. 713–720.

Travaille, P. (2011), "Electronic Fraud Detection in the U.S. Medicaid Healthcare Program: Lessons Learned from other Industries", *AMCIS 2011 Proceedings - All Submissions*, presented at the AMCIS 2011, p. 11.

Vaisu, L., Warren, M. and Mackay, D. (2003), "Defining Fraud: Issues for Organizations from an Information Systems Perspective", *PACIS 2003 Proceedings*, presented at the Pacific Asia Conference on Information Systems (PACIS), p. 10.

Viaene, S., Ayuso, M., Guillen, M., Van Gheel, D. and Dedene, G. (2007), "Strategies for detecting fraudulent claims in the automobile insurance industry", *European Journal of Operational Research*, Vol. 176 No. 1, pp. 565–583.

Waghade, S.S. and Karandikar, A.M. (2018), "A Comprehensive Study of Healthcare Fraud Detection based on Machine Learning", Vol. 13 No. 6, p. 4.

Wang, Y., Adams, S., Beling, P., Greenspan, S., Rajagopalan, S., Velez-Rojas, M., Mankovski, S., *et al.* (2018), "Privacy Preserving Distributed Deep Learning and Its Application in Credit Card Fraud Detection", *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, New York, NY, USA, pp. 1070–1078.

Wardlaw, G. (1999), "The future and crime: challenges for law enforcement", *3rd National Outlook Symposium on Crime in Australia*, Canberra.

Webster, J. and Watson, R.T. (2002), "Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly*, pp. xii–xxiii.

Yang, K. and Xu, W. (2019), "FraudMemory: Explainable Memory-Enhanced Sequential Neural Networks for Financial Fraud Detection", presented at the Hawaii International Conference on System Sciences, available at:https://doi.org/10.24251/HICSS.2019.126.

Yang, W., Zhang, Y., Ye, K., Li, L. and Xu, C. (2019), "FFD: A Federated Learning Based Method for Credit Card Fraud Detection.", in Chen, K., Seshadri, S. and Zhang, L. (Eds.), *Big Data – BigData 2019. BIGDATA 2019. Lecture Notes in Computer Science*, Vol. 11514, Springer, Cham.

Yuan, C. and Yang, H. (2019), "Research on K-Value Selection Method of K-Means Clustering Algorithm", *Multidisciplinary Scientific Journal*, Vol. 2 No. 2, pp. 226–235.

Zerka, F., Barakat, S., Walsh, S., Bogowicz, M., Leijenaar, R.T.H., Jochems, A., Miraglio, B., *et al.* (2020), "Systematic Review of Privacy-Preserving Distributed Machine Learning From Federated Databases in Health Care", *JCO Clinical Cancer Informatics*, No. 4, pp. 184–200.

Zheng, L., Chen, C., Liu, Y., Wu, B., Wu, X., Wang, L., Wang, L., *et al.* (2020), "Industrial Scale Privacy Preserving Deep Neural Network", *ArXiv:2003.05198 [Cs, Stat]*, available at: http://arxiv.org/abs/2003.05198 (accessed 17 November 2021).