A Study of Fraud Types, Challenges and Detection Approaches in Telecommunication

Kasra Babaei
Faculty of Science and Engineering, University of Nottingham Malaysia
Khyx6kbb@nottingham.edu.my
ZhiYuan Chen *
Faculty of Science and Engineering, University of Nottingham Malaysia
zhiyuan.chen@nottingham.edu.my
Tomas Maul
Faculty of Science and Engineering, University of Nottingham Malaysia
tomas.maul@nottingham.edu.my

Received: 13/Nov/2019 Revised: 02/May/2020 Accepted: 26/May/2020

Abstract

Fraudulent activities have been rising globally resulting companies losing billions of dollars that can cause severe financial damages. Various approaches have been proposed by researchers in different applications. Studying these approaches can help us obtain a better understanding of the problem. The aim of this paper is to investigate different aspects of fraud prevention and detection in telecommunication. This study presents a review of different fraud categories in telecommunication, the challenges that hinder the detection process, and some proposed solutions to overcome them. Also, the performance of some of the state-of-the-art approaches is reported followed by our guideline and recommendation in choosing the best metrics.

Keywords: Fraud Detection; Machine Learning, Telecommunication

1- Introduction

Telecommunications companies have long been suffering from fraudulent. In addition to the financial losses caused by fraudulent activities, companies that are incapable of foiling these activities will lose their customers as well. However, by developing adaptive and automatic systems it is possible to hinder fraud.

Telecommunication fraud is eventuating a tremendous financial loss for companies annually. Hardly possible to calculate and state the financial loss caused by fraudulent activities in the telecommunications industry, because some companies prefer not to reveal to protect their reputation. In addition, not all frauds are detected by telecommunication companies and the efficiency of their detection systems is not clear. Nonetheless, based on some analyses, it was concluded that telecommunication fraud caused 46.3 billion USD in 2013 globally, which was about 2 percent of the worldwide telecom revenues [1]. Also, according to [2], telecommunication companies lose around 7% of their revenue due to fraudulent activities. This financial loss can produce pernicious effects on companies' revenues [3]. It is worth to note that even though wireless communication has become more predominant, telecommunication companies are still suffering, particularly in developing countries such as China [4]. As listed in Table 1, companies all over the world lose a considerable amount of their revenue due to fraudulent activities [2].

In this paper, the aim is to provide a thorough overview of different fraud related systems, namely fraud detection systems and fraud prevention systems, followed by the techniques and challenges that cause problems to these systems. As depicted in Figure 5**,**the paper tries to keep the focus on research works that were published during the past decade but also covers some of the earlier works that we find relevant. Also, an extensive review of different evaluation metrics used for performance measurement is carried out to understand the most employed and appropriate metrics in telecommunication fraud.

Table 1 Revenue loss in 2015 [2]

Fraud type		Fraud loss in B. of dollars		
		Globally	Western Europe	North America
Fraud type	International Revenue Share Fraud (IRSF)	10,75	2,07	3,21
	Interconnect Bypass Frau	5,97	1,15	1,78
	Premium Rate Service Frau	3,74	0,72	1,12
Fraud methods	Subscription Frau	8,05	2,4	1,55
	PBX Hacking IP PBX Hacking	7,47	2,22	1,44
	Wangiri Fraud	1,77	0,53	0,34
	Phishing	1,57	0,47	0,3
	Abuse of Service Terms and Condition	1,17	0,53	0,34
	SMS Faking or Spoofing	0,79	0,23	0,15

* Corresponding Author

2- Related Works

Fraud detection is very important for companies to thwart fraudsters from causing financial loss, reputational damage, and invading their customers' private information. Various surveys have reviewed electronic fraud (also known as e-fraud), which is any sort of illegal action committed by using electronic technology and equipment such as computers. Some of the main categories of fraud that have been covered include credit card fraud, money laundering, insurance fraud, financial statement fraud, and mortgage fraud [5]–[7].

Financial fraud includes a vast area and researchers have reviewed and categorised them differently, which is important to be studied. Recent research in financial fraud such as [6] investigated methods and approaches in various areas including telecommunications fraud, credit card fraud, and insurance fraud. In [8], the authors reviewed four other types of financial fraud, namely computer intrusion, money laundry, telecommunications fraud, and credit card fraud. Four different types of fraud in telecommunications were defined by [8] (i.e. superimposed or surfing fraud, subscription fraud, ghosting fraud, and insider fraud), and they also investigated some major issues and challenges as well as tools that were used to detect them.

Another review was conducted by [9] in which the authors looked into three fraud areas, namely credit card fraud, computer intrusion, and telecommunications fraud. In telecom fraud, fraud attacks were categorised into superimposed fraud and subscription fraud. Each category includes some subcategories as well, such as phone cloning and ghosting that are under the superimposed fraud category. The review emphasised on three major approaches to detect telecom fraud (i.e. rule-based, neural networks, and visualisation).

Another comprehensive survey was conducted by [10] in which data-mining methods used in fraud detection within a 10 year period (i.e. from 2000 to 2010) were reviewed. The review was more focused on the data-mining methods used, including semi-supervised and also one-class classification methods in which the model is trained with only one class, which is often the non-fraudulent class.

A recent and comprehensive review was done in [6] that covered five different areas of fraud (i.e. telecommunications, health insurance, credit card, and online auction) and investigated four major challenges along with the efforts made to overcome them in each area. Issues and challenges in fraud detection regardless of the area were likewise studied in [5].

Fraud systems are very important in providing secure and reliable services and eliminating financial losses incurred by fraudsters. Studying different approaches proposed in the literature can provide useful insights related to the problems and challenges in this area, which can lead to identifying the gaps for further investigation. Also, such research works embody a pool of ideas that can be refined, extended, and combined, in order to further improve current performance levels in this area.

3- Fraud

This section presents a comprehensive definition of fraud in general and also in the specific context of telecommunication. It also reviews the different motivations that push people to commit fraudulent activities in this area.

There are numerous definitions of fraud. The Cambridge Advanced Learner’s Dictionary defines fraud as "the crime of getting money by deceiving people", and the Merriam-Webster Dictionary defines it as "the crime of using dishonest methods to take something valuable from another person". In other words, any deliberate action with the purpose of making unfair or unlawful gain is known as fraud [1]. In telecommunications, fraud refers to the misuse of services provided by telecom companies, including voice or data, without gaining permission and without the intention of paying [11]–[13]. Fraud detection refers to the efforts made to spot and catch undesirable behaviours relating to this misuse [14]. These undesirable behaviours include delinquency, intrusion, and account defaulting [9].

It is important to understand the motivation behind fraudulent activities. One main motivation is to use services with no intent to pay for them (self-usage), where another is based on financial gain obtained from reselling premium services to customers for a lower price [15]. In [8], the motives for fraudulent activities were categorised into two groups based on revenue, namely revenue fraud and non-revenue fraud, where in the former the fraudster tries to earn money and in the latter the purpose is only to gain free services. Furthermore, fraudsters can make untraceable communications and hide their identity [16], which is very useful for criminals and terrorists who want to stay hidden to perpetrate their vicious plans. The opacity of communication is partly due to the complex topology and massive size of networks that make it extremely difficult, time consuming, and costly to identify and find the location of the fraudsters [17].

3-1- Fraud Types

There are several forms of telecommunication fraud and previous works have categorised them differently; however, almost all of them have categorised fraud in telecommunications based on the methods used by fraudsters to gain unauthorised access [14]. A very broad categorisation was made by [18] that divided fraud into subscription fraud and superimposed fraud. In subscription fraud, fraudsters possess an account whose services they do not intend to pay for (high debt fraud is also under this category). The account is completely genuine, and fraud happens when it is active. Another fraud case in subscription fraud is registering with a false identity. It is worth noting that there are two types of users, namely domestic and commercial, where in the latter case, the cost is at a higher rate because the usage of commercial users is at a higher level [19]. A very common subscription fraud happens when a commercial user registers with a false identity as a domestic user to reduce the cost of communication. In [20] the authors divided subscription fraud into two subcategories based on intention: (a) for making profit, and (b) for personal usage. Detecting subscription fraud is, arguably, the most challenging kind of fraud in telecommunication, and this type can cause a huge revenue loss for companies [21]. Superimposed fraud happens when fraudsters take control of an account, which in fact belongs to a legitimate customer. Scrutinising calling records on the bill is a very common method for detecting superimposed fraud [22], [23]. Also, [9] used the same approach and classified fraud into superimposed fraud and subscription fraud. The authors further subcategorised superimposed fraud into other types such as phone cloning, ghosting, insider, and tumbling, while insolvent cases were considered a subcategory of subscription fraud. Another classification was proposed by [18] in which fraud types were categorised based on their source and nature, into internal fraud and external fraud. In external fraud, fraudsters' identities are hidden due to the nature of the source, which is from outside of the organisation, often with no geographical limitation. In contrast, the source of an internal attack is from within the organisation, which makes the investigation process easier. Some common examples of internal fraud are [18]:

- **Ghosting:** using technical means to get a cheap or free rate.
- **Sensitive Information Disclosure:** selling important and sensitive information to external entities.
- **Secret Commissions:** Secret profits (e.g. vouchers) are traded for obtaining goods or services.

On the other hand, common examples of external fraud are [18]:

- **Surfing:** obtaining another customer's service without their authorisation, for instance, by cloning SIM cards, or manipulation of Private Branch Exchange (PBX).
- **Premium Rate Fraud (PRS):** fraudsters inflate the revenue payable to a provider by sending traffic to a PRS line [24].
- **Roaming Fraud:** a fraudulent subscriber uses the long delay of transferring Call Detail Records (CDR) between the visiting network and the home network to refuse payment.

As illustrated in Figure 1 and explained in [15], fraud types can be divided into three main categories known as the 3M's classification, namely motive, means, and methods. The motive includes non-revenue fraud and revenue fraud (refer to Section 3 for detail), and the means are the nature or form of the fraud which satisfy the motive, where some examples are:

- **Call Selling:** selling high rate calls, often international calls, below the real price.
- **Sensitive Information Disclosure:** an internal fraud in which the fraudster sells important information such as access codes.
- **Content Selling:** obtaining content such as games and ringtones for free by exploiting the payment system.

Referring to generic methods to perpetrate fraud, the authors in [15] defined four main methods:

- **Subscription Fraud:** obtaining an account with true or false credentials with no intent to pay for it.
- **Technical Fraud:** exploiting vulnerabilities in the network for financial benefits.
- **Internal Fraud:** committing fraud from inside the organisation.
- **Point of Sale:** fabricating sale documents to increase the compensations which should be paid by the telecommunications company.

Another fraud classification was made by [25] where fraud was divided into four groups:

- **Contractual Fraud:** obtaining a service with no intention of paying. An example of this type is subscription fraud and premium rate fraud.
- **Hacking Fraud:** misusing system vulnerabilities to make revenue by exploiting or selling functionalities. Network attack and Private Automatic Branch Exchange (PABX) fraud are two examples of hacking fraud.
- **Technical Fraud:** exploiting the technical vulnerabilities of the network to perpetrate fraud. Detecting the vulnerabilities often requires technical knowledge, however, once discovered, non-technical fraudsters can also utilise it to their benefit. Cloning and technical internal fraud are examples of this type.
- **Procedural Fraud:** where a fraudster tries to attack the implemented procedure, normally business procedures, whose goal is to minimise exposure to fraud. Often, the purpose of procedural fraud is to grant access to the system. Examples of this type are roaming fraud and voucher ID duplication.

Another fraud classification was given in [14]. Telecommunication fraud was classified into two main groups based on transmission medium, namely traditional networks and Voice over Internet Protocol (VoIP). In traditional networks, fraud can be subcategorised into further types such as subscription fraud, SIM cloning, Premium Rate Service (PRS), dealer fraud, roaming fraud, calling card fraud, and internal fraud. In VoIP, fraud is committed by employing VoIP techniques, and some examples of this category are Arbitrage fraud, call transfer fraud, location route number, and bypass fraud. Other types of attacking methods in VoIP are Man in the middle Attack, Replay Attack, Teardown Attacks, Flooding Attacks and SPIT (Spam over IP Telephony) [26].

With the growth of smartphones and broadband Internet, users prefer to use VoIP to make their calls or send their messages to reduce cost. Consequently, new types of fraudulent activities have also emerged such as registration hijacking, spam, and message tampering [27]. Currently, smartphone advertising is used in many mobile applications, which has attracted fraudsters who use computer bots to generate abundant click events on advertisements thus earning money from them [28].

Arguably, there is no single perfect classification framework for fraud, and scholars have come up with various categories such as in [29] and [30] often dividing fraud into similar groups in which superimposed fraud and subscription fraud are the two dominant types [11].

Table 2 shows a summary of fraud detection systems since 2011, based on the type of fraud that the reported systems were designed to deal with. As depicted in **Error! Reference source not found.** and

Table 2, subscription fraud, targeted by almost half of the research papers published since 2011, was the most studied type of fraud, followed by SIM box fraud. It is worth mentioning that there are only a scant number of papers targeting a specific type of telecommunication fraud while in some research works such as [31], [32] and [33] the authors have tried to detect any type of telecommunication fraud instead of identifying merely a specific type.

4- Fraud Systems

In this section, different fraud management systems are reviewed, followed by methods commonly used in each system. The increase of fraudulent activities in the telecommunications industry and the financial losses incurred by this lucrative crime have compelled companies to look for automatic and intelligent systems that can foil fraud. These systems generally fall into two main categories which are prevention systems and detection systems. The following subsections will explain the differences between the aforementioned systems.

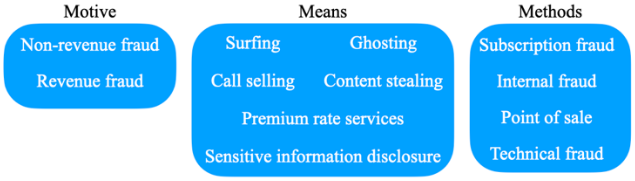

Figure 1 3M's fraud classification proposed by [15]

4-1- Fraud Prevention Systems

The idea behind fraud prevention systems (FPSs) is to block or prevent any fraudulent activity from occurring [8], [34]. Fraud prevention systems are the first barrier in controlling and confronting fraudulent activities. There are various mechanisms for this purpose such as using a firewall, encryption, or other forms of procedures such as Personal Identification Number (PIN) or Subscriber Identity Module (SIM) used in Private Branch Exchange (PBX) [34], and analysing applications and identifying potential customers before providing any service [20]. The problem with these kinds of systems is that they are not infallible, their performance is usually questionable, and perpetrators can usually adapt and change their methods to overcome the prevention mechanisms [18]. Besides the low effectiveness of these systems, FPSs are usually intrusive from the users' perspective [8]. For example, assigning a security code is a typical approach for protecting SIM card users [16], however, users often forget the code as it is rarely used, and repeatedly re-entering incorrect codes can result in SIM lock.

4-2- Fraud Detection Systems

Fraud detection systems (FDSs) are the next defensive system where it is assumed fraudsters have managed to bypass the FPS, or in other words, fraud has already occurred. An optimum detection system should be capable of identifying and reporting fraud activities at the time of their occurrence (also known as real-time detection). Fraud detection systems can help system managers to overcome the limitations of prevention systems by continuous monitoring. As depicted in Figure 2 and according to [33], the mechanisms used by FDSs can be divided into three main categories that are rule-based systems, visualisation systems, and user-profiling systems. Authors in [35] categorised detection systems into statistical and probabilistic, or machine learning and rule-based.

It is also worth mentioning that a data mining process can be categorised into offline and online modes [36]. In the offline mode, relevant data has been already been collected and stored, and models are trained to be used later for predicting the outcome of unseen data. In fraud detection, data usually comes in the form of streams that require an online mode of data mining [37]. The focus of this survey is on online fraud detection systems. This is due to the potential and flexibility of these systems (i.e. they can automatically adapt to new types of fraud). Besides, with an online system it is possible to take actions such as terminating the call while the call is still in progress, but with an offline system, detection is generally not possible until the user terminates the call [38]. These characteristics have made online systems more attractive to both researchers and the industry. The following subsections provide an overview of the various detection techniques used in FDSs. The techniques are categorised into the following methods: 1) rule-based systems; 2) visualisation systems; and 3) user-profiling.

In rule-based systems, a set of rules are defined by a field expert, and an alarm is triggered when a certain criterion is met. Although these systems are straightforward, effective and efficient, they come with some deficiencies which are [39], [40]:

- Vulnerability to unknown fraud attacks.
- Rules should be programmed precisely for every possible fraud.
- A field expert and prior knowledge is needed for setting new rules.

- Setting new rules is not immune to human error.
- Defining new rules is time consuming and often complicated.

As mentioned above, a big disadvantage of rule-based systems is that adversaries can adapt and change their attacking methods to avoid triggering an alarm, which makes rule-based approaches ineffective against new attacking patterns. In [41], a rule-based expert system for detecting superimposed fraud was proposed to evaluate a user's account upon the user's request.

Another technique used by FDSs is visualisation in which human visual pattern recognition is required to identify any sudden changes in the patterns of subscribers' activities such as a location change or a dramatic increase in usage [42], [43]. After an initial anomaly detection, further investigation of the visualised data is still required to detect fraud. A disadvantage of this technique is that it is not a fully automated technique and relies on a human field expert to scrutinise and pick out suspicious cases for further investigation.

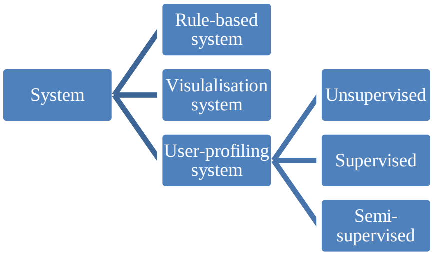

Figure 2 Classification of methods used in fraud detection systems [33]

The basic idea behind user-profiling consists of accumulating user characteristics to build a profile (also known as 'user dictionary') that represents the user's behaviour [34]. This profile that shows the user's behaviour in the past is then used to compare with the recent activities to determine significant changes, which are often signs of fraud. The data used by the system to describe a user's behaviour is usually derived from call detail records (CDRs) that contain information such as call duration, call location, time of the call, the destination and call cost [18]. Recently, user-profiling has attracted a lot of attention because of its effectiveness in automatic fraud detection and learning new fraud patterns [33]. User-profiles are constructed using data mining methods. Previous works have used various statistical methods based on the availability of labelled data, which can be mainly divided into supervised and unsupervised learning approaches [40]:

In supervised learning, a portion of the dataset, which is labelled as "fraudulent" or "non-fraudulent", is used as a training set. There are two main types of supervised learning models: classification and regression. In a classification model, the outcomes are discrete, and the model tries to map unseen instances into defined classes. Alternatively, when the outcomes are continuous, regression models are used, where the aim is to predict continuous values. Supervised learning requires a labelled training set which is known as a limitation, given the cost (temporal and financial) of generating labels. Without a labelled dataset, it is not possible to train the model. Moreover, and as a result of the above mentioned cost of labelling, training sets are often not large enough to effectively train the model [44]. Common supervised learning methods consist of support vector machines (SVMs), artificial neural networks (ANNs), decision trees, naïve bayes, and *k*-nearest neighbours (KNNs). The authors of [45] tried to accumulate characteristics of a user based on weekly activities and then detected fraudulent accounts using feed-forward neural networks (FF-NNs).

Table 2 Fraud Type & Reference & Description

Fraud type	Refence	Description
Superimposed fraud	[22], [23], [46]	Taking control of a legitimate account and making unauthorised calls
Subscription fraud	[1], [19], [30], [47]	Obtain a genuine account with no intention to pay for its services
Toll fraud	[39]	Make costly long-distance calls without authorisation that will be paid by subscribers
SIM box fraud	[11], [14], [35]	Channel national and international calls away from mobile operators and deliver them as local calls

Unlike supervised learning, unsupervised learning does not require labelled training data. This represents a significant cost saving, which in turn avoids the insufficient training data problem mentioned in the previous point [33]. It is usually a better approach when the majority of the dataset is negative for fraud; however, it can also produce a high false alarm rate if this assumption is not met [48]. Some common unsupervised learning algorithms consist of hierarchical clustering, self-organising maps (SOMs), and gaussian mixture models (GMMs). Generally, supervised learning algorithms can achieve higher detection rates and lower false positive rates while in unsupervised learning it is possible to detect unseen attacks [49]. The authors in [50] tried two different clustering methods to detect fraud based on weekly accumulated characteristics of users. Another unsupervised approach was conducted by [51] in which they used expectation maximisation for tuning a hierarchical regime-switch model for call-based detection.

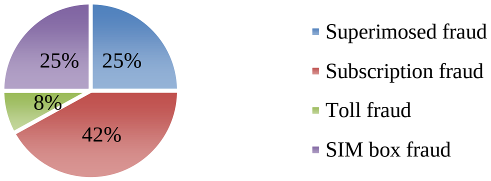

Figure 3 Types of Telecommunication Fraud Investigated Since 2011

There is also another method known as semi-supervised learning that lies between supervised learning and unsupervised learning. Semi-supervised learning is used under various circumstances such as paucity of training data or lack of certainty about all instances' labels [30]. This method uses both labelled data and unlabelled data for the learning process [52], which makes the method very suitable for fraud detection where the number of positive instances in the dataset is very small [53]. Table 3 presents a summary of various approaches and techniques used for telecommunication fraud detection in the literature since 2011. We believe these recent works that we studied are more influential and can represent various learning methods.

As Table 3 illustrates, recently, there has been an upward trend in unsupervised learning methods in this area. A recent unsupervised learning approach was reported in [39] to overcome the limitations of rule-based systems in which Local Outlier Factor (LOF) was utilised on real call data to detect toll fraud attacks, and prevent VoIP fraud. Another user-profiling approach using unsupervised methods was used in [33] that tried to use Latent Dirichlet Allocation (LDA) and a straightforward threshold-type classifier with automatic threshold setting. They also used three different approximation methods to calculate the Kullback Leibler divergence (KL-divergence) between two layers of LDA, ultimately finding the most effective method. In an earlier work, they introduced four different approximation methods to compute the KL-divergence between two LDAs, and unlike other similar work their approach aimed to detect the whole fraudulent accounts instead of merely one single fraudulent call [54].

Another extensive research was conducted by [30] in which a semi-supervised approach was applied to the dataset to detect subscription fraud in telecommunications. The authors proposed a framework consisting of 3 phases: preprocessing, clustering, and classification. After data cleaning, transformation, and dimensionality reduction in the preprocessing phase, SOM and *k*-means techniques were employed for clustering the data. In the classification phase, three different classifiers including Decision Trees (DTs), SVMs, and Neural Networks (NNs) were utilised to label the accounts into fraudulent and non-fraudulent. An ensemble of the three aforementioned classifiers was also built and compared to the original classifier results, with the ensemble showing superior performance.

Recently, deep learning techniques have also been employed. After their success in other fields such as image processing, authors in [55] proposed an approach based on a deep learning architecture. In particular they employed Deep Convolutional Neural Networks (DCNN), to separate normal behaviours from fraudulent ones.

Table 3 Telecommunication Detection Techniques Used Since 2011

Strategy	Learning Method	Reference	Detailed Description
Knowledge-based	Rule-based	[47], [58]–[60]	Triggering an alarm based on pre-defined rules
Supervised	SVM & ANN	[35]	Comparing the performances of SVMs and ANNs
	ANN	[11]	Applied a supervised learning method using multilayer perceptron (MLP)
	One-Class SVM	[22]	Applying Quarter-Sphere SVM which is a formulation of One-Class SVM
	Naïve-Bayesian	[19]	Used Naïve-Bayesian classification to calculate the probability and KL-divergence to detect subscription fraud
	Fuzzy logic	[14]	Used the Min and Max values for 5 predefined patterns to design the fuzzy logic membership function
Unsupervised	Local Outlier Factor (LOF)	[39], [61]	An outlier detection approach based on local density
	Self-Organising Map (SOM)	[32]	A framework based on SOM clustering with a threshold classifier
	Gaussian Mixture Model (GMM)	[23]	Applied a probabilistic model for superimposed fraud
	Latent Dirichlet Allocation (LDA)	[33], [62]	A probabilistic approach that used LDA and a secondary phase for separating fraudulent profiles
	ROCK algorithm and Subspace	[31]	Constructed a bi-level clustering methodology using ROCK clustering algorithm and subspace clustering
	Graph-based	[1]	Used a graph-based approach and a threshold classifier
Semi-supervised	SOM and *k*-means with an ensemble	[30]	Used bagging and boosting ensembles to create classifiers from Decision Trees, SVMs, and ANNs

5- Challenges

The fraud detection process is hindered by various challenges that are explained briefly in this section.

5-1- Concept Drift

Concept drift refers to the condition of an online supervised learning system where the distribution of the input and output changes, which will affect the prediction model, and can be defined as [36]:

$$\exists X: p_{t_0}(X, y) \neq p_{t_1}(X, y)$$

Equation 1

where p_{t_0} is the joint distribution at time t_0, X refers to the input features, and y refers to the output. In supervised learning, the model is trained with the input features X and the respective output y. In the prediction phase, a new set of (previously unseen) input features X is given and the aim is to predict the output y. Concept drift can happen when normal behaviours keep evolving or altering, for example when the purchasing behaviour of customers changes on especial occasions such as the new year, or when fraudsters change their attacking methods. Hence, the model cannot perform accurate predictions since, under a more general perspective of drift, the relationship between the input features and the output has changed. Concept drift thus requires either updating the model incrementally or re-training it with recent batches of data [36], [56]. Adaptive learning is a solution to the concept drift problem where classical learning is not suitable. It is an advanced method of incremental learning in a non-stationary environment where the system has the capability of adapting to the stream of data [36], [57].

In certain cases, the occurrence of drift is cyclic and expected (e.g. changes in the buying preferences of customers during holidays) [56] while typically it is unanticipated and it may happen erratically. An optimal fraud detection system is expected to be able to adapt to concept drift quickly whether it is cyclic or unexpected, and also to distinguish it from noise (some learning algorithms interpret noise as concept drift) [56].

According to [56], there are three types of approaches that can handle concept drift, namely instance selection, instance weighting, and ensemble learning. In the instance selection approach, instances that are relevant to the concept are selected from the recent batches of data using a window. The pertinence of the instances is determined by how well the current model can classify them. In instance weighting, algorithms that can handle concept drift by themselves using weighted instances are used (e.g. support vector machines), however, instance weighting is prone to overfitting and [63] showed that it is inferior to instance selection. Instances are weighted by two factors, namely their age, and their appropriateness to the current concept. The ensemble learning approach tries to regularly replace the old batches of data with the most relevant and recent batches of data [64]. It hoards a series of concept descriptions, predictions that are merged by voting, weighted voting, or merely the most pertinent description is picked.

5-2- Imbalanced Data Distribution

A common problem in real-world datasets is that distributions are often imbalanced (also known as skewed data distributions). In an imbalanced binary dataset, the instances are not equally distributed amongst classes as one class, usually known as the majority class, includes more instances than the other class, which is called the minority class [65]. For instance, in a data set that is related to medical diagnosis, there might be only a few cases that have cancer with many cases being normal. This is a serious problem for supervised learning algorithms where often there are only scarce abnormal instances for training, which makes training hard due to the resulting skewed distribution [66]. In a typical imbalanced dataset, the ratio between the minority and majority classes can be, for example, 1 to 100, 1 to 1,000, 1 to 10,000 or even more [67]. The proposed methods for dealing with the imbalanced data distribution problem can be categorised into algorithmic methods and data level methods [6], [68].

At the data level, some instances are replicated or removed to balance the dataset. Under-sampling is the notion used when a portion of the majority class is removed in order to re-balance the distribution of the dataset. In contrast, over-sampling is the process by which some instances of the minority class are replicated to obtain the balance. Both approaches come with some disadvantages. Under-sampling can remove useful data while over-sampling often causes over-fitting and also increases the training time as it enlarges the dataset [69]. It is also possible to apply both under-sampling and over-sampling especially when the dataset is profoundly imbalanced or when the minority class is extremely small [67].

At the algorithmic level, there are various approaches including: (i) cost-sensitive learning that tries to offset the misclassification by putting a cost-variable, (ii) adjusting the decision threshold when using one-class classification where the model is trained merely with the target class, and (iii) adjusting the probability of the estimate when using decision trees [67]. Another solution is to apply various algorithms that are capable of dealing with skewed distributions (meta-learning) [68], [70]. In meta-learning, various classifiers are utilised to carry out the classification task, and then, their performances are integrated, via an ensemble, to outperform classification with a single classifier.

* Corresponding Author

5-3- Curse of Dimensionality

Telecommunication companies produce a large amount of data every day [34]. One aspect of this consists of a significant number of attributes, which together form a high-dimensional space that can cause several problems, often encapsulated by the term 'curse of dimensionality'. In high-dimensional space, data instances become more spread out, leading to decreased density, which in turn causes the convex hull to become stretched and difficult to distinguish [71]. High-dimensional datasets are very complicated, require larger amounts of memory and cause longer computing time that make the detection process extremely difficult and time consuming [30], [72]. Therefore, dimensionality reduction is a crucial preprocessing step especially in telecommunication fraud detection. Its goal is to reduce the dimensions and complexity of a high-dimensional dataset without losing valuable information [73]. There are two main approaches for dimensionality reduction, namely feature selection and feature extraction. The aim of feature selection methods is to extract a smaller portion of the features that contains useful information and excludes noisy, redundant and irrelevant features [74]. In feature extraction, the goal is to embed the high-dimensional dataset into a lower dimensional space thus reducing the number of effective attributes [75].

Feature selection includes three methods, which are filter, wrapper, and embedded methods [75][74] In filter methods, which act as a pre-processing step, the features are ranked using different criteria and scoring functions, then top ranked features are selected. Wrapping methods use the classifier itself to evaluate the features and have three categories, namely forward wrapping, backward wrapping, and forward-backward wrapping. Forward wrapping adds features gradually to the classification until the optimum feasible improvement is achieved. In contrast, backward wrapping tries to remove features gradually until no further improvement is feasible, and in forward-backward wrapping, features are added and also removed until maximum improvement is achieved. In embedded methods, the optimal features are selected during the model construction process using classifiers that have embedded feature selection methods.

5-4- Real Time Detection

As mentioned earlier, there are two different modes in fraud detection, namely online and offline modes. In a fraud detection system that is working in online mode, it is crucial to minimise the gap between the time when the fraud happened and the time when it was detected (known as the median duration) [76]. In fact, minimising the median duration can profoundly decrease the financial loss caused by the fraudster. Reducing the amount of data needed is considered as an effective method to achieve a system that is capable of real time detection as it can cause less memory usage and shorter computing time [30], [72].

5-5- Availability of Data

The paucity of publicly accessible data to perform research on is one the issues that hinders doing research in this area [11], [35]. Companies are usually not keen on providing their data to researchers due to the confidential information that the data contain. Also, sometimes there are laws that prevent companies from furnishing researchers with data for experimental purposes. Companies also avoid exposing details of their FDSs, because they believe this can help fraudsters understand the underlying mechanisms and create new techniques to avoid detection [34].

5-6- Noisy Data

Most real-world datasets are incomplete, noisy, and contain redundant, or obsolete records [30]. Therefore, many researchers tend to apply a preprocessing step before designing their model to clean the dataset and transform the dataset to a suitable form. As [30] explains, data preprocessing consists of three steps, namely data cleaning, data integration, and data dimensionality reduction. In data integration, the purpose is to deal with missing values, outliers, and erratic data. Data integration tries to deal with data (usually disparate) that are derived from various sources and maintaining them in one set. Data dimensionality reduction, as explained earlier, tries to transform high dimensional data into a lower dimension space. Noisy data can cause severe effects on the fraud detection process, especially with regards to accuracy. Noise is known as meaningless data that can cause variations in observations [5]. The difference between noise and outliers is that the former is not in the interest of the system and could have been caused by human error for instance. On the other hand, an outlier is a meaningful anomaly and is generally of interest to the system. It is worth noting that sometimes algorithms consider noise as outliers (in this case the outlier is the fraud instance) [77], which proves the importance of a preprocessing step prior to training the model. This is basically because the root cause of noise can be random or intentional (i.e. generated by a fraudster) [5]. Thus, FDSs should be capable of distinguishing between noise and actual outliers.

5-7- Misclassification Costs

Misclassification happens when a non-fraudulent instance is incorrectly classified as a fraudulent instance (also known as a false positive), or **when** a fraudulent instance is classified as a non-fraudulent instance (also known as a false negative). In fraud detection, the cost of a false positive misclassification is unequal to the cost of a false negative misclassification [78]. To explain further, the cost of a false negative is more expensive than a false positive because a false positive can be classified correctly after further investigation, but a false negative means that the fraudster has managed to stay undetected and can continue committing fraud. Therefore, in an FDS, a lower false negative error rate is much more important than a false positive error rate. However, it should not be deemed that the false positive rate is trivial. Further investigation requires human resources and is expensive, thus, a system with a high false positive rate can be a problem especially for companies and organisations with limited budget and human resources [79].

Table 4 Accuracy and AUC results of papers in Table 3

Ref.	Method Investigated	Accuracy	AUC
[30]	SOM, k-means with an ensemble of Decision Trees, SVM, and ANN	83.4% - 89.8%	0.796 - 0.948
[33]	A probability approach that used LDA and an automatic threshold classifier		0.967 - 0.998
[11]	Applied a supervised learning method using a multilayer perceptron (MLP)	56.1% - 98.71%	0.997
[32]	A framework based on SOM clustering with a threshold classifier	60% - 87.75%	0.717 - 0.936
[22]	Applying Quarter-Sphere SVM which is a formulation of One-Class SVM	90.0%	
[35]	A comparison between the performances of SVM and ANN	98.67% - 98.87%	0.997 - 0.985

6- Evaluation Metrics

Model evaluation is very important, because it allows one to conduct performance comparisons between different proposed systems. Besides that, evaluation makes it possible to compare different approaches, to find the best algorithm, and optimise it further for a specific problem. This section reviews the evaluation metrics used by the papers that are tabulated in Table 3.

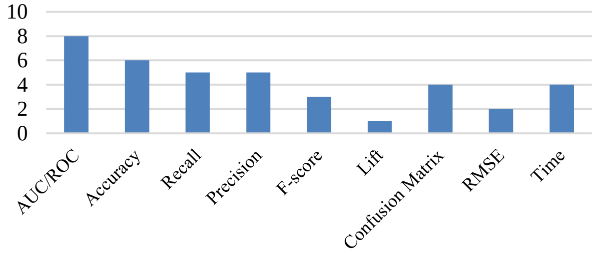

Figure 4 The number of papers in Table 3 that used evaluation metrics

As Figure 4 shows, the most widely used evaluation metrics in telecommunication fraud detection systems are accuracy (Equation 2) and AUC/ROC. However, according to [80], accuracy can lead to incorrect conclusions when it is used under certain conditions including skewed data, whereby the metric becomes biased towards the class with the majority of instances (please refer to Section 5-2 for more details).

Another very common performance metric used in this area for evaluation is the Receiver Operating Characteristic (ROC) curve, which basically visualises the probability of fraud detection versus the probability of false alarm, and the Area under ROC, also named AUC, is the area under the curve in which 1 is the perfect value [32], [81]. In cases where the model does not depend on a threshold classifier, the area under ROC metric can be superior to accuracy [30]. Although, imbalanced distributions have no effect on ROC, which makes it very attractive for datasets with skewed distributions [82], ROC curves can generate an optimistic performance evaluation in the case that the data is significantly skewed [83].

Besides the aforementioned challenges, there are other issues that should be noted. An integral requirement of a supervised learning approach is labelled data, however, its availability is often an issue, moreover, labelling can be costly, time consuming, and requires an expert [71]. Also, an anomaly can have various meanings in different application domains as some have a more generic form while others have a specific form [48], and often it is very hard and expensive in some areas to provide labels for anomalous cases such as failures in aircraft engines [84]. Moreover, the performance of fraud detection systems depends heavily on the sources of data, given that data often originates from different sources with different formats and standards [76]. For instance, attributes can be binary, categorical, continuous, or a mixture of these.

Table 5 Summary of recommended evaluation metrics

Metric	Advantages	Disadvantages
Accuracy	Frequently used, very traditional, general and intuitive	Can be biased towards the majority class
AUC/ ROC	Conceptually simple, visual performance evaluation and immune to skewed data	Can generate optimistic performance evaluations under large skewed distributions
FNR	Simple and an important financial factor	Not a thorough measurement

It is also good to introduce some metrics that are used less frequently. While some of the authors paid more attention to the time factor by revealing the detection time and also the computation time of their approaches, Root Mean Square Error (RMSE), F-score (Equation 5), and lift (Equation 6) evaluation metrics were rarely used. F-score is a measurement that shows the harmonic mean of precision and recall at a certain threshold, and lift (LFT) evaluates the true positive rate in the fraction of instances that are higher than the threshold [85]. In Table 4 the performance of the research papers that are tabulated in Table 3 are presented based on accuracy and area under ROC.

Choosing the right evaluation metric is often a problem dependent process. While a metric might fit perfectly to some problems, it may be unsuitable for other problems. Based on previous works in this area, it can be concluded that accuracy is a useful metric for performance evaluation, although it should not be concluded that it is sufficient for determining whether a proposed approach is suitable or not. In telecommunication fraud detection, ROC and AUC are vital metrics that can present important information. The advantages of ROC consist of being conceptually simple and useful for experiments in which the data is skewed, and giving a more extensive measure of classification performance [82]. Also, the false negative (FN) rate should be considered when evaluating an FDS. A high FN rate means a large number of fraudulent cases are determined as non-fraudulent cases by the system, which can cause huge financial losses as there will be no further investigation on them. However, it should be noted that solely FN rate cannot represent a comprehensive evaluation of the system as it basically concentrates on merely one specific factor. Table 5 shows a summary of the pros and cons of three evaluation metrics that are recommended by this research work.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Equation 2

$$Recal = \frac{TP}{TP + FN}$$

Equation 3

$$Precision = \frac{TP}{TP + FP}$$

Equation 4

$$F - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Equation 5

$$Lift = \frac{\%of\ positive\ above\ the\ threshold}{\%of\ dataset\ above\ the\ threshold}$$

Equation 6

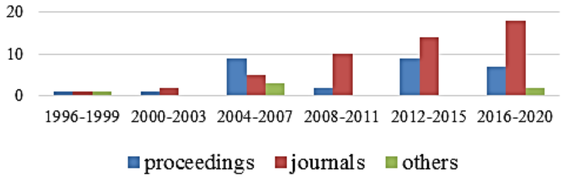

Figure 5 Source and published year of references in this paper

7- Discussion and Analysis

In previous sections, fraud types such as superimposed fraud, and subscription fraud were explained briefly. Also, various major challenges and issues in telecommunication fraud that hinder the detection process such as the curse of dimensionality and data imbalance data were reviewed.

The challenge that has received the least attention in telecommunications is arguably the problem of imbalanced class distributions. The two major works covering this issue are [20] and [30]. The authors in [20] preferred to use oversampling (they tripled the fraudulent cases), and they claimed this would avoid biasing the neural network toward classes with more instances. In contrast, in [30] the authors argued that oversampling has no advantage as it adds no new information. Therefore, they preferred to employ under-sampling to balance the dataset and tackle the issue of a skewed class distribution.

In an attempt to design a detection system that is capable of performing real-time subscription fraud detection, [20] designed a prediction model that used a multilayer perceptron neural network to evaluate customers and detect potential fraudsters at the time of subscribing, and a classification module that employed fuzzy rules to classify subscribers into four categories based on their previous behaviour. However, the performance of this approach becomes questionable when there is no previous record of new customers. In [30] the authors argued that by reducing the dimensionality of the data it is possible to reduce the time and memory needed for the algorithm, however, they believed that the problem of classifying residential subscribers (i.e. subscription fraud) is not under the category of real-time applications as there is time to perform the detection. Nonetheless, the proposed model was claimed to be capable of working in real-time as well. In another approach [33], by using merely three variables instead of a large range of variables, the authors managed to build a model that was capable of performing close to real-time detection, and did not require waiting for additional data to perform detection.

Recall that one of the major problems of fraud detection in the area of telecommunications was concept drift. Within Table 3, [31] tried to use every profile (also known as signature) only for a short period of time, and updated the profile gradually as behaviours of users evolved. They also discarded the old records or decreased their weights.

To avoid taking into consideration the noise and redundancy caused by combining all features of the high-dimensional space of the original data, [31] used a subspace clustering method, which is capable of disregarding unimportant attributes in each cluster. In [30] and [22] the authors took a different approach and preferred to use principle component analysis (PCA) to select the best features. To reduce the inner-dimensionality (fields of records) of variables, [32] employed SOMs to plot the variables to a SOM grid, thus projecting a multidimensional space into a 2-dimensional space, reflecting pattern similarities. Pruning was used to reduce the size of data in [1]. The authors of [39] selected half of the variables at their disposal to decrease complexity, and generated two additional variables for the purpose of better detection.

Cleaning the dataset from outliers or noise is also important to improve the performance (refer to Section 5 for more details). The authors of [35] utilised descriptive statistics, graphical methods, and Z-score standardisation to identify outlier values and remove them. In another work, [11] developed a model by employing neural networks that are capable of producing good performance even when the dataset contains noise. In [30] a thorough preprocessing step to clean data and deal with missing values, outliers and inconsistent data, was used.

Some of the research works in Table 3 such as [30] and [19] are based on real-world data sets while others such as [33] are based on simulated data sets. Also it is worth mentioning that some research work such as [4] is based on data sets received from third parties like banks. Another type of data set used in telecommunication fraud detection is internal audit data, which is used to detect employee fraud and misconduct. The authors of [86] tried to detect fraudulent activities in a telecommunication company based on internal audit data.

8- Conclusions

In this paper, the aim was to provide a review of different fraud systems in telecommunications. Two different fraud systems, namely fraud detection systems and fraud prevention systems, were investigated with more focus on the former system as it has arguably more potential for improvement. The mechanisms used in fraud detection systems were studied and divided into three categories, namely rule-based, visualisation, and user-profiling systems. There is no standard or uniform way to categorise fraud types, therefore, researchers have divided fraud into several groups based on different factors. This research paper attempted to review the most prevalent and thorough approaches of categorising fraud types. Four fraud types that recently were investigated in the literature are superimposed fraud, subscription fraud, toll fraud, and SIM box fraud, where superimposed fraud witnessed the most attention from researchers. Likewise, various major challenges and problems that hinder the fraud detection process were studied in this research work. Some major challenges that hinder performance are real-time constraints, skewed data, concept drift, and high-dimensionality. In addition, we tried to explore evaluation metrics that were frequently used in the literature for measuring the performance and efficiency of the proposed systems and recommended three metrics that are profoundly vital in measuring system performance, namely accuracy, AUC/ROC, and FN rate. Moreover, the paper presented the performance of several recently designed fraud detection systems since 2011 in terms of accuracy and area under ROC.

9- Future Work

The performance of a fraud detection system is very dependent upon the data that it was designed for. Therefore, it would be impactful to investigate the performance of the same system on different datasets. Moreover, FDSs in the literature have often focused on building a system that is exclusively designed for either offline or online detection. However, an optimal system should be able to effectively integrate both these types of fraud detection.

References

[1] W. Henecka and M. Roughan, “Privacy-Preserving Fraud Detection Across Multiple Phone Record Databases,” *Dependable Secur. Comput. IEEE Trans.*, vol. 12, no. 6, pp. 640–651, Nov. 2015.

[2] E. I. Tarmazakov and D. S. Silnov, “Modern approaches to prevent fraud in mobile communications networks,” in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, 2018, vol. 2018-Janua, pp. 379–381.

[3] M. Pejic-Bach, “Invited Paper: Profiling Intelligent Systems Applications in Fraud Detection and Prevention: Survey of Research Articles,” in *2010 International Conference on Intelligent Systems, Modelling and Simulation*, 2010, pp. 80–85.

[4] Y.-J. Zheng, X.-H. Zhou, W.-G. Sheng, Y. Xue, and S.-Y. Chen, “Generative adversarial network based telecom fraud detection at the receiving bank,” *Neural Networks*, vol. 102, pp. 78–86, 2018.

[5] M. Behdad, L. Barone, M. Bennamoun, and T. French, “Nature-Inspired Techniques in the Context of Fraud Detection,” *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 42, no. 6, pp. 1273–1290, Nov. 2012.

[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] J. West and M. Bhattacharya, “Intelligent financial fraud detection: A comprehensive review,” *Comput. Secur.*, vol. 57, pp. 47–66, 2016.

[8] R. J. Bolton and D. J. Hand, “Statistical Fraud Detection: A Review,” *Stat. Sci.*, vol. 17, no. 3, pp. 235–255, 2002.

[9] Y. Kou, C.-T. Lu, S. Sirwongwattana, and Y.-P. Huang, “Survey of fraud detection techniques,” in *Networking, Sensing and Control, 2004 IEEE International Conference on*, 2004, vol. 2, pp. 749-754 Vol.2.

[10] S. Wang, “A comprehensive survey of data mining-based accounting-fraud detection research,” in *2010 International Conference on Intelligent Computation Technology and Automation, ICICTA 2010*, 2010, vol.

1, pp. 50–53.

[11] A. H. Elmi, S. Ibrahim, and R. Sallehuddin, "Detecting SIM Box Fraud Using Neural Network," in *IT Convergence and Security 2012*, J. K. Kim and K.-Y. Chung, Eds. Dordrecht: Springer Netherlands, 2013, pp. 575–582.

[12] P. Gosset and M. Hyland, "Classification, detection and prosecution of fraud in mobile networks," *Proc. ACTS Mob. summit, Sorrento, Italy*, 1999.

[13] V. Jain, "Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining," *Int. J. Inf. Technol.*, vol. 9, no. 3, pp. 303–310, 2017.

[14] H. M. Marah, O. M. Elrajubi, and A. A. Abouda, "Fraud detection in international calls using fuzzy logic," in *Proceedings - International Conference on Computer Vision and Image Analysis Applications, ICCVIA 2015*, 2015.

[15] L. Cortesão, F. Martins, A. Rosa, and P. Carvalho, "Fraud management systems in telecommunications: a practical approach," in *12th International Conference on Telecommunications*, 2005, pp. 167–182.

[16] T. Fawcett and F. Provost, "Adaptive Fraud Detection," *Data Min. Knowl. Discov.*, vol. 1, no. 3, pp. 291–316, 1997.

[17] C. S. Hilas and J. N. Sahalos, "An Application of Decision Trees for Rule Extraction Towards Telecommunications Fraud Detection," in *Knowledge-Based Intelligent Information and Engineering Systems: 11th International Conference, KES 2007, XVII Italian Workshop on Neural Networks, Vietri sul Mare, Italy, September 12-14, 2007. Proceedings, Part II*, B. Apolloni, R. J. Howlett, and L. Jain, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 1112–1121.

[18] J. Lopes, O. Belo, and C. Vieira, "Applying User Signatures on Fraud Detection in Telecommunications Networks," in *Advances in Data Mining. Applications and Theoretical Aspects: 11th Industrial Conference, ICDM 2011, New York, NY, USA, August 30 -- September 3, 2011. Proceedings*, P. Perner, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 286–299.

[19] P. Saravanan, V. Subramaniyaswamy, N. Sivaramakrishnan, M. Arun Prakash, and T. Arunkumar, "Data mining approach for subscription-fraud detection in telecommunication sector," *Contemp. Eng. Sci.*, vol. 7, no. 9–12, pp. 515–522, 2014.

[20] P. A. Estévez, C. M. Held, and C. A. Perez, "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks," *Expert Syst. Appl.*, vol. 31, no. 2, pp. 337–344, 2006.

[21] F. M. Kau and O. P. Kogeda, "Impact of Subscription Fraud in Mobile Telecommunication Companies," in *2019 Open Innovations (OI)*, 2019, pp. 42–47.

[22] S. Patnaik, S. Subudhi, and S. Panigrahi, "Quarter-Sphere Support Vector Machine for Fraud Detection in Mobile Telecommunication Networks," *Procedia Comput. Sci.*, vol. 48, pp. 353–359, 2015.

[23] M. I. M. Yusoff, I. Mohamed, and M. R. A. Bakar, "Fraud detection in telecommunication industry using Gaussian mixed model," in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013, pp. 27–32.

[24] M. Arafat, A. Qusef, and G. Sammour, "Detection of Wangiri Telecommunication Fraud Using Ensemble Learning," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 330–335.

[25] G. Phil and H. Mark, "Classification Detection and Prosecution of Fraud on Mobile Networks," in *Proceedings of ACTS Mobile Summit, Sorrento Italy*, 1999.

[26] S. Kamas and M. A. Aydin, "SPIT detection and prevention," *Istanbul Univ. - J. Electr. Electron. Eng.*, vol. 17, pp. 3213–3218, 2017.

[27] L. Carvajal, L. Chen, C. Varol, and D. Rawat, "Detecting unprotected SIP-based Voice over IP traffic," in *4th International Symposium on Digital Forensics and Security, ISDFS 2016 - Proceeding*, 2016, pp. 44–48.

[28] G. Cho, J. Cho, Y. Song, D. Choi, and H. Kim, "Combating online fraud attacks in mobile-based advertising," *Eurasip J. Inf. Secur.*, vol. 2016, no. 1, pp. 1–9, 2016.

[29] M. Yelland, "Fraud in mobile networks," *Comput. Fraud Secur.*, vol. 2013, no. 3, pp. 5–9, 2013.

[30] H. Farvaresh and M. M. Sepehri, "A data mining framework for detecting subscription fraud in telecommunication," *Eng. Appl. Artif. Intell.*, vol. 24, no. 1, pp. 182–194, 2011.

[31] L. P. Mendes, J. Dias, and P. Godinho, "Bi-level clustering in telecommunication fraud," in *ICORES 2012 - Proceedings of the 1st International Conference on Operations Research and Enterprise Systems*, 2012, pp. 126–131.

[32] D. Olszewski, "Fraud detection using self-organizing map visualizing the user profiles," *Knowledge-Based Syst.*, vol. 70, pp. 324–334, 2014.

[33] D. Olszewski, "A probabilistic approach to fraud detection in telecommunications," *Knowledge-Based Syst.*, vol. 26, pp. 246–258, 2012.

[34] C. S. Hilas and J. N. Sahalos, "User profiling for fraud detection in telecommunication networks," in *In: 5th Int. Conf. technology and automation*, 2005, pp. 382–387.

[35] R. Sallehuddin, S. Ibrahim, A. M. Zain, and A. H. Elmi, "Detecting SIM box fraud by using support vector machine and artificial neural network," *J. Teknol.*, vol. 74, no. 1, pp. 137–149, 2015.

[36] J. Gama, I. Zliobaite, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 44:1--44:37, Mar. 2014.

[37] Z. Shaeiri, J. Kazemitabar, S. Bijani, and M. Talebi, "Behavior-Based Online Anomaly Detection for a Nationwide Short Message Service," *J. AI Data Min.*, vol. 7, no. 2, pp. 239–247, 2019.

[38] L. Manunza, S. Marseglia, and S. P. Romano, "Kerberos: A real-time fraud detection system for IMS-enabled VoIP networks," *J. Netw. Comput. Appl.*, vol. 80, pp. 22–34, 2017.

[39] K.-I. Kim, T. Kim, N.-W. Cho, and M. Kim, "Toll Fraud Detection of VoIP Service Networks in Ubiquitous Computing Environments," *Int. J. Distrib. Sens. Networks*, vol. 2015, 2015.

[40] J. Li, K.-Y. Huang, J. Jin, and J. Shi, "A survey on statistical methods for health care fraud detection," *Health Care Manag. Sci.*, vol. 11, no. 3, pp. 275–287, 2008.

[41] C. S. Hilas, "Designing an expert system for fraud detection in private telecommunications networks," *Expert Syst. Appl.*, vol. 36, no. 9, pp. 11559–11569, 2009.

[42] K. C. Cox, S. G. Eick, G. J. Wills, and R. J. Brachman, "Brief Application Description; Visual Data Mining: Recognizing Telephone Calling Fraud," *Data Min. Knowl. Discov.*, vol. 1, no. 2, pp. 225–231, 1997.

[43] W. N. Dilla and R. L. Raschke, "Data visualization for fraud detection: Practice implications and a call for future research," *Int. J. Account. Inf. Syst.*, vol. 16, pp. 1–22, 2015.

[44] J. A. Lasserre, C. M. Bishop, and T. P. Minka, "Principled Hybrids of Generative and Discriminative Models," in *2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06)*, 2006, vol. 1, pp. 87–94.

[45] C. S. Hilas and J. N. Sahalos, "Testing the fraud detection ability of different user profiles by means of FF-NN classifiers," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4132 LNCS, pp. 872–883, 2006.

[46] C. S. Hilas and P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection," *Knowledge-Based Syst.*, vol. 21, no. 7, pp. 721–726, 2008.

[47] S. S. Rajani and M. Padmavathamma, "A Model for Rule Based Fraud Detection in Telecommunications," in *International Journal of Engineering Research and Technology*, 2012, vol. 1, no. 5 (July-2012).

[48] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 15:1--15:58, Jul. 2009.

[49] J. Tamboli and M. Shukla, "A survey of outlier detection algorithms for data streams," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 3535–3540.

[50] C. Hilas, P. Mastorocostas, and I. Rekanos, "Clustering of telecommunications user profiles for fraud detection and security enhancement in large corporate networks: a case study," *Appl. Math. Inf. Sci.*, vol. 9, pp. 1709–1718, 2015.

[51] J. Hollmén and V. Tresp, "Call-based Fraud Detection in Mobile Communication Networks Using a Hierarchical Regime-switching Model," in *Proceedings of the 1998 Conference on Advances in Neural Information Processing Systems II*, 1999, pp. 889–895.

[52] X. Zhu and A. B. Goldberg, "Introduction to semi-supervised learning," *Synth. Lect. Artif. Intell. Mach. Learn.*, vol. 3, no. 1, pp. 1–130, 2009.

[53] A. Daneshpazhouh and A. Sami, "Semi-Supervised Outlier Detection with Only Positive and Unlabeled Data Based on Fuzzy Clustering," *Int. J. Artif. Intell. Tools*, vol. 24, no. 03, p. 1550003, 2015.

[54] D. Olszewski, "Fraud Detection in Telecommunications Using Kullback-Leibler Divergence and Latent Dirichlet Allocation," in *Adaptive and Natural Computing Algorithms*, 2011, pp. 71–80.

[55] A. Chouiekh and E. L. H. I. E. L. Haj, "ConvNets for Fraud Detection analysis," *Procedia Comput. Sci.*, vol. 127, pp. 133–138, 2018.

[56] A. Tsymbal, "The Problem of Concept Drift: Definitions and Related Work," 2004.

[57] J. L. Lobo, J. Del Ser, M. N. Bilbao, I. Laña, and S. Salcedo-Sanz, "A probabilistic sample matchmaking strategy for imbalanced data streams with concept drift," *Stud. Comput. Intell.*, vol. 678, pp. 237–246, 2017.

[58] S. Augustin *et al.*, "Telephony fraud detection in next generation networks," in *AICT 2012 - 8th Advanced International Conference on Telecommunications*, 2012, pp. 203–207.

[59] Y. Alraouji and A. Bramantoro, "International call fraud detection systems and techniques," in *MEDES 2014 - 6th International Conference on Management of Emergent Digital EcoSystems, Proceedings*, 2014, pp. 159–166.

[60] X. Liu and X. Wang, "A Network Embedding Based Approach for Telecommunications Fraud Detection," in *Cooperative Design, Visualization, and Engineering*, 2018, pp. 229–236.

[61] G. Kaiafas, C. Hammerschmidt, R. State, C. D. Nguyen, T. Ries, and M. Ourdane, "An Experimental Analysis of Fraud Detection Methods in Enterprise Telecommunication Data using Unsupervised Outlier Ensembles," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 37–42.

[62] N. Ruan, Z. Wei, and J. Liu, "Cooperative Fraud Detection Model With Privacy-Preserving in Real CDR Datasets," *IEEE Access*, vol. 7, pp. 115261–115272, 2019.

[63] R. Klinkenberg, "Learning drifting concepts: Example selection vs. example weighting," *Intell. Data Anal.*, vol. 8, no. 3, pp. 281–300, 2004.

[64] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in *2015 International Joint Conference on Neural Networks (IJCNN)*, 2015, pp. 1–8.

[65] Y. Yan, M. Chen, M.-L. Shyu, and S.-C. Chen, "Deep Learning for Imbalanced Multimedia Data Classification," in *Proceedings - 2015 IEEE International Symposium on Multimedia, ISM 2015*, 2015, pp. 483–488.

[66] S. Al-Stouhi and C. K. Reddy, "Transfer learning for class imbalance problems with inadequate data," *Knowl. Inf. Syst.*, vol. 48, no. 1, pp. 201–228, 2016.

[67] N. V Chawla, N. Japkowicz, and A. Kotcz, "Editorial: Special Issue on Learning from Imbalanced Data Sets," *SIGKDD Explor. Newsl.*, vol. 6, no. 1, pp. 1–6, Jun. 2004.

[68] C. Phua, D. Alahakoon, and V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data,"

SIGKDD Explor. Newsl., vol. 6, no. 1, pp. 50–59, Jun. 2004.

[69] R.-C. CHEN, T.-S. CHEN, and C.-C. LIN, "A new binary support vector system for increasing detection rate of credit card fraud," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 20, no. 02, pp. 227–239, 2006.

[70] S.-C. Lin, Y. I. Chang, and W.-N. Yang, "Meta-learning for Imbalanced Data and Classification Ensemble in Binary Classification," *Neurocomput.*, vol. 73, no. 1–3, pp. 484–494, Dec. 2009.

[71] V. J. Hodge and J. Austin, "A Survey of Outlier Detection Methodologies," *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, 2004.

[72] L.-A. Gottlieb, A. Kontorovich, and R. Krauthgamer, "Adaptive metric dimensionality reduction," *Theor. Comput. Sci.*, vol. 620, pp. 105–118, 2016.

[73] M. Sugiyama, "Local Fisher Discriminant Analysis for Supervised Dimensionality Reduction," in *Proceedings of the 23rd International Conference on Machine Learning*, 2006, pp. 905–912.

[74] J. Miao and L. Niu, "A Survey on Feature Selection," *Procedia Comput. Sci.*, vol. 91, pp. 919–926, 2016.

[75] S. Agarwal, P. Ranjan, and R. Rajesh, "Dimensionality reduction methods classical and recent trends: A survey," *Int. J. Control Theory Appl.*, vol. 9, no. 10, pp. 4801–4808, 2016.

[76] A. Bănărescu, "Detecting and Preventing Fraud with Data Analytics," *Procedia Econ. Financ.*, vol. 32, pp. 1827–1836, 2015.

[77] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying Density-based Local Outliers," *SIGMOD Rec.*, vol. 29, no. 2, pp. 93–104, May 2000.

[78] C. Phua, V. C. S. Lee, K. Smith-Miles, and R. W. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research," *CoRR*, vol. abs/1009.6, 2010.

[79] B. Barbarioli and R. M. Assuncao, "Anomaly Detection under Cost Constraint," in *Proceedings - 2016 5th Brazilian Conference on Intelligent Systems, BRACIS 2016*, 2016, pp. 247–252.

[80] G. Haixiang, L. Yijing, J. Shang, G. Mingyun, H. Yuanyue, and G. Bing, "Learning from class-imbalanced data: Review of methods and applications," *Expert Syst. Appl.*, vol. 73, pp. 220–239, 2017.

[81] Z. Chen, L. D. Van Khoa, E. N. Teoh, A. Nazir, E. K. Karuppiah, and K. S. Lam, "Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review," *Knowl. Inf. Syst.*, vol. 57, no. 2, pp. 245–285, Nov. 2018.

[82] T. Fawcett, "An introduction to {ROC} analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, 2006.

[83] J. Davis and M. Goadrich, "The Relationship Between Precision-Recall and ROC Curves," in *Proceedings of the 23rd International Conference on Machine Learning*, 2006, pp. 233–240.

[84] P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, "A Survey of Outlier Detection Methods in Network Anomaly Identification," *Comput. J.*, 2011.

[85] R. Caruana and A. Niculescu-Mizil, "Data Mining in Metric Space: An Empirical Analysis of Supervised Learning Performance Criteria," in *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2004, pp. 69–78.

[86] A. Nawawi and A. S. A. P. Salin, "Employee fraud and misconduct: empirical evidence from a telecommunication company," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 129–144, 2018.

Kasra Babaei is currently a PhD candidate at University of Nottingham Malaysi, received the MSc in Information Technology (Merit) from University of Nottingham in 2014, and his BSc in Business Administration from University of Payam Noor, Anzali Branch, Iran in 2011

Dr. Chen ZhiYuan curently is an Assistant Professor with the University of Nottingham Malaysia (UNM) and a Principal Consultant with MIMOS at the Accelerative Technology Lab. She received the MPhil and a PhD in Computer Science from the University of Nottingham. Before joining UNM, she has been a research associate in the UK Horizon Digital Economy Research Institute. Her research interests are in the area of computer science, machine learning, data mining, user modelling and artificial intelligence.

Tomas Maul received a BSc (Hons.) degree in Psychology from the University of St. Andrews, St. Andrews, UK, two MSc degrees in Computer Science from Imperial College, London, UK, and a PhD degree in Computer Science (Computational Neuroscience) from the University of Malaya, Kuala Lumpur, Malaysia. He is currently Associate Professor at the School of Computer Science, University of Nottingham Malaysia.