IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 4, August 2026, pp. 3269~3285
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i4.pp3269-3285

Systematic review of fraud detection using AI and ML with an emphasis on telecommunication industry

Soly Mathew Biju, Sindi Rryta
School of Computer Science, University of Wollongong in Dubai, Dubai, United Arab Emirates

Article Info

Article history:

Received May 22, 2025
Revised Jun 3, 2026
Accepted Jul 9, 2026

Keywords:

Artificial intelligence
Behavioral pattern
Fraud detection
Machine learning
Performance metrics
Telecommunication industry

ABSTRACT

The telecommunications industry is one of the top industries affected by fraudulent activities. Given the financial impact, on top of confidentiality breaches, security concerns, and reduced service quality as well as consumer dissatisfaction, there is an immediate need to implement effective fraud detection approaches. While there have been different fraud detection systems implemented, technological advancements as well as the improved techniques of fraudsters have made the traditional approaches no longer efficient. This paper aims to further investigate the use of artificial intelligence (AI) and machine learning (ML) to create efficient and advanced fraud detection models based on the strategy used, models applied, accuracy of the system, as well as future research work suggested. A systematic review of 50 papers was conducted. The most prevalent strategy was supervised one, majority of papers used software instead of hardware, and the most common ML models were artificial neural network (ANN), support vector machine (SVM), and decision tree.

Corresponding Author:

Soly Mathew Biju
School of Computer Science, University of Wollongong in Dubai
Office 201, Block 15, Knowledge Park, PO Box 20183, Dubai, United Arab Emirates
Email: solymathewbiju@uowdubai.ac.ae

1. INTRODUCTION

In a technologically advanced world, the potential threat from economic crimes and fraud has increased drastically, creating new security concerns for businesses and consumers among all types of industries. Fraud is defined as the act of getting money by lying to people [1]. In other words, it includes any opportunistic behavior through which one party exploits the other one for monetary benefits. Statistics suggest that in 2025 fraud accounts for more than $1 trillion losses worldwide in all types of industries, out of which only 4% of affected businesses do retrieve their assets back [2]. According to the Association of Certified Fraud Examiners, telecommunication is one of the top affected industries from fraud [3]. Such a thing can be explained by many factors. Firstly, the complex nature of the telecommunication network which includes many processes increases the opportunity for profit. Moreover, the high number of parties involved which aim to maximize their individual benefit besides the company's one, adds to such complexity. Another important reason is the existence of different legal and regulatory frameworks upon which agreements and settlements are built. Lastly, opportunity for high profit margins due to differences in termination rates among different countries makes telecom a highly fraud prone industry.

Given the severity, financial as well as security concerns of fraud among telecommunication industry, different approaches regarding fraud detection have been proposed. According to Yehya and Salhab [4], the main fraud detection techniques are call data record (CDR) analysis, pattern recognition, real-time monitoring, rule-based system, and machine learning (ML) algorithms. CDR analysis consists of data records

for each call such as duration, count, origin, destination, repetition and other related details. This analysis is crucial in understanding patterns and identifying anomalies in user behavior. Moreover, pattern recognition is applied to differentiate between normal and suspicious behaviors, which depends on the relationship between data points and data usage. Many mobile operators utilize statistical models to conduct recognition pattern analysis. Regarding the real-time monitoring, it is a crucial component considering the nature of fraud, which needs to be detected as soon as the fraud has been conducted. Usually, fraud management systems use alerts and real time monitoring to manage fraud cases. A rule-based system is a fraud detection method that functions upon pre-defined rules that match fraud patterns. Such rules are defined based on historical data and are applied to the live traffic, to generate alerts in case such rules are breached. However, this technique needs continuous rule update and enrichment to ensure accuracy. Lastly, ML algorithms are a very efficient method considering their ability to handle a large amount of CDR traffic and provide great prediction rates. Such modules can continuously be updated by learning through new data, hence, improving their performance.

The aim of this paper is to provide a detailed review of the existing literature on fraud detection methods that use artificial intelligence (AI) and ML models in the telecommunications industry as in Table 1 (see in Appendix). For each reviewed study, this review presents the aim of the study and the applied strategy, including supervised, unsupervised, semi-supervised, knowledge-based, and visualization-based approaches. It also describes the utilized hardware/software, applied algorithms, sample size, achieved model accuracy, used database, and suggested future study.

2. METHOD

This systematic literature review focuses on the existing research work on the detection of fraud in the telecommunications industry by using AI and ML models. Different models and approaches have been proposed by different scholars, given the changing nature of fraud while adopting the technological advancements of each time. This study aims to provide an overview of the existing research work while pointing out any existing gaps regarding the use of AI and ML in fraud detection. The following are the main elements upon which this literature review is built: strategy (supervised, unsupervised, and semi-supervised), algorithms used, hardware or software or both, accuracy of model, data sample size, and future suggestions.

This paper detected relevant studies by using the keyword search method. Several keywords were discovered on Google Scholar, Research Gate, IEEE, Academia, Elsevier, and Springer. Such keywords were ‘Fraud detection’, ‘Telecommunication network’, and “AI and ML”. The primary objective of this study is to provide an overview of the existing literature regarding fraud detection in telecommunications networks while using AI and ML models, which can provide added value within the telecom industry. After searching in different journals and credible websites for research publications as mentioned above, 50 articles were carefully selected. Each paper contains three main elements, such as aim of the study, methodology, and accuracy. Please refer to the results and discussion section for more details.

3. RESULTS AND DISCUSSION

AlBougha [5] proposes the use of different data mining classification algorithms in detecting a particular telecom fraud type, such as subscriber identity module (SIM) box. This paper compares the performance of four different ML models such as boosted trees classifiers, support vector machines (SVM), logistic classifiers, and neural networks (NN). Findings of the study suggest that the boosted trees and logic classifiers performed the best when compared to the other models with an accuracy of more than 91% and a false positive rate smaller than 1%. Sallehuddin *et al.* [6] suggest the use of 9 features to identify SIM box fraud while using artificial neural network (ANN) and SVM models. All combinations of the parameters have been tested though a 10 cross validation to check the performance of these two ML models. The best models were chosen on the criteria of accuracy, time, generalization error and precision from 80 ANN and 40 SVM models created. These two best models were then compared with each other by applying different partitions of training and testing. Such paper suggests that SVM has a higher accuracy of 99.06% than ANN with 98.69%. Moreover, the former performs better in terms of false negatives and takes three times less processing time than the latter when detecting SIM box. Krenker *et al.* [7] showcase use of bidirectional artificial neural network (Bi-ANN) to detect mobile phone fraud by predicting individual behaviors. This system manages to detect fraud in offline processing and real time CDRs. Moreover, such models were able to predict complex time series such as call duration, but with a better accuracy of 90% when compared to other models. It was also concluded that the longer input time series and shorter predicted time series yielded better results, while the number of hidden layers in Bi-ANN was crucial in improving the prediction results.

Saravanan *et al.* [8] adopt a probability-based model such as naïve Bayesian to predict subscription fraud while also using six attributes to create the fraud profiles such as duration, daytime, nighttime, weekdays, weekends, and total call count. To resolve the misclassification of fraudulent cases due to the threshold-based nature of the model, this study utilizes naïve Bayesian for continuous values and an adjusted version of Kullback–Leibler (KL) divergence, which supports in findings the difference between two probabilistic quantities and resolves the need of a big training dataset. The study shows that the CDRs that have big divergence value identify the fraudulent customers. In the same line of thought, Wassie [9] suggests the use of a predictive model using deep autoencoder in detecting subscription fraud. This model performs with 98.95% accuracy on detecting real fraud cases by combining deep neural autoencoder, convolutional neural network (CNN), and long short-term memory (LTSM) autoencoder algorithms with thresholds of 0.0103 and 0.0173, respectively. Grosser *et al.* [10] also suggest the use of NN in creating mobile fraudulent users' profiles based on several parameters such as international mobile subscriber identity (IMSI), date, time, duration, and call type (local, national, and international). Once such profiles are created, the NN model is trained to detect such fraudulent behavioral patterns, which make sure the model performs with high accuracy in detecting real future fraud cases and provides more insights into the change of such users' behavior over time. Elmi *et al*. [11] support the use of an ANN utilizing a multi-layer perceptron (MLP) classifier in detecting SIM box fraud. This study created 240 NN models which were evaluated regarding their accuracy, generalization error, building time, precision, and record. Results showed that the best performing accuracy was achieved when two hidden layers with a learning rate of 0.6 were applied, meaning a lower momentum and a higher learning rate combination. The best performing NN model had an accuracy of 98.71% with a false negative rate of 2.9%.

Sanver and Karahoca [12] consist of a comparative study between different data mining techniques to determine the best model for the telecom fraud prediction. This model uses several data mining methods such as JRip, Ridor, PART, OneR, Nnge, decision table, conjunction rules, AD tree, IB1, Bayesnet, and adaptive neuro fuzzy inference (ANFIS). Findings of the study suggest that the ANFIS method is the best one with an accuracy of 98.33%, sensitivity of 97, and specificity of 99%. One of the main advantages of ANFIS method is that it combines the precision of fuzzy logic classification and the adaptation of NNs, providing a great performance. Thaddeus *et al.* [13] do support the use of the ANN model in predicting SIM box. A class of ANN model, namely MLP, was used to analyze the CDRs by being trained 50 times in a data set containing true data classified as true and not true SIM box cases and using specific parameters such as call duration, call frequency, time, originating, and terminating number. The accuracy of the ANN improves from 57.04% to 80.01% after 50 iterations with a top layer of 16 nodes. Hilas and Mastorocostas [14] compare several ML models, such as random forest (RF), logistic regression, SVM, gradient boosting, and naive Bayes, to predict the International Revenue Share Fraud (IRSF). The evaluation of the best model was conducted on several criteria such as accuracy, precision, recall, and F1-score. Findings of the study conclude that the best model for IRSF prediction is RF with 99% accuracy while also conveying that ML models are a powerful tool that should be considered for telecom fraud detection and mitigation. Moreover, Li *et al*. [15] also suggest the use of different ML models in detecting malicious phone calls. The study considers 29 parameters of CDRs and the historical data to obtain the average first prediction (AFP) metric, which presents the amounts of calls a fraudulent person must make before being predicted and blocked in advance. Out of all the models, RF is the best one with 90% accuracy.

Elmi *et al.* [16] suggest the use of SVM and ANN in detecting SIM box in the telecommunication industry. For the development of the ANN model, 240 models with all the possible parameter combinations were created and the models' evaluation was conducted based on prediction accuracy, generalization error, running time, precision, and recall. Similarly, for the SVM model, 40 models were created, while the evaluation criteria were prediction accuracy, running time, precision, and recall rate. Findings of the paper suggest that SVM model performs better than the ANN with 98.9% accuracy, 99.064% classification accuracy of false positives and negatives and 5.55 seconds running time. Barson *et al.* [17] explore the use of a supervised approach utilizing the MLP network in detecting mobile phone frauds with 92.5% accuracy. For each user, the details from the CDR help create a user profile, which can belong to historical or recent times. By using a MLP network, with 18 inputs and two outputs (valid or fraud), the model is tested and trained continuously to improve the detection, however, the size of the time window from which the recent pattern behavior is taken and the aging of the data used may impact the accuracy. Murynets *et al*. [18] suggest use of different classifiers to detect SIM box cases with high accuracy. Namely, this study uses alternating decision tree, functional tree, and RF and evaluates their performance on their own with an accuracy of 99.1%, 99.90%, and 99.93%, respectively. The study does also combine all three classifiers into a classification rule, which performs better than any standalone classifier with 99.95% prediction accuracy of the SIM box cases.

However, Marah *et al.* [19] suggest the use of fuzzy logic and profiling the fraudulent users' behavior to detect SIM box. The study utilizes real-life data, out of which five parameters such as subscriber's mobility, incoming to outgoing calls ratio, suspicious cell activity, irregular calls, and service

type, are used to build the membership function (MF) and the fuzzy logic rules. Each rule has inputs which are the chosen parameters, an output which can be fraud or not fraud, as well as a defined threshold. Moreover, each rule has the minimum and maximum values defined. Such values do affect how the model performs and can be easily adjusted in building the visualization model. The model obtains the IMSI and the threshold by the user and provides the fraud score MF. If the latter breaches the threshold value, cases are considered as fraudulent. However, the model needs to be trained on trusted data, meaning data that is confirmed as fraudulent for accuracy improvement. Following the same line of thought, Ogwueleka [20] also suggests the use of user profiling and classification techniques to detect fraud in mobile telecommunication networks. The first step of the study consists of learning the user profiling from labeled data, which is then later used to detect fraud. Both probabilistic and NNs were trained at user level, user profile level, and class level, out of which the second performed better. This study uses the receiver operating characteristic (ROC) curve for both training and testing sets, which resulted in less than 3% of false positives, entailing more than 97% accuracy. Aranuwa [21] provides an interesting hybrid model that mixes differential and absolute analysis to model the network mechanism while utilizing the NNs to learn the subscribers' call data. The absolute approach provides whether a user is fraudulent or not based upon the call pattern statistics, while the differential one focuses on changes of behavior patterns when moving from a normal user to a fraud one. Results of the study provide an 89% accuracy and 2.71 mean absolute error (MAE) in detecting fraud of postpaid mobile communication networks.

Rebahi *et al*. [22] propose a full framework of implementing a platform that mitigates fraud on voice over internet protocol (VoIP) environments. This framework is built on unsupervised methods such as signature and clustering-based techniques. The main idea of the framework is to use clustering methods to track changes in user behavior by first training the model with data that is assumed to be clean data of normal users and testing to ensure that the user behavior does match with the normal user behavior learned in the former phase. The main parameters that are used for clustering are A-number, B-number, start time, duration, status, A-IP, B-IP, group, and flags. While this framework is still under development, it envisions a 360 solution, from obtaining VoIP CDRs data to modeling, analysis, and automation of the alarms whenever some changes in the clustering models are indicative of fraudulent activities. Hollmén [23] also proposes the use of an unsupervised approach in detecting mobile communications network fraud using NNs and probabilistic models. However, the added value of this work consists of the fact that it learns how to detect fraud behavior from partially labeled data with an unknown mixing mechanism, because the data set does not differentiate the fraud and non fraud cases. Moreover, the representation of data is important for the prediction's accuracy but the trade-off between the latency in detection time and richness of description should be considered. The models perform relatively well with a ratio of 2%–3% of false positives. Moreau *et al.* [24] suggested several fraud detection strategies in mobile telecommunication networks such as supervised NN, unsupervised network and rule based. According to this paper, the parameters that should be considered as the most fraud-relevant ones are charged IMSI, first cell ID, chargeable duration, B number type, and called number. Regarding the rule-based approach, both absolute or differential usage can be applied to provide a better view of whether a user is fraudulent or not and what changes are observed in his/her behavior. Moreover, the need for near real time data is also emphasized for this approach. In supervised NN approach, the model will group similar patterns in clusters, however; the user must assign which class is associated with each cluster. However, for the supervised NN approach the data must be pre-labelled before learning of the model.

Taniguchi *et al.* [25] explore the detection of telecom fraud by using NN, Gaussian model, and Bayesian network while using the ROC curve to assess their respective performance. The former model uses several parameters such as duration average, duration standard deviation, call number during the day, maximum duration, and call number per day during the observed time window. The ROC for this model indicated 85% accuracy without any false positives. The Gaussian probabilistic model calculates the probability density function of the past and current subscriber's behavior. Parameters used in this approach were daily calls count and call duration during on-peak and off-peak hours. The ROC curve suggests a 70% accuracy of such model without any false positives. Lastly, for the Bayesian network, two models were built, one that modeled the behavior of fraudulent users and another for legitimate users to calculate what would be the fraud probability for the considered user. The ROC curve shows 85% accuracy in prediction. In another article, Hollmén and Tresp [26] suggest a hierarchical regime-switching model to detect call-based fraud. Inference rules of the model are retrieved from the junction tree algorithm while the model is trained using the expectation-maximization (EM) and discriminative algorithms. Lastly, the model is tested through on-line detection mode and retrospective classification. Findings of the article suggest that with a false alarm probability of 0.3% the on-line detection and retrospective classification perform well with accuracy of 97.4% and 93.4%, respectively. However, when the false alarm probability is increased to 2%, their performance drops to 92.8% and 92.1%, respectively. Hollmén *et al.* [27] suggest the use of a self-organizing

map (SOM) to cluster probabilistic models that can help detect fraudulent cases in telecommunications networks. The paper trains a SOM of 80 units, with a rectangular topology (8×10 map units), on the statistics of the time series. Training of the map was conducted on two steps, the coarse ordering and fine tuning. Results of the map to class-specific distributions show that the upper parts of the map are fraudulent users while the lower parts are legitimate ones.

Kehelwala [28] proposes a new approach which uses complex event processing (CEP), business activity monitoring (BAM) to ensure real-time detection of off-net and on-net SIM box cases. The model was able to capture certain fraud features that cannot be manipulated by fraudsters. These features enable the model to detect gray call instances with a 99.9% accuracy in both on-net and off-net SIM box cases while also increasing the detection speed. Moreover, the model not only detects fraudulent cases but also manages to predict 9.93 call attempts earlier than other operators' existing solutions. Kashir and Bashir [29] try different ML techniques to provide the best SIM box prediction accuracy for ANN and SVM models. When building ANN model, 25 attributes of the usual and fraudulent users are used as inputs while the model's performance is evaluated based upon confusion matrix, ROC, and variants of ANN. As per the confusion matrix, the ANN performs with an accuracy of 100% in predicting SIM box cases and 99.3% predicting legitimate ones. Moreover, based on the ROC, continuous training of the model improved the ratio of the true positives over the false positives. Lastly, 5 different NN algorithms were used to predict SIM box cases and results suggest that Bayesian regularization performs the best while resilient back propagation the worst with accuracy 99.87% and 99.535%, respectively. As for the SVM model, the performance was evaluated on different SVM kernels, and findings suggest that use of polynomial, radial basis and sigmoid kernels perform better with an accuracy of 99.24% and a regression of 3% while pre-computed kernel and liner kernel perform worst with an accuracy and regression of 95.78% and 17%, and 95.18% and 19%, respectively.

Li *et al* [30] propose a novel natural language processing (NLP) based model to detect telecom fraud. The study adopts an extensive five category data set such as the impersonation of customer service, the impersonation of leadership acquaintances, loans, public security fraud, and normal texts. Moreover, it also combines the inconsistency loss function with cross entropy function, which created a new loss function network, that has improved fraud detection performance. Lastly, a new data model for telecom fraud detection is created based on a robustly optimized bidirectional encoder representations from transformers pretraining approach (RobERTa), which is improved with multi-head attention and residual connections (MHARC). When compared with five other models that were tested in the same three data sets, RoBERTa-MHARC, suggested by this study, performed the best with an accuracy of 93.69%. This confirms that the use of pre-trained models can positively improve performance in multi-class classifications. Moreover, the use of multi-head attention enables the model to focus on different parts of the input, capturing information about specific semantics, making the model better understand relationships between variables. Another interesting new approach is provided by Zhao *et al*. [31], which uses speech recognition through natural language programming to detect keywords from fraudulent calls and later use these keywords as parameters in the models that will be created, namely logistic regression, NN, and decision tree. Moreover, the authors of this paper have created a mobile application that performs real time fraudulent detection through voice recognition of the key words, which are registered through an option within the application, converted into text, and compared to the existing rules obtained by training and testing the ML models, and in case the call is determined as fraudulent, an alarm will be sent to mobile application to notify the user. Findings of the study suggest that the models perform with an accuracy higher than 98.53%.

Subudhi and Panigrahi [32] suggest the use of probabilistic fuzzy C-means clustering (PFCM) to detect telecom fraud. The study considers four main parameters of a CDR such as international mobile equipment identity (IMEI), time of the call, duration of the call, and type of the call. Once the required parameters are obtained, several tests are handled to find the optimal number of clusters needed, which results in two clusters. Moreover, the PFCM clustering is run several times with different parameter values to observe which threshold is required for efficient fraud detection. Results of the study suggest that a threshold of 0.003 ensures an accuracy of 93.09% which is the highest among all the combinations. Moreover, the study also compares the PFCM with other clustering techniques. Such analysis suggests that the former is the most accurate one (93.03%) while maintaining the highest ratio of true positives (95.07%) and the lowest ratio of false positives (9.25%). Daniel [33] adopts an unsupervised model that combines evidence from multiple sources for fraud detection, such as the Dempster-Shafer model and compares it to the Bayesian one. The study starts by checking the performance of each model separately; the former performs better with an accuracy of 85.71% when compared to the latter with an accuracy of 50.4%. However, the aim of the study is to combine probabilities of several individual fraudulent rules into a global belief for a given hypothesis, which is done through the Dempster-Shafer model. The main takeaway of the study is that this model considers the level of uncertainty, providing an interval instead of a single point for the true probability of a case being fraudulent. Therefore, the model can provide better accuracy of fraud prediction cases. Boukerche and Notare [34] suggest the use of NN within an intrusion detection system to capture the cloning mobile

phones. While there are few intrusion detection systems, many of them do ignore the phone cloning fraud, which can have huge consequences if not tackled. The study suggests the use of NN to ensure detection of any call that does not have a normal customer's behavioral pattern, control the imposters, and protects the revenue of the carrier by detecting the cloned phone within the same day of occurrence, rather than at the end of the month when the billing cycle is closed.

Alghawi [35] uses a classification algorithm to predict SIM box cases. Such classification algorithm is obtained as a linear combination of decision tree, functional tree, and RF. The evaluation criteria of such an algorithm are the ratio of false positives and false negatives. Results of the study show that when ran individually RF algorithm had the lowest false positives of 0.01% while providing higher false negatives of 16%. However, when compared to the latter, the functional tree algorithm yielded the lowest false negatives of 7% while providing only 0.07% false positives. To further improve the accuracy of the model, a multiple regression technique was applied which considered the prediction output of the three classifiers as predictor values and its linear combination as a criterion variable. Findings of the regression model suggested 99.95% accuracy while minimizing the false positives to 0.01% and false negatives to 9%. Bhowmik [36] suggests the use of naïve Bayesian classifier as a reliable metric when detecting fraud. The classifier is initially trained using simulated data, and based on the former predictions, fraud or legal instance is obtained. Results of the study suggest that such classifier performs well with an accuracy of 85.1% in predicted fraud cases. Moreover, naïve Bayes approach is easy as it can handle any missing values by omitting their probability and is also time efficient, as it only must run once. Yehya and Salhab [4] provide a comparative view between different ML models to detect IRSF fraud. The data was obtained from public test accounts, and the following models were compared namely: RF, logistic regression, SVM, gradient boosting, and naïve Bayes. All the classifiers were trained and tested using the same data and the results show that the worst performing models in terms of accuracy are logistic regression (0%) and naïve Bayes (64%) while the other three do perform very well (100%). After this, the three classifiers were evaluated based on the confusion matrix where SVM performed poorly in terms of true negatives and false positives. To decide which is the best performing model between RF and gradient boosting the feature importance analysis was applied. Findings of the study show that RF can provide wider information, with the minutes as a parameter being the top one, which is crucial in IRSF detection. Therefore, the best performing model for this fraud type is RF.

Estévez *et al.* [37] suggest the use of fuzzy logic and NN in detecting subscription fraud. The fraud types were divided into subscription fraudulent, otherwise fraudulent, insolvent and normal. As per the system architecture, this study is built upon one classification model which categorizes the subscribers to one of the four above-mentioned categories based on historical data, and one prediction module which uses as input new information about subscribers and detects fraudulent users. The latter model was trained and tested, and its performance was evaluated upon the ROC analysis. Results of the study suggest that the cluster model performed greatly with a 100% accuracy rate while the prediction one had an accuracy rate of 56.2%. Qayyum *et al.* [38] approve the use of NN to detect subscription telecom fraud. After training, the developed NN consists of 14 input neurons, 5 hidden layer neurons and 1 output layer neuron. Findings of the study suggested that the models performed with approximately 60 % accuracy. Moreover, Xiong [39] suggests the use of temporal method to detect only fraudulent cases by utilizing a graph-based model while using isolation forest with additional gross domestic product (GDP) features applied to detect IRSF. 80% of the data has been used for training and 20% for testing the models. Regarding the first temporal model, two definitions are established, namely T1 detects time intervals where fraud could have happened and T2 classifies if a single record is fraud or not. Study suggests that T1 detects the suspicious time slot through historical traffic and performs better than the naïve temporal models. Then the temporal model with definition T2 is compared with the isolation forest for detection accuracy and such evaluation is done through the ROC analysis. Findings of the study suggest that the combination of these two models performs with a high accuracy rate of 96.1%.

Jayasingh and Swain [40] suggest the use of NN in detecting fraud cases. After the model was trained, the performance of the rule diagnosis was created, which showcased the relationship between the share and the generalization level. Results show that there is some tradeoff between the rule number considered in the NN model and the confidence level. The more rules included, the better the model will perform, however the less general the rules are, the more the model performance will depend on the statistical variations of the fraud data. Findings of the study suggest that this model performs with 75.17% accuracy rate after decreasing the number of rules from 747 to 510. Moreover, Abidogun [41] proposes the use of SOM and LSTM recurrent NN models to predict the call pattern behaviors in an unsupervised learning approach. The LSTM RNN models are superior to the traditional RNN, as they overcome the dependency issue. On the other side, SOM are NN models that ensure visualization of high dimensional data while maintaining the important metric relationships of the primary data elements. Findings of the study suggest that while using the SOM model, information for the temporal nature of calls was lost in the process.

Moreover, different map sizes for different subscribers add a layer of complexity when it comes to comparing them, however, overall, the model can be used to provide insights for the variables dependencies. On the other hand, the LSTM RNN was trained 10 times using the nonparametric entropy optimization (NEO) algorithm, until there was no further improvement in the result, with an accuracy of 90%. Therefore, the study suggests that LSTM is a better clustering option than SOM.

Djomadji *et al.* [42] suggest the use of RF, SVM, and extreme gradient boosting (XGBoost) to detect SIM box cases. All the models were trained and tested using the same database, and the evaluation was done by the confusion matrix. Findings suggest that the SVM model performed poorly with 69% accuracy and the performance did not improve after training it. However, the RF performed with 92% accuracy after being trained again while the XGBoost model performed with 81% accuracy. Therefore, among the three ML models, the RF is the best performing one. Moreover, Olushola and Mart [43] consider the use of three ML models to detect fraud cases, such as RF, XGBoost, and logistic regression. Findings of the study suggest that different models outperform the others in different areas. For instance, combining RF and XGBoost provides a model with better accuracy. However, logistic regression on its own is more effective at identifying certain fraud types. Moreover, feature engineering is crucial to improve the model's performance since the beginning; such a thing requires to have a deep business understanding to convert the fraud cases into useful features for ML models. Lastly, considering the nature of fraud, it is a must to ensure real time monitoring and prevention of fraud cases. Sahin [44] conducts a study using test calls to detect over-the-top (OTT) bypass fraud. Two separate test call campaigns were held where the first utilizes a commercial test call generation (TCG) platform with big network coverage while the second uses a smaller dedicated call test platform built for this purpose. In the former, 1016 test calls were made using TCG platform from different network operators in 50 countries. OTT fraud cases were detected in 90% of the countries and 62% of operators, while 40% of the test calls were bypassed, which means that OTT bypass is high towards this TCG platform. Findings of the study suggest that with 95% confidence, the OTT bypass rate does not change regardless of whether the user is making domestic (36%) or roaming calls (37%). Moreover, the study uses the integrated services digital network user part (ISUP) logs from the mobile operator to create a partial map of routes starting from 7 mobile operators in United Kingdom which helps in identifying the bypassing operators, however, considering the costs of TCG platform such analysis was not conducted. However, the other test campaign is built on Android phones monitored via Wi-Fi connection. Nevertheless, collecting information from both the calling and called party. Each phone was placed in one European country where the originating operator would be a big sized mobile network operator (MNO). For each call, the parameters obtained are network name, call start time, call ring time, and call end time. Incoming call logs from Android's database and OTT are collected which provide parameters such as incoming call time, call type, called number ID. Findings of the study suggest that while generating calls for 2 months every day on an hourly basis, 6 out of 8 countries observed OTT bypass with rates from 42% to 83%.

Kilinc [45] suggests the use of ML classifiers such as decision tree, Gaussian naïve Bayes, adaptive boosting (AdaBoost) to detect telecom fraud cases. Initially, the data was labeled using the local outlier factor model, according to which 6.7% of the calls were considered as fraudulent users. Such fraudulent data was used to train all three ML classifiers. Lastly, a mixed model was created by using the average of the three individual supervised models. The latter model was trained by 70% of the dataset used. Findings of the study suggest that the best performing model is decision tree with 93% accuracy rate. Zhu *et al.* [46] adopt several ML classifiers to develop a scam message alert. Data set was obtained from an open-source message dataset from GitHub, out of which 70% was used for training the ML modes and the remaining 30% for testing. The chosen models were decision tree, SVM, logistic regression, and naïve Bayes which performed with an accuracy rate of 98.72%, 94.23%, 91.00%, and 96.28%, respectively in detecting fraudulent messages. Out of all these models, the decision tree one performed the best; however, its accuracy increases with the increase of n_estimators and then starts to fall. Therefore, the n_estimator for which the model obtained the highest accuracy was 400 and this was the chosen number for the final model. Moreover, Ezawa *et al.* [47] suggest a goal-oriented algorithm for creating Bayesian network in detecting uncollectible in telecom risk management data. The study uses different classifiers of Bayesian model, such as advanced pattern recognition and identification (APRI), goal-oriented K2, independent and goal-oriented conditional independence and Bayesian learning (CB). Such models are compared and evaluated against each other based upon the ROC analysis. Such analysis suggests that APRI, the goal-oriented model, has a way better performance when compared with all the other models, followed by the independent model and then K2 and CB which perform relatively poorly. However, when building the goal-oriented K2 and goal-oriented CB and comparing them with APRI model, the ROC analysis suggests that even though the latter model still has the best performance, the two other models' performance has improved significantly when compared to before. Therefore, this study suggests that when creating a Bayesian model, it must be adjusted as per the specific goal to achieve better performance.

Asogwa *et al.* [48] provide a theoretical framework of NN application for detection of telecommunication fraud. The study touches upon the definition of telecom fraud, its consequences, fraud types and detection techniques. Moreover, the study focuses on the use of artificial NNs on detecting telecommunication fraud from the early 1960s up to date, by explaining how to use the data to train and test a NN to efficiently detect fraudulent and non-fraudulent users. Such article analyzes the case of a NN-based fraud implementation tool, Minotuar, which was a mix of AI models and traditional computing techniques. Findings of the study suggest that only in three months of implementation the fraud loss per unit was reduced by 40% and that combination of neural, rule based, and case-based technologies are far better in fraud detection than traditional systems. Onuodu and Nnaa [49] present the use of forward and backward rule-based ANN to improve an existing platform for smart card and telecommunication fraud detection in Nigeria. Through ANN, improvement of all the components in the existing system was made including the following: intelligent agent, security measures, customer, customer bank database, credit card transaction database, and fraud detection database. Moreover, using the forward and backward rule-based ANN, the proposed system was able to not only detect in real time but also predict in advance any fraudulent users on the smartcard and telecom services, blocking them from using the service. A comparative analysis between the old and newly proposed system was conducted, where the evaluation criteria were speed in processing input validation details (SPIVD), speed in detecting and blocking fraudulent attempts (SDBFA), cross platform compatibility (CPA), model efficiency (ME), and cost benefit analysis (CBA). Results of such analysis convey that the newly proposed model is superior in all the criteria and performing with 94% accuracy rate towards 65% of the old model.

Bhavani *et al.* [50] combine the use of naïve Bayes and LSTM RNN to provide an advanced fraud prediction model for mobile fraud. The former model was trained to obtain some benchmark for performance evaluation, based on which the study applied more advanced models such as LSTM. The latter model was designed, trained and adjusted to detect complex behavior patterns of fraudulent cases in call messages. The study conducts a comparison of both models based on accuracy, precision, recall, and F1-score, highlighting the strengths and weaknesses of each. Lastly, LSTM was trained 10 times on a separate data set from the initial one, proving its ability to learn and generalize new data and compare it against the actual labeled cases. Findings of the study suggest that this model performs with 99.89% accuracy in the training sample and 97.20% accuracy in the testing one. Hu *et al.* [51] suggest an interesting use of augmented graph neural network (GNN) by mixing reinforcement and ensemble learning to detect mobile fraud, while tackling two main problems associated with it such as graph imbalance and over-smoothing. To tackle the former issue, reinforcement learning based-neighbor sampler is used while for the latter, AdaBoost for ensemble learning of the GNN models is applied. All the training of the model is supervised utilizing a class balanced focal loss function and then it is tested in two real world telecom fraud datasets to observe its performance. Findings of the study suggest that the augmented GNN model outperforms other existing graph-based models in both datasets while attaining an accuracy rate of 91.55% and 92.5%, respectively. Mawgoud *et al.* [52] suggest a combination of classification methods and NN to detect Wangiri, a specific telecommunications fraud. From the dataset used, 70% are normal users and 30% fraudulent ones. In this paper, ANN, with three layers was applied and results of the model were evaluated using the ROC map. Findings of the study suggest that this model performs relatively well with a 90.6% accuracy rate on training and 85% on testing. Lastly, Wahid *et al.* [53] present a new telecom fraud detection approach by using a neural factorization autoencoder, which itself combines neural factorization machine (NFM) and autoencoders. Such components enable the model to register user behavioral patterns and learn from the new raw data, which continuously improved the detection of the model. The trained model was tested in a real-world data set encompassing a huge amount of data. Moreover, the study suggests that memory length and threshold do impact the model's performance. In other words, the best performance of the model is obtained with a memory length of 4,096 and any increase after that does decrease the performance, while for the threshold the best performance was reached at 0.0001, and any increase after that also negatively affected the model. Findings of the study suggest that the non-deterministic finite automaton (NFA) model with memory length = 4,096, iterations = 750, and threshold = 0.001 performed the best with 95.45% accuracy rate.

4. CONCLUSION

This paper was focused on detecting telecom fraud using AI and ML. It provided an overview of main strategies and methods used by the authors. 66% of the papers used supervised strategy, using labeled dataset while 12% used unsupervised strategy, utilizing unlabeled data, and 18% used both supervised and unsupervised strategies. Moreover, only 2% of the papers used knowledge-based strategies and the last remaining 2% used a combination of supervised, unsupervised and knowledge-based strategies. Regarding the hardware and software use, 88 % of the papers reviewed used software analysis while the remaining 12% used both software and hardware. The main difference on the papers were the algorithms/classifiers used for

fraud detection. Majority of the papers used one of the following models such as ANN, SVM, or decision tree as the best one for telecom fraud prediction. However, only 10% of papers used visual models in their approaches, such as SOM and GNN. As per the accuracy of the papers, 76% of them did provide the accuracy while the remaining 24% did not.

ACKNOWLEDGMENTS

We want to thank the University of Wollongong in Dubai (UOWD) for providing the grant for this research work.

FUNDING INFORMATION

This work was supported by the University of Wollongong in Dubai (UOWD) 2024 internal grant no RC048.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Soly Mathew Biju	✓	✓		✓		✓	✓			✓		✓	✓	✓
Sindi Rryta		✓		✓	✓	✓		✓	✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

No personal information of any individual has been used or disclaimed in this work.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] Cambridge Dictionary, "Meaning of fraud in English," *dictionary.cambridge.org*, 2023. Accessed: Mar. 24, 2025. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/fraud
[2] D. Daly, "Top fraud trends and predictions for 2025 – and how will the industry respond?," *datavisor.com*, 2025. Accessed: Mar. 24, 2025. [Online]. Available: https://www.datavisor.com/blog/fraud-trends-predictions-2025
[3] Association of Certified Fraud Examiners, "Report to the Nation-2020 global study on occupational fraud and abuse," *Association of Certified Fraud Examiners, Inc.*, 2020. [Online]. Available: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf
[4] B. A. Yehya and N. Salhab, "Telecommunications fraud machine learning-based detection," in *2023 4th International Conference on Data Analytics for Business and Industry*, Oct. 2023, pp. 656–661, doi: 10.1109/ICDABI60145.2023.10629612.
[5] M. R. AlBougha, "Comparing data mining classification algorithms in detection of SIM box fraud," *M.S thesis*, Department of Information Systems, St. Cloud State University, Minnesota, United States, 2016.
[6] R. Sallehuddin, S. Ibrahim, A. M. Zain, and A. H. Elmi, "Detecting SIM box fraud by using support vector machine and artificial neural network," *Jurnal Teknologi*, vol. 74, no. 1, Apr. 2015, doi: 10.11113/jt.v74.2649.
[7] A. Krenker, M. Volk, U. Sedlar, J. Bešter, and A. Kos, "Bidirectional artificial neural networks for mobile-phone fraud detection," *ETRI Journal*, vol. 31, no. 1, pp. 92–94, Feb. 2009, doi: 10.4218/etrij.09.0208.0245.
[8] P. Saravanan, V. Subramaniyaswamy, N. Sivaramakrishnan, M. A. Prakash, and T. Arunkumar, "Data mining approach for subscription-fraud detection in telecommunication sector," *Contemporary Engineering Sciences*, vol. 7, pp. 515–522, 2014, doi: 10.12988/ces.2014.4431.
[9] G. Wassie, "Subscription fraud detection using autoencoder in case of ethio telecom," *Journal of Advance Research in Social Science and Humanities*, vol. 10, no. 7, pp. 11–23, Oct. 2024, doi: 10.61841/tp4k9012.

[10] H. Grosser, P. Britos, and R. G.-Martínez, "Detecting fraud in mobile telephony using neural networks," in *Innovations in Applied Artificial Intelligence*, Berlin, Heidelberg: Springer, 2005, pp. 613–615, doi: 10.1007/11504894_85.
[11] A. H. Elmi, S. Ibrahim, and R. Sallehuddin, "Detecting SIM box fraud using neural network," in *IT Convergence and Security 2012*, Dordrecht: Springer, 2013, pp. 575–582, doi: 10.1007/978-94-007-5860-5_69.
[12] M. Sanver and A. Karahoca, "Fraud detection using an adaptive neuro-fuzzy inference system in mobile telecommunication networks," *Journal of Multiple-valued Logic and Soft Computing*, vol. 15, no. 2, pp. 155–179, 2009.
[13] B. M. Thaddeus, M. Muhammad, Y. M. Malgwi, and E. T. Martin, "Sim-boxing fraud detection system using artificial neural network," *International Journal of Development Mathematics*, vol. 1, no. 4, pp. 201–213, Dec. 2024, doi: 10.62054/ijdm/0104.16.
[14] C. S. Hilas and P. A. Mastorocostas, "An application of supervised and unsupervised learning approaches to telecommunications fraud detection," *Knowledge-Based Systems*, vol. 21, no. 7, pp. 721–726, Oct. 2008, doi: 10.1016/j.knosys.2008.03.026.
[15] H. Li *et al.*, "A machine learning approach to prevent malicious calls over telephony networks," in *2018 IEEE Symposium on Security and Privacy*, May 2018, pp. 53–69, doi: 10.1109/SP.2018.00034.
[16] A. H. Elmi, R. Sallehuddin, S. Ibrahim, and A. M. Zain, "Classification of SIM box fraud detection using support vector machine and artificial neural network," *International Journal of Innovative Computing*, vol. 4, no. 2, pp. 19–27, 2014.
[17] P. Barson, S. Field, N. Davey, G. McAskie, and R. Frank, "Detection of fraud in mobile phone networks," *ResearchGate*, 1996.
[18] I. Murynets, M. Zabarankin, R. P. Jover, and A. Panagia, "Analysis and detection of SIM box fraud in mobility networks," in *IEEE Conference on Computer Communications*, Apr. 2014, pp. 1519–1526, doi: 10.1109/INFOCOM.2014.6848087.
[19] H. M. Marah, O. M. Elrajubi, and A. A. Abouda, "Fraud detection in international calls using fuzzy logic," in *International Conference on Computer Vision and Image Analysis Applications*, Jan. 2015, pp. 1–6, doi: 10.1109/ICCVIA.2015.7351891.
[20] F. N. Ogwueleka, "Fraud detection in mobile communications networks using user profiling and classification techniques," *Journal of Science and Technology*, vol. 29, no. 3, pp. 31–42, 2009, doi: 10.4314/just.v29i3.50052.
[21] F. O. Aranuwa, "Hybridized intelligent data analysis model for fraud detection in mobile communication networks," *Academia Journal of Scientific Research*, vol. 1, no. 5, pp. 082–089, 2013.
[22] Y. Rebahi, R. Ruppelt, M. Nassar, and O. Festor, "SCAMSTOP: a platform for mitigating fraud in VoIP environments," in *Network and Traffic Engineering in Emerging Distributed Computing Applications*, ResearchGate, 2011, pp. 302–325, doi: 10.4018/978-1-4666-1888-6.ch012
[23] J. Hollmén, "User profiling and classification for fraud detection in mobile communications networks," *Ph.D. dissertation*, Department of Computer Science and Engineering, Aalto University, Espoo, Finland, 2000.
[24] Y. Moreau, B. Preneel, P. Burge, J. S.-Taylor, C. Stoermann, and C. Cooke, "Novel techniques for fraud detection in mobile telecommunication networks," *RersearchGate*, 1998.
[25] M. Taniguchi, M. Haft, J. Hollmen, and V. Tresp, "Fraud detection in communication networks using neural and probabilistic methods," in *1998 IEEE International Conference on Acoustics, Speech and Signal Processing*, 1998, pp. 1241–1244, doi: 10.1109/ICASSP.1998.675496.
[26] J. Hollmén and V. Tresp, "Call-based fraud detection in mobile communication networks using a hierarchical Regime-switching model," in *1998 conference on Advances in neural information processing systems II*, 1998, pp. 889-895.
[27] J. Hollmén, V. Tresp, and O. Simula, "A self-organizing map for clustering probabilistic models," in *9th International Conference on Artificial Neural Networks*, 1999, pp. 946–951, doi: 10.1049/cp:19991234.
[28] K. G. D. C. Kehelwala, "Real-time fraud detection in telecommunication network using call pattern analysis," *M.S. thesis*, Department of Computer Science and Engineering, University of Moratuwa, Moratuwa, Sri Lanka, 2017.
[29] M. Kashir and S. Bashir, "Machine learning techniques for SIM box fraud detection," in *2019 International Conference on Communication Technologies*, Mar. 2019, pp. 4–8, doi: 10.1109/COMTECH.2019.8737828.
[30] J. Li, C. Zhang, and L. Jiang, "Innovative telecom fraud detection: a new dataset and an advanced model with RoBERTa and dual loss functions," *Applied Sciences*, vol. 14, no. 24, Dec. 2024, doi: 10.3390/app142411628.
[31] Q. Zhao, K. Chen, T. Li, Y. Yang, and X. Wang, "Detecting telecommunication fraud by understanding the contents of a call," *Cybersecurity*, vol. 1, no. 1, Dec. 2018, doi: 10.1186/s42400-018-0008-5.
[32] S. Subudhi and S. Panigrahi, "Use of possibilistic fuzzy C-means clustering for telecom fraud detection," in *Computational Intelligence in Data Mining*, Singapore: Springer, 2017, pp. 633–641, doi: 10.1007/978-981-10-3874-7_60.
[33] F. Daniel, "Bayesian and Dempster-Shafer models for combining multiple sources of evidence in a fraud detection system," Apr. 2021, *arXiv: 2104.07440*.
[34] A. Boukerche and M. S. M. A. Notare, "Behavior-based intrusion detection in mobile phone systems," *Journal of Parallel and Distributed Computing*, vol. 62, no. 9, pp. 1476–1490, Sep. 2002, doi: 10.1006/jpdc.2002.1857.
[35] N. Alghawi, "A study on SIM box or interconnect bypass fraud," *M.S. thesis*, Department of Informatics, The British University in Dubai, Dubai, UAE, 2019.
[36] R. Bhowmik, "Data mining techniques in fraud detection," *Journal of Digital Forensics, Security and Law*, vol. 3, no. 2, 2008, doi: 10.15394/jdfsl.2008.1040.
[37] P. A. Estévez, C. M. Held, and C. A. Perez, "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks," *Expert Systems with Applications*, vol. 31, no. 2, pp. 337–344, Aug. 2006, doi: 10.1016/j.eswa.2005.09.028.
[38] S. Qayyum, S. Mansoor, A. Khalid, Khushbakht, Z. Halim, and A. R. Baig, "Fraudulent call detection for mobile networks," in *2010 International Conference on Information and Emerging Technologies*, 2010, pp. 1–5, doi: 10.1109/ICIET.2010.5625718.
[39] C. Xiong, "Telecom fraud detection using machine learning," *M.S thesis*, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, 2022.
[40] S. K. Jayasingh and A. K. Swain, "Neural network in fraud detection," in *International Conference on Industrial Application of Soft Computing Techniques*, 2011, pp. 1-8.
[41] O. A. Abidogun, "Data mining, fraud detection and mobile telecommunications: call pattern analysis with unsupervised neural networks," *M.S thesis*, Department of Computer Science, University of the Western Cape, Cape Town, 2005.
[42] E. M. D. Djomadji, K. I. Basile, T. T. Christian, F. V. K. Djoko, and M. E. Sone, "Machine learning-based approach for identification of SIM box bypass fraud in a telecom network based on CDR analysis: case of a fixed and mobile operator in Cameroon," *Journal of Computer and Communications*, vol. 11, no. 02, pp. 142–157, 2023, doi: 10.4236/jcc.2023.112010.
[43] A. Olushola and J. Mart, "Fraud detection using machine learning," *ScienceOpen Preprints*, Jan. 2024, doi: 10.14293/PR2199.000647.v1.
[44] M. Sahin, "Understanding telephony fraud as an essential step to better fight it," *Ph.D. thesis*, Department of Digital Security, TELECOM ParisTech, Paris, France, 2017.
[45] H. H. Kilinc, "A case study on fraudulent user behaviors in the telecommunication network," *Electrica*, vol. 21, no. 1, pp. 74–84, Jan. 2021, doi: 10.5152/electrica.2021.20050.

[46] C. Zhu *et al.*, "Building of safer urban hubs: insights from a comparative study on cyber telecom scams and early warning design," *Urban Governance*, vol. 3, no. 3, pp. 200–210, Sep. 2023, doi: 10.1016/j.ugj.2023.05.004.
[47] K. J. Ezawa, M. Singh, and S. W. Norton, "Learning goal oriented Bayesian networks for telecommunications risk management," in *Thirteenth International Conference on International Conference on Machine Learning*, 1996, pp. 139–147.
[48] E. C. Asogwa, O. C. C., I. Ezeugbor, and C. C. Ngene, "Application of artificial neural networks for the detection of telecommunication fraud," *International Journal of Scientific & Engineering Research*, vol. 11, no. 6, pp. 551–557, 2020.
[49] F. E. Onuodu and S. B. Nnaa, "An enhanced fraud detection model using neural networks for telecommunications and smart cards in Nigeria," *London Journal of Research in Computer Science and Technology*, vol. 20, no. 2, 2020.
[50] B. D. Bhavani, U. Nikitha, P. Nandini, and N. R. Gogu, "Artificial intelligence based fake or fraud phone calls detection," *Journal for Educators, Teachers and Trainers,* vol. 15, no. 5, pp. 318–327, 2024, doi: 10.47750/jett.2024.15.05.31.
[51] X. Hu, H. Chen, H. Chen, X. Li, J. Zhang, and S. Liu, "Mining mobile network fraudsters with augmented graph neural networks," *Entropy*, vol. 25, no. 1, Jan. 2023, doi: 10.3390/e25010150.
[52] A. A. Mawgoud, A. A.-Talleb, and B. S. Tawfik, "A holistic neural networks classification for Wangiri fraud detection in telecommunications regulatory authorities," in *Advanced Machine Learning Technologies and Applications*, Cambridge: Springer, 2021, pp. 175–183, doi: 10.1007/978-3-030-69717-4_19.
[53] A. Wahid, M. Msahli, A. Bifet, and G. Memmi, "NFA: a neural factorization autoencoder based online telephony fraud detection," *Digital Communications and Networks*, vol. 10, no. 1, pp. 158–167, Feb. 2024, doi: 10.1016/j.dcan.2023.03.002.

APPENDIX

Table 1. Summary of all the papers reviewed

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[4]	Use of ML to detect IRSF	Supervised	Software	-	RF, logistic regression, SVM, gradient boosting, and naïve Bayes	29,716 samples of IRSF and 45,008 samples as legitimate users	100%, 0%, 100%, 100%, and 64%	Data set obtained from public test accounts	Investigate other fraud types by applying deep learning techniques for better performance
[5]	Use of data mining classification algorithms to detect SIM box	Supervised	Software	Personal laptop	Boosted trees classifiers, SVM, logistic classifiers, and NN.	100,000 subscribers	91%	One week's CDRs from one MNO	Use of methods such as TCG together with the data mining algorithms to increase efficiency
[6]	Use of ANN, SVM to detect SIM box	Supervised	Both	-	ANN, SVM, and RF	234,324 CDRs by 6,416 subscribers	98.69% and 99.06%	Offline dataset of MNO's customer DB	Use of hybridization between SVM and other computational approaches to improve SVM model
[7]	Use of Bi-ANN to detect mobile phone fraud based on the call duration parameter	Supervised	Software	MATLAB	Bi-ANN	1,082,588 calls	90%	Slovenian MNO DB	Predict other parameters to create a complete mobile phone detection system
[8]	Use of a probability-based model such as naïve Bayesian to predict subscription fraud	Supervised	Software	Dell core i7 laptop computer	Naïve Bayesian classifier	10 records from a sample dataset	-	-	Apply other probability-distribution algorithms with better accuracy
[9]	Use of deep neural autoencoder and CNN-LTSM models	Supervised	Software	-	Neural autoencoder and CNN-LTSM algorithms	104,8576 records for voice, SMS, and data, respectively	98.95%	Switch of ethiotelecom MSC DB	Use of generative adversarial network (GAN)
[10]	Use of neural networks to detect mobile fraud	Supervised	Software	-	NN algorithm		-	-	Use of differential analysis rather than absolute analysis to provide insights about the user behavior

Table 1. Summary of all the papers reviewed *(continued)*

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[11]	Use of ANN in detecting SIM box fraud	Supervised	Software	-	NN algorithm	234,324 call records made by 6414 subscribers from one Cell ID collected for two months	98.71%	-	Use of SVM in SIM box prediction besides the ANN
[12]	Use of data mining techniques to determine the best one for telecom fraud detection	Supervised	Software	-	Ridor, PART, OneR, Nnge, decision table, conjunction rules, AD tree, IB1, Bayesnet, and ANFIS	Call data of 290 subscribers for 92 days	98.33%	-	Such model must be trained to telecom networks, and then used in operation for immediate fraud detections
[13]	Use of ANN to detect SIM box	Supervised	Software	-	ANN algorithm	32810 calls made by 6563 subscribers	80.01%	-	Data set of CDRs from a real NVO's DB
[14]	Use of machine learning to detect IRSF	Supervised and unsupervised	Software	-	RF, logistic regression, SVM, gradient boosting, and naive Baye	-	99%, 50%, 99%, 99%, and 72%	-	Investigate other fraud types and integrate deep learning techniques to improve the accuracy of the model
[15]	Use of machine learning to prevent fraudulent calls in phone calls	Supervised	Both	-	SVM, logistic regression, ANN, RF, and XGBoost	9 billion call CDRs during a period of three months	90%	Touch Pal App	Mitigating spoofing scenarios in the future work
[16]	Use of SVM and ANN to detect SIM box	Supervised	Software	-	SVM and ANN algorithms	234,324 calls made by 6415 subscribers from one Cell-ID during a period of two months	98.9%	Data set of CDRs from a real NVO's DB	Use hybridization between SVM and particle swarm optimization (PSO) to further improve the model's performance
[17]	Use of MLP network in detecting mobile phone frauds	Supervised	Software	-	MLP network	100 simulated calls	92.5%	-	Use of unsupervised Self Organizing Map neural model
[18]	Use of ML classifiers to detect SIM box	Supervised	Software	-	Decision tree, functional tree, and RF model	Data set of 500 fraudulent IMEIs and 93000 legitimate IMEI accounts	99.5%	Data set of automated CDRs from a tier-1 mobile operator in United States	
[19]	Use of fuzzy logic in detecting SIM box	Supervised	Software	Computer	Fuzzy logic membership function	Data set with 65 fields, size not mentioned	-	Data set from Almandar Aljadid MNO in Lybia	Add more detection patterns and adjust their weight in accordance with their importance and contribution to the model's performance

Table 1. Summary of all the papers reviewed *(continued)*

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[20]	User of user profiling and classification methods to detect mobile communication fraud	Supervised and unsupervised	Software	-	NN and rule-based model	Data set of 180 subscribers with fraudulent behavior during a period of 75 days	97%	Real life data set from one MNO's offline DB	-
[21]	Use of hybridized data analysis model to detect fraud in mobile communication networks	Supervised and unsupervised	Software	-	Differentials and absolute analysis, user profiling, and classification analysis	Not provided	89%	Data set was obtained from the billing toll tickets of an MNO	Conduct further research to cover subscription fraud or velocity traps against this proposed method
[22]	Use of unsupervised methods to detect SIM box	Unsupervised	Software	-	Hierarchical clustering, static clustering, dynamic clustering, K-means, SVM, SOM, and NN	Data set of VoIP providers in SCAMSTOP platform during a month time	-	Data set obtained from the SCAMSTOP platform	Conduct further research to make the platform more scalable and monitor clustering membership for a long time to be able to detect malicious cluster migration
[23]	Use of profiling and classification for fraud detection in mobile communications networks	Supervised and unsupervised	Software	-	NN, probabilistic models, Bayesian networks, and EM algorithm	Dat set of 304 fraudulent subscribers for 92 days and a data set of normal subscribers for 49 days	98%-99%	Data set from real MVO's DB	Collect large data sets that can be used for training models, use of kernel-based approaches, and apply transferability of models to different networks
[24]	Use of a combined approach between absolute and differential usage to detect mobile communications networks	Supervised, unsupervised, and knowledge based	Software	-	Rule based approach and NN	-	-	-	Conduct research work that uses unsupervised learning methods where fraudulent data is distinct enough from regular data, supervised methods where fraudulent data is labeled and in a significant amount
[25]	Use of neural and probabilistic methods to detect communication networks fraud	Supervised and unsupervised	Software	-	NN, Gaussian model, and Bayesian network	Data set of 303 fraudulent users and 2100 of normal ones	85%, 70%, and 85%	Data set from toll tickets of a MNO's billing system	Combine all three presented models to improve the performance of the model

Table 1. Summary of all the papers reviewed *(continued)*

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[26]	Use of a hierarchical regime switching model to detect call-based fraud	Unsupervised	Software	-	EM algorithm, Filtering, and smoothing method	Data set of 600 accounts of legitimate users and 304 accounts of fraudulent users obtained for 49 and 92 days, respectively	97.4% and 93.4%	Data obtained from a real MNO's DB	Use more than one fraud model for different fraud cases and different user models for different user profiles
[27]	Use of a SOM for clustering probabilistic models to create user profiling in telecommunications network	Unsupervised	Software	-	SOM algorithm (NN)	Data set of 600 accounts of legitimate users and 304 accounts of fraudulent users obtained for 49 and 92 days, respectively	-	Data obtained from a real MNO's DB	Cluster models using the latent variables such as hidden Markov models or mixture models
[28]	Use of call pattern analysis to detect fraud in real time	Unsupervised	Both	16 cores × Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz	CEP and BAM	Training data set of 21,017,737 subscribers and testing data set of 12,964,108 subscribers	99.9%	Data set from a service provider	Include the ML models such as NN and Tree based classifier on derived future set
[29]	Use of ML techniques to detect SIM box fraud	Supervised	Software	-	ANN and SVM	Data set of 8,695 legitimate subscribers and 50 fraudulent ones	99.87% and 99.24%	Data obtained from a real MNO's DB	-
[30]	Use of an innovative telecom fraud text detection model	Supervised	Software	-	Advanced model with RoBERTa and dual loss functions	A data set of 12,506 data records	97.65%, 98.10%, and 93.69%	Public data set obtained from Github	Expand the data set to cover more telecom fraud text categories, optimize the model's complexity to reduce the need for training, and consider alternative model architectures to increase performance
[31]	Understanding the call contents to detect telecommunication fraud	Supervised	Both	-	Logistic regression, NN, and decision tree	A dataset of 12,368 test samples from Sina Weibo and 3,234 test samples from Baidu Normal data from THUCNews China	98.53%	Data was obtained from Sina Weibo and Baidu, the largest open communication platform and search engine in China	Use advanced voice recognition technology in the future that will be able to detect correct key words even when spoken with a certain dialect other than Mandarin

Table 1. Summary of all the papers reviewed *(continued)*

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[32]	Use of PFCMs clustering to detect telecom fraud	Unsupervised	Software	MATLAB 8.3 on a 2.40 GHzi5-4210U CPU system	PFCM clustering algorithm	A data set of Call, SMS, Data records of 106 subscribers for 9 months	93.03%	-	-
[33]	Combining multiple sources of evidence in fraud detection	Supervised and unsupervised	Software	-	Bayesian and Dempster-Shafer models	A data set of 30 users including 7 fraudulent users	50.4%, and 85.71%	-	Research how to weigh ML models or specific rules
[34]	Create an intrusion detection system for mobile phone networks	Supervised	Software	-	NN	-	-	Data set assumed to be obtained from the client DB using the intrusion detection system	Enhance the SSTCC system and SETWeb module by using the Wireless Application Protocol, and investigating the use of servlets to increase the security of the system
[35]	Use of ML models to detect SIM box	Supervised	Software	-	Classification algorithm as a linear combination of decision tree, functional tree, and RF	Data set of 93,500 subscribers where 500 are SIM box cases	99.95%	Data set form a mobile operator in UAE	Include ML models such as NN or Tree based classifiers to predict SIM box cases.
[36]	Use of data mining techniques in fraud detection	Supervised	Software	-	Naïve Bayesian	Simulated data set of 7000 users	78%	-	-
[37]	Use of fuzzy rules and NNs to detect subscription fraud in telecommunications	Supervised and unsupervised	Software	-	Fuzzy logic and NN	Data set of 10,000 real subscribers	56.2%	Data set obtained from a big MNO in Chile	Extend the techniques applied in this model to subscription fraud in mobile communication and other markets
[38]	Use of neural network to detect subscription fraud	Supervised	Software	-	NN	107,050 CDRs from 300 unique callers obtained in 4 months. Out of 300, 75 were fraudulent users	60%	-	All the mobile operators in Pakistan should adopt the neural networks when detecting fraud
[39]	Use of data mining models to predict IRSF fraud	Supervised	Software	-	GNN, gated recurrent unit (GRU), and time-independent isolation forest	Data pushed every two minutes per country for December 2020 and March, July 2021	96.1%	Real data from Sinch DB	Work with domain experts using manual detection methods to filter out the fraudulent cases
[40]	Use of NN in fraud detection	Supervised	Software	-	NN	5,850 fraud transactions and 542,8585 legal transactions	75.17%	-	-
[41]	Use of unsupervised NN to detect	Unsupervised	Software	-	SOM, LSTM, and RNN	227,318 CDRs from 500 masked subscribers for 6 months	-	-	Train LTSM RNN with other functions, Use LTSM RNN for predictive data mining tasks

Table 1. Summary of all the papers reviewed *(continued)*

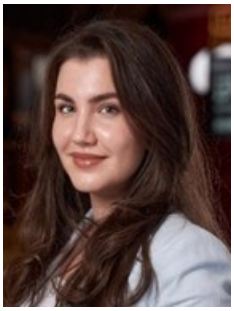
Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[42]	Use of ML to detect SIM box bypass fraud	Supervised	Software	-	RF, SVM, and XGBoost	60,000 call lines	92%	-	Combine ML approaches with AI and deep learning modules
[43]	Use of ML to detect fraud	Supervised	Software	-	Decision trees, RF, and NN	284,807 data entries	-	Data set obtained from Kaggle	-
[44]	Understand and detect the OTT fraud	Supervised	Both	Android phones	Partial map route	15,872 test calls over 8 months	-	Data obtained from a real TCG platform and a self-build TCG platform using Android mobiles	Conduct study regarding lack of caller ID authentication
[45]	Detect telecom fraudulent behavior on a case study with high call traffic	Supervised and unsupervised	Both	Nova V-GATE	Decision tree, Gaussian naïve Bayes, and AdaBoost classifier, and mixed model	420,000 calls, from which 300,000 international calls were collected for 4 months	93%, 88%, 93%, and 89%	Real data set obtained from an MNO in Turkey	Use of ML study integration with fraud detection and prevention system
[46]	Use of ML models to create a message scam alert model	Supervised and unsupervised	Software	-	Decision tree, SVM, logistic regression, and naïve Bayes	2,747 real message records	98.72%, 94,23%, 91,08%, and 96.28%	Data obtained from news and open-source message datasets of GitHub	Obtain more extensive data from several sources and improve comparison methods and predictive analysis
[47]	Learn to create a goal-oriented Bayesian network towards telco risk management	Supervised	Software	The APRI system developed at AT&T bell laboratories	APRI, K2, and CB	Training set of 68,138 collectible and 6,663 uncollectible accounts described by 21 parameters testing set 94,004 collectibles and 10,481 uncollectible	-	-	Use the Gayesian network model by meeting the exact goal of the intended model for best performance
[48]	Application of ANN for the detection of telecommunication fraud	Knowledge based	Software	-	ANN	-	-	-	-
[49]	Create an advanced platform to detect smartcard and telecommunication fraud using NN	Supervised	Software	-	ANN	-	94%	-	Include all types of fraud besides the subscription one, use a larger database for more efficient results and introduce a hybrid model using neural network and decision tree
[50]	Use of AI and ML to detect mobile fraud	Supervised	Software	-	Naïve bayes and LSTM	3,565 real life samples for training and 992 for testing the model	99.89%	-	-

Table 1. Summary of all the papers reviewed *(continued)*

Paper	Aim of study	Strategy	Hardware/ software	Devices used	Algorithms	Sample size	Accuracy	Database	Future study proposed
[51]	Use of augmented GNN to improve imbalance and over-smoothing problems in detecting telecom fraud detection	Supervised	Software	-	GNN	Random samples from two telecom fraud datasets used in the paper	91.5% and 92.5 %	-	Use augmented GNN to predict other types of fraud such as social fraud, financial fraud and cyber security where the data imbalance issue exists
[52]	Use of neural networks to detect Wangiri fraud in telecommunications regulatory authorities	Supervised	Software	-	AI NN and MLP	Data set of 1000 samples	90.6%	ISTAT dataset available in telecom field	Use a combination of ML and data processing to improve diagnostic accuracy of telecom frauds
[53]	Use of a neural factorization autoencoder to detect telephone fraud	Supervised	Software	-	NFM and AE	670,211 CDRs	95.45%	Data set of call records data from a real-world DB	Apply a factorization autoencoder in detecting other telecommunications fraud such as MTRA and Smishing

BIOGRAPHIES OF AUTHORS

Dr. Soly Mathew Biju CEng CITP FBCS FHEA is an associate professor at the University of Wollongong in Dubai. She is the program director (aka discipline leader) for Computer Science and head of the Global Health and wellbeing cluster at University of Wollongong in Dubai. She has over 25 years of work experience in academia and IT industry. Her research interests are in machine learning, sensors applications, IoT and AI application in designing systems. She is a chartered engineer and fellow higher education academy. She is an author and editor of several books and holds multiple patents. She is a keynote speaker at various international conferences. In addition, she holds mastery-level professional certifications, including IBM certified AI analyst, IBM IoT cloud developer, Security intelligence engineer, and IBM cloud application developer. She can be contacted at email: solymathewbiju@uowdubai.ac.ae.



Sindi Rryta is a revenue assurance and fraud management team lead at a vendor based in Dubai, United Arab Emirates. She has a bachelor's degree in Web and Mobile Computing and Economics and Statistics from Rocherster Institute of Technology, where she graduated with high honors and published her master thesis as her first research. She also holds a master's degree in IT Management from the University of Wollongong in Dubai, where she graduated as the top scorer in the School of Computer Science. As a new research enthusiast, her main areas of interest are machine learning, business assurance, and fraud management. She can be contacted at email: rrytasindi@gmail.com.