A Supervised Machine Learning Approach for Telecom Fraud Detection Using IPDR Data

Divya Sharma[1], Satnam Kaur*[1] , Mamta Dabra[1] and Divya Bansal[1]
[1]Department of Computer Science & Engineering, Punjab Engineering College (Deemed to be University), Chandigarh (160012), India
*satnamkaur@pec.edu.in

Abstract. With the increasing development of the telecommunication networks, the Internet Protocol Detail Records (IPDRs) have grown exponentially, and the detection of the fraud and anomalies has become more and more complicated. The conventional rule-based systems are not effective to identify changing and nuanced trends of fraud. In this paper, a supervised machine learning-based telecom fraud detection framework is presented using a synthetic IPDR dataset. A two-stage classification procedure is applied, binary classification is considered to detect the fraudulent sessions, and then multiclass classification is applied to establish the type of fraud. The models such as Support Vector Machine (SVM), Random Forest and XGBoost are trained on leak-free, session-based behavioral features. The models address class imbalance by employing weighted learning methods. Accuracy, precision, recall and F1-score are used to assess model performance. The experimental findings suggest that the best overall accuracy of an algorithm is that of the Random Forest, the most likely to be accurate in subtle and low-frequency fraud categories is SVM, and the overall performance of XGBoost is balanced across all the classes. The results prove that supervised learning is effective in detecting IPDR-based telecom fraud and that the selection of the model depends on the nature of the frauds.

Keywords: Machine Learning, Artificial Intelligence, Fraud Detection, Anomaly Detection, Tele communication Networks, Internet Protocol Detail Record (IPDR).

1 Introduction

The high growth of telecommunication networks and mobile services has resulted in an unprecedented growth in Internet Protocol Detail Records (IPDRs), which are records that capture traffic on information about user sessions and network activities. As much as these records are useful in network management and billing, they also pose the risk of advanced fraud and malicious activity, such as SIM swap attacks, VoIP spoofing, mass messaging abuse, and data exfiltration. Large volumes of telecom data, changing patterns of attacks, and imbalance between normal and fraudulent events have complicated the detection of such activities in large-scale telecom data. Conventional

A. Agnihotri et al. (eds.), *Proceedings of the Conference on Bridging Engineering Disciplines with AI and Machine Learning (BEDAIML 2026)*, Advances in Intelligent Systems Research 209,
https://doi.org/10.2991/978-94-6239-697-5_6

rule-based detection systems fail to detect less obvious and novel pattern of frauds, which spurs the utilization of machine learning-based solutions in telecom security analytics(Yehya & Salhab, 2023).

Recent studies have shown that machine learning methods are effective in detecting telecom-fraud and anomaly analysis. Indicatively, (Yehya & Salhab, 2023) demonstrated that telecom fraud detection accuracy can be enhanced by more than 75 percent through supervised learning models in contrast with traditional methods. Equally, (Skansi et al., 2020) investigated synthetic telecom data analysis techniques to learn about behavioral patterns in communication patterns, and real synthetic data were advantageous to telecom analytics. Other papers have used machine learning architectures to identify cyber threats and anomalous activity in networked systems, and it has been highlighted that scalable and adaptive detection models are required in large communication systems (Poudyal et al., 2018; Zhang et al., 2025). All of these works suggest supervised learning with behavioral feature analysis as a promising way of telecom fraud detection.

Although these advances have been made, there are still a number of challenges. Telecom fraud data are often very skewed, with fraud sessions making only a tiny part of the total traffic. In addition, fraud patterns differ in intensity and activity, with high-volume fraud (i.e. mass SMS campaigns) at one end to low-profile fraud (i.e. SIM swapping). Most of the available research concentrates on binary fraud detection without identifying which type of anomaly is relevant, which limits their applicability in real telecom settings. This necessitates a single framework which is capable of not only identifying fraudulent activity but also to classify the type of the activity based on dependable and leak-free properties of IPDR data.

In order to meet these issues, this paper will present a controlled machine learning model of IPDR-based telecom fraud detection and anomaly categorization. The design has been based on a two-step approach: a binary classifier is used to differentiate between normal and fraudulent sessions, and a multiclass classifier is used to detect the type of fraud. A leak-free feature selection strategy is used to extract session-level behavioral features of IPDR records to ensure realistic deployment conditions. Three supervised learning models-Support Vector Machine (SVM), Random Forest and XGBoost are introduced and compared on the basis of performance. Accuracy, precision, recall and F1-score are used to measure model performance.

This paper is organized as follows: **Section 2** presents the literature review and discusses existing research related to telecom fraud detection using machine learning techniques. **Section 3** describes the proposed methodology, including the supervised learning models used in this study. **Section 4** explains the experimental setup, including the dataset description, model framework and evaluation metrics used. **Section 5** presents the experimental results and provides a comparative discussion of the performance of SVM, Random Forest and XGBoost models. Finally, **Section 6** concludes the paper by summarizing the key findings of this study.

2 Literature Review

The development of machine learning has been used to detect telecom fraud, as communication networks have grown in scale and complexity. The initial methods relied mostly on rule-based systems and expert-set limits and proved insufficient to detect changing and behaviorally nuanced patterns of fraud. As a result of the access to massive datasets of telecommunication and the growth of computing power, the applications of supervised learning have become efficient in detecting fraudulent behaviors in network traffic (Yehya & Salhab, 2023).

(Yehya & Salhab, 2023) showed that compared to traditional telecom fraud detection, supervised machine learning models can dramatically increase the accuracy of detection of telecom fraud, especially when dealing with large-scale telecom datasets. Their activity emphasizes the relevance of behavioral characteristics based on the records of calls and sessions. In the same vein, (Krasic & Celar, 2022) discussed the problem of imbalance in the detection of telecom fraud and demonstrated that machine learning-based methods trained using imbalance-sensitive approaches are capable of delivering trustworthy performance in fraud detection even in the case of infrequent occurrence of fraud. These papers substantiate the appropriateness of supervised learning to telecom fraud analysis.

Some researchers have also examined the anomaly detection in communication and network data with machine learning frameworks. (Nizar et al., 2022) used ensemble learning methods to identify anomalies in telemetry data and their study revealed better detection in a complex network setup. (Kayacik et al., 2021) suggested real-time fraud detection of streaming behavioral on-demand, the significance of scalability and adaptability of the model used with telecom systems. Moreover, (Al-Hababi & Tokgoz, 2020) applied machine learning to detect malicious behaviors in encrypted network flows and demonstrated that a behavioral pattern may unveil the hidden threat even without knowledge of the content information.

In spite of these developments, the majority of current research is more associated with binary fraud detection and does not differentiate between various manifestations of fraud. In addition, certain methods are based on programmed features which can cause information leakage or cannot be present in real time deployment environments. It is still necessary to have a single supervised learning model that can not only detect fraud, but also classify anomalies based on leak-free behavioral features that are learnt directly on IPDR data. The current article fills this gap by suggesting a two-stage supervised learning strategy and comparing SVM, Random Forest, and XGBoost as a method of detecting telecom fraud and classifying types of anomalies.

3 Methodology

This work uses three monitored machine learning algorithms including Support Vector Machine (SVM), Random Forest, and Extreme Gradient Boosting (XGBoost) to detect telecom fraud and classify anomalies using IPDR data. The methodology is based on a two-stage taxonomic system. During the initial step, binary classification is used to

differentiate between fraudulent and normal sessions. The second step involves multiclass classification, in which the type of fraud among fraudulent sessions is determined. To ensure realistic deployment conditions, all models are trained on leak-free session-based behavior features produced directly based on IPDR records.

3.1 Support Vector Machine (SVM)

The Support Vector Machine is a margin supervised learning algorithm that gives a good separating hyperplane between classes in a high dimensional feature space. It mostly works well with datasets in which the boundaries between classes are complicated and cannot be separated in a linear fashion. SVM is also applicable in telecom fraud detection because it can be used to detect minor deviations in network sessions.
An SVM classifier as obtained in this case is based on the radial basis function (RBF) kernel to model non-linear decision boundaries within the IPDR feature space.

The SVM model is set using the following hyper parameters:

- Kernel: Radial Basis Function (RBF)
- Regularization parameter, C=1.0
- Kernel coefficient, γ=0.01
- Class weighting: class_weight = ‘‘balanced’’.

The regularization parameter, C controls the trade-off parameter between the maximization of margin and the minimization of classification errors, while γ determines the influence range of individual training samples in the RBF kernel. This structure makes SVM model capable of capturing concealed and low-frequency fraud activities like SIM swaps and anomaly of data exfiltration.

3.2 Random Forest

Random Forest is an ensemble learning algorithm where a number of decision trees are built in the course of the training process but the predictions are combined to come up with a final classification outcome. The ensemble form enhances the performance of generalization as well as lowers overfitting in contrast to single decision trees. Random Forest works well with tabular telecom data because it is capable of non-linear interactions among features and non-homogeneous distribution of features.

The Random Forest model is configured with the following parameters:

- Number of trees: n_estimators = 300
- Maximum tree depth: max_depth = 20
- Class weighting: class_weight = "balanced"
- Random seed: random_state = 42

The appropriate large number of trees enhances the stability of the ensembles and the max depth parameter size restricts the complexity of trees and decreases overfitting. This setup enables Random Forest to successfully identify high volume and rule-based frauds like mass SMS and OTP redirection attacks.

3.3 Extreme Gradient Boosting (XGBOOST)

XGBoost is an ensemble algorithm that applies the gradient boosting using decision trees sequentially with each trees learning how to correct the mistakes of the previous ensemble. It uses regularization, shrinkage and subsampling schemes to enhance generalization and computational efficiency. XGBoost has been known to perform well in structured tabular data and imbalanced classification applications and is thus very apt when it comes to telecom fraud detection.
The XGBoost model is configured with the following hyperparameters:
Common parameters (binary and multiclass):

- Number of trees: n_estimators = 300
- Maximum tree depth: max_depth = 6
- Learning rate: learning_rate = 0.05
- Subsample ratio: subsample = 0.8
- Column sampling: colsample_bytree = 0.8
- Random seed: random_state = 42

Binary classification–specific parameters:

- Objective: binary:logistic
- Imbalance handling: scale_pos_weight = (#normal / #fraud)
- Evaluation metric: auc

Multiclass classification–specific parameters:

- Objective: multi:softprob
- Number of classes: num_class = K (fraud types)
- Evaluation metric: mlogloss

The medium depth of the tree and low learning rate enables the model to detect complex non-linear trends of fraud and prevent overfitting. Subsampling and column sampling are random and this increases generalization. This kind of arrangement allows XGBoost to achieve balanced performance, both on the large volume and low-level type of fraud.

4 Experimental Setup

This part explains the properties of the dataset used, the feature included, the training procedure, and the evaluation technique adopted in the telecom fraud detection experiment and the anomaly classification experiment.

4.1 Dataset Description

The experiments are conducted using the synthetic Internet Protocol Detail Record (IPDR) data on telecom networks sessions. The dataset has a total of about 78000 session records and up to 50 behavioral features of traffic that characterize features of communication such as volume of data transferred, session duration, protocols used, as well as, session statistics. The features consist of unique identities including user_id,

event_id, imsi number and imei number. Each record contains a binary indicator of a fraud (is_fraud) to provide information on whether the session is a fraud or not. One more categorical variable (anomaly_type) in the case of fraudulent sessions, tells the type of fraud, i.e. mass messaging abuse, VoIP spoofing, SIM swap, data exfiltration, and OTP redirection attacks.

4.2 Two-Stage Classification Framework

A two-level supervised classification model is used to capture real world telecom fraud analysis processes.
Stage 1: Binary Classification of Fraud Type
All the session records are utilized to learn a binary classifier that separates between the fraud and normal traffic based on the is-fraud label.
Stage 2: Multiclass Classification of Fraud Type
Records are only selected when they are marked as fraudulent and an error detector (referred to as a multiclass classifier) is trained to determine the type of anomaly or (anomaly_type). This step finds out the type of fraud after the activity has been identified to be malicious.
This hierarchical structure is similar to operational telecom monitoring systems where anomaly is detected and then a threat is assigned.

4.3 Evaluation Metrics

Performance of models is measured by standard classification measures; these measures measure the overall and the class-wise detection performance. Considering that the telecom fraud detection is a scenario when the imbalanced classes are involved and various types of frauds are encountered, the accuracy is not the only metric as precision, recall and F1-score are under focus. Confusion matrices and Receiver Operating Characteristic (ROC) curves can also be used as the method of visual performance analysis. In binary classification, the potential prediction cases are divided into True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). These values are the base of the metrics of analysis below.

- Accuracy is a measurement of the percentage of the correctly classified instances in all the samples:

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

- Precision measures the proportion of predicted fraud instances that are actually fraudulent:

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

- Recall measures the proportion of actual fraudulent instances that are correctly detected:

$$\text{Recall} = \frac{TP}{TP + FN}$$

- The harmonic mean of precision and recall is known as F1-Score which is a balanced metric that assesses detection performance:

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

5 Results and Discussion

This section provides the results of SVM, Random Forest, and XGBoost performance in terms of telecom fraud detection and the type of fraud on IPDR data.

5.1 Binary Fraud Detection

The three models have good performance in the separation of fraudulent and normal telecoms. The accuracy of SVM is approximately 98%, whereas that of Random Forest and XGBoost are 99%, as shown in fig1, fig2 and fig3 respectively. This demonstrates that the chosen behavioral IPDR features are useful in the identification of fraud. On the whole, the binary fraud detection is very accurate in all of these three algorithms.

=== Classification Report (Binary: Normal vs Fraud) ===

	precision	recall	f1-score	support
0	0.99	1.00	0.99	12046
1	0.97	0.89	0.93	1056
accuracy			0.99	13102
macro avg	0.98	0.94	0.96	13102
weighted avg	0.99	0.99	0.99	13102

Figure 1 Binary Classification Report of SVM

Binary Classification Report:

	precision	recall	f1-score	support
0	0.99	1.00	0.99	6428
1	0.95	0.86	0.91	562
accuracy			0.99	6990
macro avg	0.97	0.93	0.95	6990
weighted avg	0.99	0.99	0.99	6990

Figure 2 Binary Classification Report of Random Forest

Classification Report (XGBoost):

	precision	recall	f1-score	support
0	0.99	1.00	0.99	14369
1	0.94	0.88	0.91	1249
accuracy			0.99	15618
macro avg	0.97	0.94	0.95	15618
weighted avg	0.99	0.99	0.99	15618

Figure 3 Binary Classification of XGBoost

5.2 Multiclass Fraud Type Classification

The models in the second stage determine the type of fraud that occurred among the observed fraudulent sessions. The multiclass accuracy is once again quite high, around

98% in the case of SVM and about 99% in the case of Random Forest and XGBoost as presented in fig 4, fig5 and fig6 respectively.

However, there is a difference in performance with the types of fraud. Random Forest works best when the attack volume is high like with MASS_SMS and OTP_REDIRECTION attacks as the traffic patterns are highly differentiated. SVM is more effective with less severe types of fraud like SIM_SWAP and DATA-EXFIL that imply behavioral modification over the extreme traffic volume. VOIP provides the same performance in all models.

=== Classification Report (Fraud Type – SVM) ===

	precision	recall	f1-score	support
DATA_EXFIL	0.97	0.99	0.98	191
MASS_SMS	0.97	0.99	0.98	339
OTP_REDIRECTION	0.99	0.95	0.97	188
SIM_SWAP	1.00	0.95	0.97	121
VOIP_SPOOF	0.99	1.00	0.99	218
accuracy			0.98	1057
macro avg	0.98	0.98	0.98	1057
weighted avg	0.98	0.98	0.98	1057

Figure 4 Multi-class Classification Report of SVM

Multiclass Anomaly Type Report:

	precision	recall	f1-score	support
DATA_EXFIL	0.95	0.98	0.97	102
MASS_SMS	1.00	1.00	1.00	184
OTP_REDIRECTION	1.00	1.00	1.00	106
SIM_SWAP	0.96	0.93	0.95	56
VOIP_SPOOF	1.00	0.99	1.00	114
accuracy			0.99	562
macro avg	0.98	0.98	0.98	562
weighted avg	0.99	0.99	0.99	562

Figure 5 Multi-class Classification Report of Random Forest

	precision	recall	f1-score	support
DATA_EXFIL	0.98	0.99	0.99	224
MASS_SMS	1.00	1.00	1.00	405
OTP_REDIRECTION	1.00	0.98	0.99	224
SIM_SWAP	0.96	0.97	0.96	139
VOIP_SPOOF	1.00	1.00	1.00	258
accuracy			0.99	1250
macro avg	0.99	0.99	0.99	1250
weighted avg	0.99	0.99	0.99	1250

Figure 6 Multi-class Classification Report of XGBoost

5.3 Model Comparison

The obtained results are presented in Table 1. Random Forest provides the largest overall accuracy, and is highly useful in trends of large-scale fraud. SVM is more susceptible to minor and low-frequency fraud patterns. XGBoost offers an average performance with all types of frauds without a heavy inclination to one type. The performance of a model is based on the type of a fraud pattern. The combination of several supervised models into a systematic framework enhances the general detection reliability.

Table 1. Results and Comparative Analysis of Models

Metric / Fraud Type	Support Vector Machine (SVM)	Random Forest (RF)	XGBoost (XGB)	Best Model
Binary Accuracy	99%	**99%**	98–99%	RF
Multiclass Accuracy	98%	**99%**	99%	RF
MASS_SMS Recall	0.99	**1.00**	**1.00**	Tie
VOIP_SPOOF Recall	**1.00**	0.99	**1.00**	Tie
OTP_REDIRECTION Recall	0.95	**1.00**	0.98	RF
DATA_EXFIL Recall	**0.99**	0.98	**0.99**	Tie
SIM_SWAP Recall	0.95	0.93	**0.97**	XGB
Overall Behavior	Strong for subtle fraud	Strong for high-volume fraud	Balanced	—

5.4 Discussion

The experiments validate that telecommunication fraud is recognizable with precision in terms of supervised machine learning using behavioral feature based on IPDR data. The two-stage model is efficient: the binary model is capable of identifying fraudulent sessions reliably, and the multiclass model identifies the type of fraud. It is also demonstrated that the overall accuracy is not the only metric that is necessary when it comes to telecom fraud detection. The importance of class-wise performance is that various types of frauds are characterized differently.

Altogether, the findings indicate that all SVM, Random Forest, and XGBoost can be used to detect telecom fraud, and they have complementary positive aspects of various types of fraud.

6 Conclusion

This paper suggested a monitored machine learning model on the detection of telecommunication fraud and anomalies by learning behavioural features based on IPDR data. An iterative approach involving binary classification followed by multiclass classification was chosen whereby a binary classification identified the presence of fraudulent sessions and the actual type of fraud was determined using a multiclass classification methodology. The Support Vector Machine (SVM), Random Forest and XGBoost models have been implemented and tested. It was experimentally

demonstrated that all the models had high detection accuracy of more than 98%, which proved the efficiency of leak-free IPDR behavioral features. Random Forest was the most accurate overall and the best in the high-volume type of frauds like MASS_SMS and OTP_REDIRECTION. SVM was more sensitive to small-scale and low-frequency types of frauds, especially the SIM_SWAP and the DATA_EXfil. XGBoost also gave an equal spread of performance in all categories of frauds. The findings reveal that the suitability of a model is determined by the characteristics of fraud behavior as opposed to general accuracy. In general, the suggested framework provides a credible and convenient method of telecom fraud detection and classification.

References

Al-Hababi, A., & Tokgoz, S. C. (2020). Man-in-the-Middle Attacks to Detect and Identify Services in Encrypted Network Flows using Machine Learning. *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, 1–5. https://doi.org/10.1109/CommNet49926.2020.9199617

Kayacik, A. F., Ozcan, B., Baltaoglu, G., Cakir, E., & Aktas, M. S. (2021). Real-Time Fraud Prediction On Streaming Customer-Behaviour Data. *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 1–6. https://doi.org/10.1109/ICECCE52056.2021.9514169

Krasic, I., & Celar, S. (2022). Telecom Fraud Detection with Machine Learning on Imbalanced Dataset. *2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1–6. https://doi.org/10.23919/SoftCOM55329.2022.9911518

Nizar, N. A., P. M., K. R., & Bp, V. K. (2022). Anomaly Detection In Telemetry Data Using Ensemble Machine Learning. *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 1–6. https://doi.org/10.1109/CONECCT55679.2022.9865730

Poudyal, S., Subedi, K. P., & Dasgupta, D. (2018). A Framework for Analyzing Ransomware using Machine Learning. *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1692–1699. https://doi.org/10.1109/SSCI.2018.8628743

Skansi, S., Sekrst, K., & Kardum, M. (2020). A Different Approach for Clique and Household Analysis in Synthetic Telecom Data Using Propositional Logic. *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1286–1289. https://doi.org/10.23919/MIPRO48935.2020.9245421

Yehya, B. A., & Salhab, N. (2023). Telecommunications Fraud Machine Learning-based Detection. *2023 4th International Conference on Data Analytics for Business and Industry (ICDABI)*, 656–661. https://doi.org/10.1109/ICDABI60145.2023.10629612

Zhang, S., Zhang, B., Hou, S., & Fu, Z. (2025). Leveraging LightGBM for High-Accuracy Telecom Fraud Detection with Clustering-Based Undersampling. *2025 8th International Symposium on Big Data and Applied Statistics (ISBDAS)*, 384–388. https://doi.org/10.1109/ISBDAS64762.2025.11117117