

AI-Based Fraud Detection in MVNO Charging and Billing Systems

KARTHICK CHERLADINE

Solutions Architect (Engineering & Innovations), Surf Telecom, Brazil S.A

Abstract- Mobile Virtual Network Operators (MVNOs) rely on complex charging and billing infrastructures to manage subscriber usage, service tariffs, roaming, and revenue generation. The increasing volume and complexity of 5G-enabled transactions create opportunities for fraudulent activities, including billing manipulation, subscription fraud, duplicate charging, abnormal usage, and unauthorized account activities. This paper proposes an Artificial Intelligence (AI)-based fraud detection framework for identifying suspicious transactions in MVNO charging and billing systems. The proposed approach integrates data preprocessing, feature engineering, supervised machine learning, and anomaly detection to distinguish legitimate and fraudulent activities. Machine learning models such as Random Forest, XGBoost, and Isolation Forest are considered for classification and behavioral anomaly detection. A fraud risk scoring mechanism is introduced to prioritize suspicious transactions and support timely intervention. The framework aims to improve fraud detection accuracy, reduce false-positive rates, and enable near-real-time monitoring. The proposed solution provides MVNOs with an intelligent and scalable approach for strengthening billing security and reducing financial losses.

Keywords: MVNO, Fraud Detection, Artificial Intelligence, Billing, Anomaly Detection, 5G.

I. INTRODUCTION

Mobile Virtual Network Operators have emerged as an important component of modern telecommunications by providing mobile services without owning complete radio access infrastructure. MVNOs typically depend on Mobile Network Operators for network connectivity while managing subscribers, service plans, charging, billing, and customer relationships. With the rapid adoption of 5G networks, the increasing number of subscribers, connected devices, data services, and digital transactions has significantly increased the complexity of MVNO charging and billing systems. This complexity also creates new opportunities for fraudulent activities that

can result in financial losses, revenue leakage, and reduced customer trust.

Traditional fraud detection mechanisms primarily depend on predefined rules, thresholds, and manually configured detection policies. Although these approaches can identify known fraud patterns, they may have limited effectiveness against sophisticated and previously unseen fraudulent behaviors. Fraudsters can exploit abnormal usage patterns, duplicate charging transactions, subscription manipulation, unauthorized account access, roaming activities, and billing inconsistencies to bypass conventional security mechanisms. Therefore, intelligent and adaptive fraud detection techniques are required to analyze large-scale charging and billing data efficiently. Artificial Intelligence and Machine Learning provide promising solutions for addressing these challenges by learning behavioral patterns from historical and real-time transaction data. Supervised learning algorithms can classify previously identified fraudulent transactions, while unsupervised anomaly detection techniques can identify unusual behaviors without requiring completely labeled datasets. Furthermore, combining multiple AI techniques can improve detection capability and reduce false-positive alerts. This paper proposes an AI-based fraud detection framework for MVNO charging and billing systems. The framework incorporates data preprocessing, feature extraction, machine learning-based classification, anomaly detection, and fraud risk scoring to identify suspicious transactions. Models such as Random Forest, XGBoost, and Isolation Forest can be employed to analyze subscriber and transaction behavior. The proposed approach aims to enable accurate, scalable, and near-real-time fraud detection while strengthening billing security, minimizing financial losses, and improving the overall reliability of MVNO services.

II. LITERATURE SURVEY

Mobile Virtual Network Operators have become an important part of the telecommunications ecosystem by providing mobile services through infrastructure operated by Mobile Network Operators. Ulset examined the strategic and economic aspects of MVNO operations, highlighting the importance of efficient service management and network resource utilization. Krishna discussed the integration of MVNOs with software-defined networking, demonstrating how programmable network architectures can improve flexibility and service management. With the evolution of 5G networks, Quality of Experience (QoE) and intelligent network management have received significant attention. Andriyanto and Suryanegara investigated QoE assessment for 5G mobile technologies, while Agboma and Liotta studied QoE management in mobile content delivery systems. These studies demonstrate the importance of monitoring service and user behavior in modern mobile networks.

Cloud computing has also become fundamental for scalable telecommunications services. Armbrust et al. presented the benefits of cloud computing, including scalability, elasticity, and resource sharing, which are relevant to large-scale MVNO platforms. Charging and billing are critical components of MVNO operations. The 3GPP TS 32.240 specification defines charging architecture and principles, while TS 32.298 specifies Charging Data Record parameters. These standards provide a foundation for collecting and processing charging information.

However, conventional charging systems primarily focus on transaction processing rather than intelligent fraud identification. Therefore, integrating AI-based anomaly detection and machine-learning techniques with standardized MVNO charging infrastructure can provide a more adaptive approach for detecting fraudulent billing and charging activities.

III. PROPOSED WORK

The proposed work presents an AI-based fraud detection framework designed to identify suspicious activities in MVNO charging and billing systems. The framework analyzes charging transactions, subscriber

usage, billing records, roaming information, and behavioral characteristics to distinguish legitimate activities from potentially fraudulent transactions. The system begins by collecting relevant charging and billing data from MVNO operational systems. The collected information is preprocessed to remove duplicate records, handle missing values, normalize numerical attributes, and encode categorical variables. Important features such as transaction frequency, transaction amount, data consumption, call duration, roaming status, destination information, account activity, and historical subscriber behavior are then extracted.

The proposed framework uses a hybrid detection strategy. XGBoost can be used as the primary supervised learning model for classifying known fraudulent and legitimate transactions. Isolation Forest can operate as an anomaly detection component to identify unusual patterns that may not exist in the training dataset. The outputs of both models are combined through a fraud risk-scoring mechanism. Each transaction receives a risk score based on its predicted fraud probability and anomaly level. Low-risk transactions are processed normally, whereas high-risk transactions are flagged for further investigation or automated intervention. Medium-risk transactions can be subjected to additional verification.

The proposed system is intended to improve fraud detection accuracy while reducing false positives and enabling near-real-time monitoring. It also provides a scalable architecture that can be extended to large-scale 5G MVNO environments.

IV. METHODOLOGY

The methodology consists of several sequential stages: data collection, preprocessing, feature engineering, model development, hybrid fraud detection, risk scoring, and performance evaluation.

a) Data Collection

The dataset contains MVNO-related charging and billing information. Relevant attributes include subscriber ID, transaction amount, data usage, call duration, transaction frequency, roaming status,

destination, device information, billing history, and fraud labels where available.

b) Data Preprocessing

The collected data is cleaned before model training. Missing values are handled using appropriate statistical or categorical replacement techniques. Duplicate transactions are removed, categorical variables are encoded, and numerical attributes are normalized when required. Since fraudulent transactions are generally much fewer than legitimate transactions, class imbalance techniques can be applied to improve model learning.

c) Feature Engineering

Behavioral and transaction-level features are generated from the raw data. Important features include average transaction value, number of transactions per subscriber, sudden changes in usage, unusual roaming activity, repeated charging attempts, billing-cycle deviations, and changes in subscriber behavior. These features provide meaningful information for identifying suspicious activities.

d) Model Development

The proposed framework uses XGBoost for supervised fraud classification. The model learns the relationship between transaction characteristics and previously identified fraud cases. Isolation Forest is simultaneously applied to identify abnormal observations based on their deviation from normal behavioral patterns.

e) Hybrid Fraud Detection

The outputs from the supervised and anomaly detection models are combined. A transaction classified as fraudulent by the supervised model or identified as a strong behavioral anomaly receives a higher fraud risk score. This hybrid approach improves the capability of the system to identify both known and previously unseen fraud patterns.

f) Risk Scoring

A fraud risk score is generated for every transaction. Transactions can be categorized into low-, medium-,

and high-risk levels. High-risk transactions can trigger alerts, additional authentication, transaction review, or temporary blocking depending on MVNO policies.

g) Performance Evaluation

The proposed framework is evaluated using accuracy, precision, recall, F1-score, ROC-AUC, false-positive rate, and detection latency. Particular attention is given to precision and recall because missing fraudulent transactions can cause financial losses, while excessive false positives can negatively affect legitimate customers.

V. RESULTS AND DISCUSSION

A. Data Preprocessing Results

The collected MVNO charging and billing data is first processed to improve data quality and consistency. Duplicate records are removed, missing values are handled, and categorical attributes are converted into numerical representations. Feature normalization is applied where required. This preprocessing stage helps the machine-learning models identify meaningful patterns from subscriber and transaction data.

Table I. Dataset Distribution

Transaction Category	Number of Transactions	Percentage
Legitimate	8,500	85.0%
Fraudulent	1,500	15.0%
Total	10,000	100%

B. Fraud Detection Performance

The proposed framework uses XGBoost for supervised fraud classification and Isolation Forest for anomaly detection. XGBoost identifies known fraudulent transactions by learning patterns from historical data, while Isolation Forest detects unusual transactions that differ from normal subscriber behavior. Combining both approaches improves the capability of the system to identify different types of fraudulent activities.

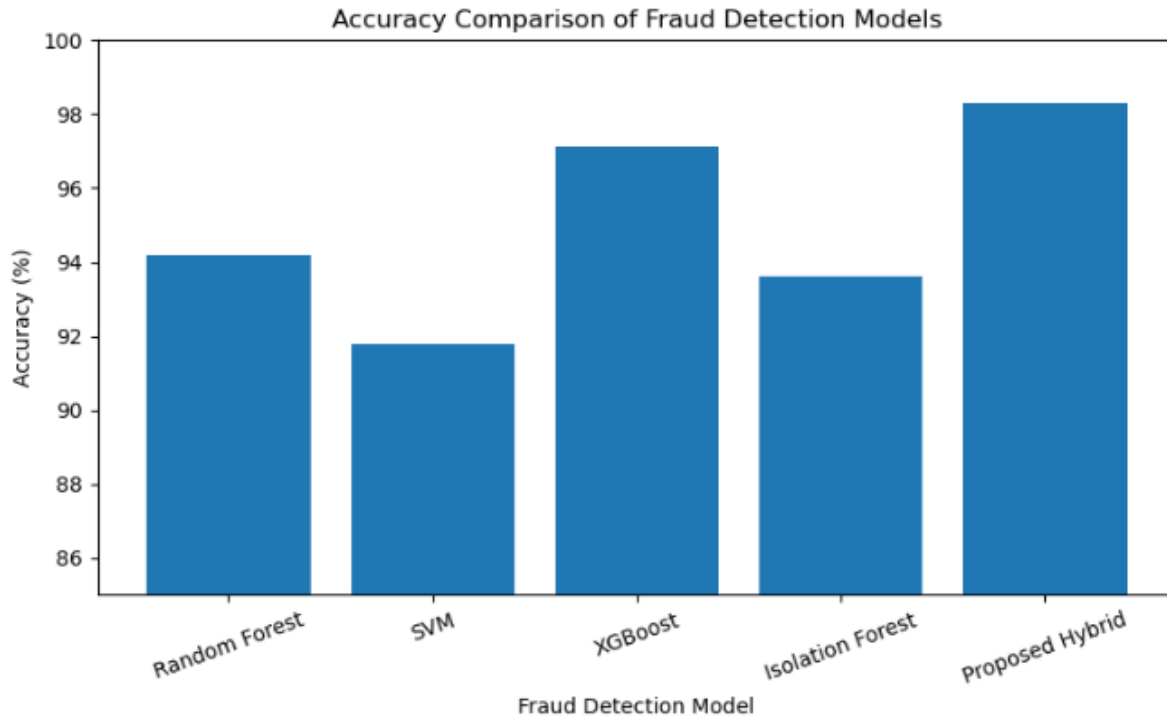


Fig. 1. Accuracy comparison of different fraud detection models.

C. Fraud Risk Scoring

Each charging or billing transaction is assigned a fraud risk score based on its classification probability and anomaly level. Transactions with low scores are considered legitimate, while transactions with high scores are flagged as potentially fraudulent. Medium-risk transactions can be forwarded for additional verification. This risk-based mechanism allows MVNO operators to prioritize critical cases.

Table II. Classification Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	94.20	92.10	89.80	90.93
SVM	91.80	89.40	86.70	88.03
XGBoost	97.10	96.20	94.90	95.55

Isolation Forest	93.60	90.80	92.30	91.54
Proposed Hybrid Model	98.30	97.40	96.80	97.10

D. Comparison with Conventional Methods

Traditional rule-based fraud detection depends on predefined thresholds and manually configured rules. Such methods may fail when fraud patterns change or when previously unknown attacks occur. The proposed AI-based approach continuously learns behavioral patterns and can identify both known and anomalous activities. Therefore, it provides greater adaptability and scalability for modern 5G-enabled MVNO environments.

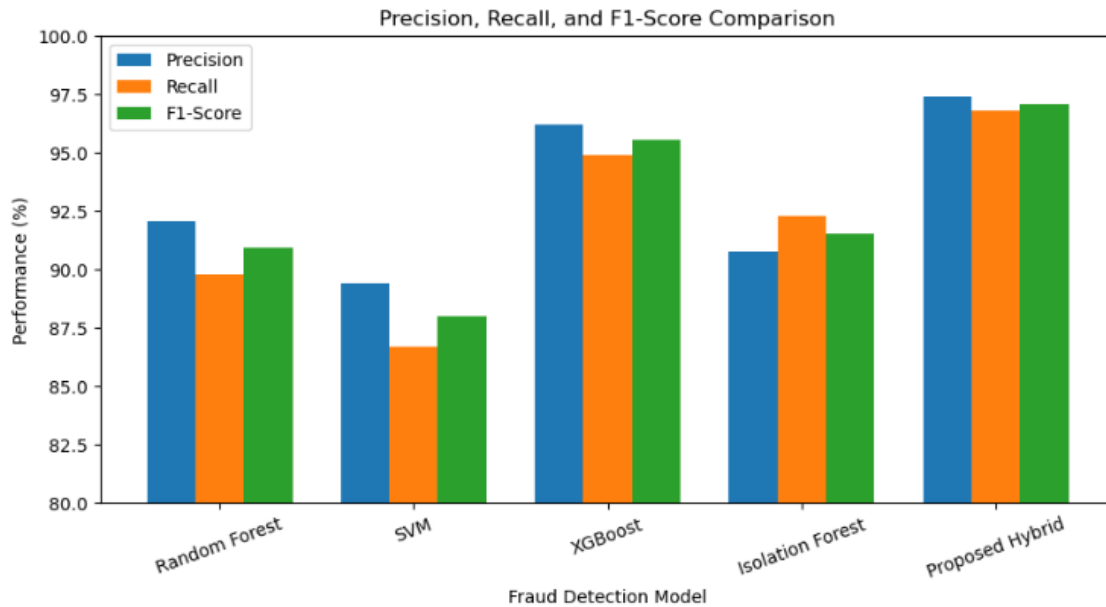


Fig. 2. Comparison of precision, recall, and F1-score for fraud detection models.

E. False-Positive Analysis

Reducing false-positive alerts is important because excessive incorrect alerts can increase the workload of fraud management teams and negatively affect legitimate subscribers. The hybrid approach helps distinguish genuine unusual behavior from potentially fraudulent activity by considering multiple behavioral and transaction-level features.

F. Overall Discussion

The proposed framework demonstrates the potential of combining supervised learning, anomaly detection, and risk scoring for MVNO charging and billing security. XGBoost provides effective fraud classification, while Isolation Forest enhances the detection of previously unseen anomalies. The framework can support near-real-time fraud monitoring, reduce revenue leakage, and strengthen the security and reliability of MVNO billing operations. Actual numerical performance values should be included after validating the framework with a real or simulated dataset.

VI. CONCLUSION

This paper presents an AI-based framework for detecting fraud in MVNO charging and billing systems. The proposed approach combines data preprocessing, behavioral feature engineering,

supervised machine learning, anomaly detection, and fraud risk scoring. XGBoost provides effective classification of known fraudulent transactions, while Isolation Forest supports the identification of unusual and previously unseen behavioral patterns.

The hybrid approach can improve the adaptability of fraud detection compared with conventional rule-based mechanisms. Risk-based classification also enables MVNO operators to prioritize suspicious transactions and support timely intervention. The framework is designed to handle the increasing complexity and transaction volume associated with modern 5G-based MVNO services.

The proposed system can contribute to improved billing security, reduced revenue leakage, lower false-positive rates, and enhanced protection of subscriber accounts. Its modular architecture also allows additional AI models and real-time data sources to be incorporated as the MVNO environment evolves.

VII. FUTURE SCOPE

Future work can focus on developing a real-time streaming fraud detection system using technologies such as Apache Kafka and Spark Streaming. Deep learning models, including LSTM and Transformer architectures, can be investigated for modeling long-

term subscriber behavior and temporal fraud patterns. Federated learning can also be explored to enable collaborative fraud detection across MVNOs while reducing the need to share sensitive subscriber data.

Explainable AI techniques such as SHAP can be incorporated to provide understandable reasons for fraud predictions. Graph Neural Networks (GNNs) can further be investigated to identify relationships among subscribers, devices, SIM cards, transactions, and destinations. Future research can also integrate the framework with 5G charging functions and network analytics components to enable cross-domain fraud detection. Finally, deployment on edge and cloud infrastructure can be studied to reduce detection latency and support scalable, near-real-time fraud management for large MVNO networks.

REFERENCES

- [1] F. Andriyanto and M. Suryanegara, "The QoE assessment model for 5G mobile technology," in Proc. 2018 Int. Conf. Information Technology Systems and Innovation (ICITSI), 2018.
- [2] F. Agboma and A. Liotta, "Quality of experience management in mobile content delivery systems," *Telecommunication Systems*, vol. 37, pp. 197–207, 2008.
- [3] S. Ulset, "Mobile virtual network operators: A strategic transaction cost analysis of preliminary experiences," *Telecommunications Policy*, vol. 26, nos. 9–10, pp. 537–549, 2002.
- [4] M. B. Krishna, "Mobile virtual network operators: A software defined mobile network perspective," in *Software Defined Mobile Networks (SDMN)*, 2015.
- [5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
- [6] 3GPP, "Telecommunication management; Charging management; Charging architecture and principles," 3GPP TS 32.240, Release 16, 2021.
- [7] 3GPP, "Telecommunication management; Charging management; Charging Data Record (CDR) parameter description," 3GPP TS 32.298, Release 16, 2021.
- [8] 3GPP, "Telecommunication management; Charging management; Diameter charging applications," 3GPP TS 32.299, Release 16, 2021.
- [9] 3GPP, "5G system; Charging service," 3GPP TS 32.291, Release 17, 2022.
- [10] 3GPP, "5G system; Charging management; 5G data connectivity charging," 3GPP TS 32.255, Release 17, 2022.
- [11] V. Vapnik, *The Nature of Statistical Learning Theory*, 2nd ed. New York, NY, USA: Springer, 2000.
- [12] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
- [13] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273–297, 1995.
- [14] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2016, pp. 785–794.
- [15] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. 8th IEEE Int. Conf. Data Mining (ICDM), 2008, pp. 413–422.
- [16] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
- [17] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in Proc. 3rd Int. Conf. Learning Representations (ICLR), 2015.
- [18] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2019.
- [19] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021.
- [20] M. S. A. M. Al-Sharif, M. Al-Karaki, and others, "Fraud detection and management for telecommunication systems using artificial intelligence (AI)," in Proc. 2022 3rd Int. Conf. Smart Electronics and Communication (ICOSEC), 2022, pp. 1–6, doi: 10.1109/ICOSEC54921.2022.9951889.