A Comparative Study of Machine Learning Approaches for Fraud Detection in Telecommunication Networks

Divya Sharma[1], Satnam Kaur*[1], Divya Bansal[1] and Mamta Dabra[1]

[1]Department of Computer Science & Engineering, Punjab Engineering College (Deemed to be University), Chandigarh (160012), India
*satnamkaur@pec.edu.in

Abstract. As the telecommunication technologies continue to expand, they have brought about many opportunities in terms of global connectivity, yet they have equally enhanced the chances of other frauds like phishing, SMiShing, voice spam and revenue share fraud. The old systems of detection, which rely on fixed rules and manual inspection, are becoming ineffective against new, changing and unknown threats. The current review explores the published articles within the past year 2018-2025 concerning the use of the techniques of Machine Learning (ML) and Artificial Intelligence (AI) in enhancing the process of detecting telecom fraud. The analysis is based on supervised, unsupervised, and hybrid ML models, such as Random Forest, SVM, Gradient Boosting, and LightGBM, and the literature on the issue of data imbalance and privacy concerns. Findings in the reviewed literature indicate that systems based on ML have the ability to attain accuracy rates of over 95 percent and can help in real-time detection. The review also highlights the existing challenges like the scarcity of public datasets, non-explainable, and ethical issues. On the whole, this paper highlights the increasing use of ML in the development of smart, expandable, and secure fraud detection systems in next-generation telecom networks.

Keywords: Machine Learning, Artificial Intelligence, Fraud Detection, Anomaly Detection, Telecommunication Networks.

1 Introduction

The rate of growth of Telecommunication networks has been extremely rapid, particularly in recent years, owing to 5G technology, the Internet of Things (IoT), and the emergence of digital payment systems. Such advancements have simplified and increased the efficiency of global communication and provided novel opportunities to carry out fraud and other cybercrimes. Phishing, ransomware, SMS phishing (SMiShing), International Revenue Share Fraud (IRSF) and voice spam are increasingly common. A report by the Communications Fraud Control Association indicates globally, telecom fraud led to losses of approximately 39.89 billion in 2021(Yehya & Salhab, 2023). This is a clear indication of the urgency and importance of developing improved fraud detection and prevention systems. 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_3

methods, which rely on the rule logic or manual checks, are no longer able to keep pace with the speed and smartness of the attackers. Due to this, the telecom industry has witnessed a major migration towards learning-based and automated systems.

Artificial Intelligence (AI) and Machine Learning (ML) are becoming important aspects of the process of fraud detection. They are capable of managing large volumes of customer and network data, learn past trends, and detect outliers or abnormal behavior in a more competent and efficient manner than the old systems. The paper examines 19 articles that have been published in 2018-2025 that use the techniques of ML to identify fraud in telecommunication networks. Studies by Skansi et al.(Skansi et al., 2020) , Poudyal et al.(Poudyal et al., 2018) , and Zhang et al.(Zhang et al., 2025) indicate a variety of options, such as supervised and unsupervised models, as well as methods, such as propositional logic analysis and clustering-based under-sampling. Various applications have been examined in these studies including phishing web sites detection(Anakal et al., 2023), anomaly detection in telemetry data(Nizar et al., 2022), and prediction of real time fraud according to user activity(Kayacik et al., 2021). Data applied in these studies includes synthetic samples up to real call records that represent both controlled and natural settings.

Based on these works it is possible to note that ML models have achieved significant advances in enhancing the accuracy of anomaly detection and response time. One recent study(Zhang et al., 2025) used the LightGBM model with an estimated detection rate of approximately 98%. However, there are still some issues such as unbalanced data sets, lack of explainability to models, and the problem of privacy of user data, particularly when attacks like Man-in-the-Middle (MITM) happen as discussed by Al-Hababi et al (Al-Hababi & Tokgoz, 2020). Combining these findings this review will set out to offer a brief description of the current implementation of ML in telecom fraud detection and areas that require enhancement. It is imperative to note that future research might investigate ways of how technologies such as blockchain, explainable AI and federated learning can make fraud prevention systems more transparent, secure and scalable in real-time telecom environments.

This review paper is organized as follows: **Section 2** presents the background and related work, discussing existing research on telecom fraud detection and anomaly detection using machine learning techniques. **Section 3** discusses the challenges of the review and highlights the research gaps in the field of telecom fraud detection. **Section 4** describes the review methodology, including the criteria and process used for selecting and analyzing the relevant research papers. **Section 5** presents the results of the literature review along with a comparative analysis of the selected studies. **6** concludes the paper by summarizing the main insights obtained from the reviewed studies. Finally, **Section 7** outlines potential directions for future research in this domain.

2 Background and Related Work

The quick development of telecommunication networks under the impulse of 5G, IoT, and digital services has both increased the number of data flow and the number of

people who can be connected and provided an opportunity to develop new loopholes and options of breaches and mass fraud (Prabhu Rajasekar & Vezhaventhan, 2024), (Mahmoud & Ismail, 2020) . The conventional detect systems, founded on static rules or manual checks, cannot deal with large scale telecom data and are ineffective when it comes to anomalies of rare occurrence. Consequently, to enhance the accuracy of anomalies detection, scale, and automation, researchers have resorted to the use of Machine Learning (ML) and Artificial Intelligence (AI) (Poudyal et al., 2018; Skansi et al., 2020; Zhang et al., 2025).

Early research progress like (Poudyal et al., 2018) investigated managed models, including Random Forest and SVM, in the classification of ransomware, and (Skansi et al., 2020) used propositional logic to examine artificial telecom information. Subsequent research used hybrid and ensemble models to deal with imbalanced data and streaming data (Krasic & Celar, 2022; Mir et al., 2025; Nizar et al., 2022). LightGBM with under-sampling (clustering) demonstrated the effectiveness of ensemble learning in telecom fraud detection with up to 98 percent accuracy (Zhang et al., 2025)). Later studies were devoted to domain-specific threats, such as phishing (Anakal et al., 2023), SMiShing (Boukari et al., 2021), and voice spam (Lin et al., 2022). AutoAD (Putina et al., 2022) and encrypted flow analysis (Al-Hababi & Tokgoz, 2020), which were frameworks that were not supervised, further improved detection of anomalies in limited or private data.

The solutions to the problem of anomaly detection using deep learning have a number of limitations, as observed by (Pang et al., 2022). Models that are learned through reconstruction tend to learn generic compressed features, instead of anomaly-specific patterns. GANs training is prone to several issues including failure to converge, mode collapse, which contributes to high difficulty in training GANs-based anomaly detection models.

(Nezhadsistani & Stiller, 2024) pointed to the absence of labelled anomaly data. This survey targeted 6G network anomaly detection using machine learning. Current deep learning methods are still subject to a number of constraints such as large amount of data produced by 6G environments which causes a burden of computational load and lowering of detection rates.

Overall, current literature indicates that ML is an effective tool in enhancing fraud detection in telecom services, although such issues as data imbalance, explainability, and real-time implementation are still at the research stage (Reypnazarov et al., 2025; Yehya & Salhab, 2023).

3 Challenges and Research Gaps

Nevertheless, the use of machine learning (ML) in telecommunication fraud detection has achieved significant advancements, but there are still numerous gaps and research issues. Few of the studies were conducted on actual telecom data, and the majority had fabricated or simulated data because of confidentiality, privacy issues and/or low data availability (Prabhu Rajasekar & Vezhaventhan, 2024; Reypnazarov et al., 2025; Skansi et al., 2020). IPDR and CDR data were not used very frequently as well,

although these sources can provide useful information about user trends and network-wide dynamics (Kayacik et al., 2021; Nizar et al., 2022; Zhang et al., 2025). Indeed, none of the studies employed synthetic IPDR. The variations of these supervised learning algorithms were being applied by many researchers resulting in lower methodological variety and novelty (Das et al., 2022; Doraiswamy & Adakane, 2025; Poudyal et al., 2018; Toma et al., 2021). There are no established benchmark datasets that can be used to compare the results of the models across the literature (Anakal et al., 2023; Krasic & Celar, 2022).

One of the clear limitations in most works is the limited application of evaluation metrics. Some of the studies quantified only the overall accuracy, without considering complementary measures of the performance of fraud detection, which include precision, recall, F1-score, detection latency, and rates of false-positive, which are crucial in measuring the performance of fraud detection in real-time settings (Mahmoud & Ismail, 2020; Nizar et al., 2022; Yehya & Salhab, 2023). Most researchers applied qualitative metrics to determine the performance of models instead of concentrating on quantitative metrics. The second significant difficulty was the problem of the imbalance of classes since frauds usually constitute a small proportion of network transactions, which predisposes models to normal behavior (Krasic & Celar, 2022; Zhang et al., 2025). Moreover, not all works used feature selection or dimensionality reduction, which led to prolonged training time and non-efficient model performance (Lin et al., 2022; Reypnazarov et al., 2025).

Despite the growing interest in data security, privacy-preserving such as federated learning and homomorphic encryption have remained infrequent components of telecom ML pipelines(Al-Hababi & Tokgoz, 2020; Mir et al., 2025; Yehya & Salhab, 2023). The interpretability of models and explainable AI (XAI) are also insufficiently investigated, and operators have little knowledge about how automated systems make decision. Moreover, real time flexibility is not usually provided, with a large proportion of models being trained offline, and not able to identify rapidly changing fraud patterns(Kayacik et al., 2021; Mir et al., 2025; Putina et al., 2022). The combination of ML and blockchain, edge computing, and streaming analytics is incomplete, although they can make the process more transparent and faster in response (Putina et al., 2022; Zhang et al., 2025).

On balance, the analyzed literature shows that although ML techniques can be very accurate and efficient, their practical implementation in telecom settings is limited by the inability to access, interpret, and measure various metrics and data privacy. Resolution of these issues will involve joint research to develop open datasets, adaptable models and ethically based fraud detection systems.

4 Methodology

This review was conducted in a systematic manner to review and analyze research articles that dwelled on machine learning use in identifying anomalies in telecommunication networks. It starts with retrieving 368 papers in IEEE Xplore database with Search string **‘‘Fraud OR Anomaly AND Detection AND Supervised**

AND 'machine learning' OR ML AND Telecom OR Telecommunication AND Network''. In order to reduce the scope, the papers were initially filtered using the titles, where 305 papers were filtered out as they were not pertinent to telecom or did not necessitate the use of ML-based detection systems. Out of the rest of 63 papers, 33 papers were eliminated due to lack of enough attention to the field of anomaly detection or limited technical contribution. The rest of the 30 articles were reviewed in full text with 11 others being discarded due to lack of experimental results, non-availability of datasets etc.

This narrowing down process left 19 final papers that were the background of this study. Fig. 1 illustrates the selection flow step by step.

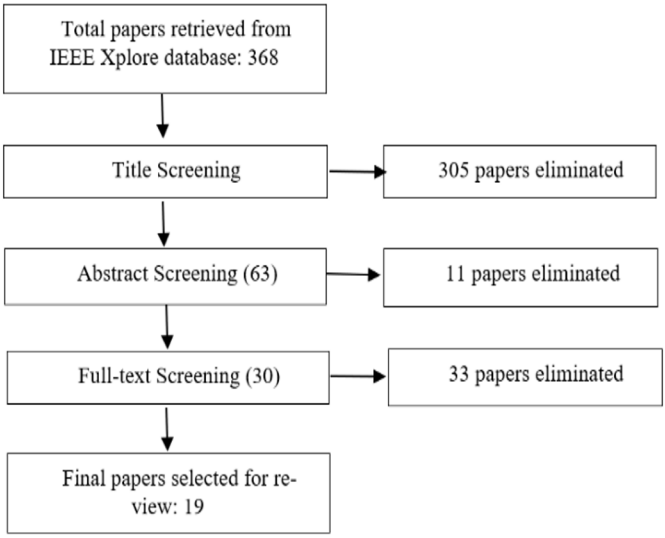

Figure 1 Selection process of research papers for reviewing.

All the chosen papers were thoroughly reviewed to come to terms with their methodology, type of datasets, model choice, and effectiveness. The methods that most of the researchers employed included supervised learning methods such as Random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting, with some employing unsupervised and hybrid models to address data imbalance and unlabeled samples.

Before model training, most researchers applied data preprocessing steps such as normalization, feature extraction, and transformation of categorical variables into numeric form.

5 Results & Comparative Analysis

Table 1 shows results and comparative analysis of all the papers that were selected for the review.

Table 1 Results and Comparative Analysis

Study	Year	Methodology / Model	Dataset Used	Results / Metrics	Advantages	Limitations
(Yehya & Salhab, 2023)	2023	ML-based telecom fraud detection	Telecom datasets	Feasible ML detection	Broad telecom coverage	Dataset not public
(Skansi et al., 2020)	2020	Propositional logic–based analysis	Synthetic telecom data	Qualitative improvement in clique/household detection	Interpretable, works with synthetic CDRs	No validation on real datasets
(Poudyal et al., 2018)	2018	Random Forest, SVM	Ransomware binaries	Accuracy: 76–97%	High detection rate	Domain not telecom-specific
(Zhang et al., 2025)	2025	LightGBM + clustering undersampling	Telecom fraud logs	Accuracy ≈ 98%	High accuracy, imbalance handling	Complex hyperparameter tuning
(Anakal et al., 2023)	2023	ML for phishing detection	Phishing website data	High accuracy and precision	Effective on URL features	Domain-specific only
(Nizar et al., 2022)	2022	Ensemble ML	Telemetry data	Enhanced detection rates	Robust ensemble performance	Computationally expensive
(Kayacik et al., 2021)	2021	Online/streaming ML	Customer behaviour data	Strong predictive performance	Supports live prediction	Prone to concept drift
(Al-Hababi & Tokgoz, 2020)	2020	ML for encrypted flow analysis	Encrypted traffic data	High identification rate	Works under encryption	Privacy concerns
(Prabhu Rajasekar & Vezhaventhan, 2024)	2024	AI-based detection framework	Simulated telecom data	Conceptual results	Integrates AI and privacy	Lacks experimental depth
(Mahmoud & Ismail, 2020)	2020	Literature survey on ML use-cases	N/A	N/A	Broad coverage of telecom ML	No experimental validation
(Mir et al., 2025)	2025	Real-time anomaly detection	Streaming telecom data	Low latency and high accuracy	Real-time operation	Implementation complexity

Study	Year	Methodology / Model	Dataset Used	Results / Metrics	Advantages	Limitations
(Krasic & Celar, 2022)	2023	Imbalanced ML models	Telecom fraud data	Better recall/F1	Handles class imbalance	Risk of overfitting
(Boukari et al., 2021)	2021	ML for SMS Phishing	SMS corpus	Improved F1-score	Telecom relevant domain	Small dataset
(Lin et al., 2022)	2022	Governance + ML framework	Voice spam logs	Effective governance design	Combines policy & tech	No quantitative results
(Putina et al., 2022)	2022	Unsupervised AutoAD framework	Anomaly datasets	Effective unsupervised detection	No labels required	High false positives possible
(Reypnazarov et al., 2025)	2025	ML for billing anomaly detection	Telecom billing data	Reduced false positives	Real-world telecom focus	Limited metrics reported
(Doraiswamy & Adakane, 2025)	2025	Supervised ML models	Cybercrime datasets	Improved detection accuracy	Recent, applicable to threat detection	Dataset details not shared
(Das et al., 2022)	2022	Supervised ML classifiers	Instagram account data	High fraud account detection	Demonstrates ML versatility	Not telecom-specific
Toma et al.(Toma et al., 2021)	2021	Supervised ML comparison	Email spam corpora	Improved spam classification	Clear algorithm comparison	Limited transferability

(Yehya & Salhab, 2023) introduced a telecommunication fraud detection system which is based on several ML models with an emphasis on the shift towards intelligent systems. Their result confirmed that ML can be used in telecom security, yet due to the lack of publicly available datasets, reproducibility and comparison were limited.

(Skansi et al., 2020) suggested a rational thinking process in order to examine synthetic telecom data through propositional logic. Their methods were aimed at finding relationships between users, households, and network behavior patterns. The method also showed successful grouping of entities but had been tested on synthetic data only, thus limited to real-world use.

(Poudyal et al., 2018) proposed a machine learning framework which is used to identify ransomware by using supervised algorithms, including Random Forest and

SVM. Their experiments had an accuracy of between 76-97%, which emphasizes the possibilities of ML in cyber threat analysis. Nonetheless, the research was about ransomware binaries, and not directly about telecom data, which limited the relevance to the domain.

(Zhang et al., 2025) used LightGBM with clustering-based undersampling as an approach to telecom fraud detection with high accuracy. Their model achieved an approximation of 98% accuracy exceeding traditional algorithms on imbalanced data. Although effective, the method was delicate to tune, and it was computationally expensive.

(Anakal et al., 2023) developed phishing websites detection by applying ML techniques that included Decision Tree and Random Forest. Their model worked well in determining the malicious URL and metadata sites. Even though this is not a telecom-related study, the study illustrates the transportability of methods in detecting fraud in communication networks.

(Nizar et al., 2022) suggested an ensemble learning system to detect anomalies in telemetry data. They combined several classifiers, which resulted in better stability and detection rate. Nevertheless, the ensemble method has computational complexity issues that have been hindering its implementation in real time telecommunications.

(Kayacik et al., 2021) designed a real-time system of fraud prediction based on customer behavior data sent by telecom activities. The model proved to be highly predictive and was responsive to the evolving usage patterns. However, the system might be hindered by labeled training data in quickly changing fraud situations.

(Al-Hababi & Tokgoz, 2020) examined the use of machine learning in detecting Man-in-the-Middle (MITM) attacks in encrypted network flows. Their model was effective to classify encrypted traffic without its decryption, which retained privacy of users. Nonetheless, the scheme caused some ethical doubts in terms of traffic monitoring and scaling in massive telecommunication systems.

(Prabhu Rajasekar & Vezhaventhan, 2024) examined AI-based fraud detection, data protection, and privacy improvement in the telecommunication systems. Their theoretical model focused on the combination of ML models with trustworthy communication systems. The study though creative in nature had not been quantitatively experimented and had not been validated using real data.

(Mahmoud & Ismail, 2020) have had a general review of the literature about the applications of ML in the telecom industry in the 5G era. They talked about customer churn, network optimization, and fraud detection. The article does present a useful overview but does not give much empirical analysis or model performance comparison.

(Mir et al., 2025) developed a real time anomaly detection architecture in telecom data streams through data mining and predictive modeling. The framework accommodated real-time identification of fraud with low latency. These were encouraging findings, but the research noted that larger scalable and distributed architectures were required.

(Krasic & Celar, 2022) solved the issue of class imbalance in telecom fraud data with the help of machine learning. Their experiments revealed that recall of detection was enhanced by varying weights of classes and sampling strategies. The research was

capable of dealing with skewed data, but had difficulties with overfitting and model stability in diverse datasets.

A machine learning-based SMiShing (SMS phishing) detection model was proposed by (Boukari et al., 2021), who aimed at textual or structural SMS characteristics. The experiments they conducted were found to be significantly precise and recalled the malicious messages. The primary weakness of the study was the limited size of the data that limited the generalization of the model.

(Lin et al., 2022) proposed a governance structure on voice spam detection and interception of telecom networks. They used policy-level regulation and ML-level filtering systems to reduce voice-based frauds. The work provided a pragmatic guidance but was deficient of quantitative analysis and algorithmic comparison.

(Putina et al., 2022) introduced AutoAD, an automatic unsupervised anomaly detector model that can detect abnormal behavior without any labels. This system showed successful outcomes on different data sets and showed flexibility to unrecognized attacks. But its high false-positive rate and computational penalty are subject to concern.

(Reypnazarov et al., 2025) produced an AI-based system of fraud detection in telecom billing, using pattern recognition and anomaly detection methods. Their model minimised false positives in billing anomalies. Although the paper talked a lot on the topic of billing data, there was little discussion about scalability on large network settings.

(Doraiswamy & Adakane, 2025) suggested AI-based supervised ML models that could be used to identify cybercrime threats with a focus on classification-based detection of suspicious trends. Their findings demonstrated a better detection accuracy than traditional methods. But little information was available regarding the properties of datasets and feature engineering which decreased reproducibility.

(Das et al., 2022) introduced a method to identify fraudulent Instagram users with the help of supervised learning models like Decision Trees and Logistic Regression. The system was found to be quite effective in classifying fake profiles with high precision and recall rates. Although not specific to telecom, the methodology demonstrates how the use of social networks to detect fraud is similar to telecom fraud issues.

(Toma et al., 2021) compared the performance of supervised ML models in identifying spam emails and described the algorithms, such as Naïve Bayes and Random Forest. The research identified the tradeoffs between processing time and accuracy. Although it is not directly related to telecom, it provided valuable information regarding text-based fraud detection that would be applicable in SMS or email filtering within a network.

6 Conclusion

The task of fraud detection has turned into a research problem because of the growing complexity of telecom networks and the emergence of the digital ecosystem and 5G infrastructure. The review has noted the role played by recent advances in Machine

Learning and how such advances can be used to develop adaptive, data-driven solutions that can detect abnormal behavior in the large-scale network environment. Other than speed and accuracy, the present study pays attention to the reliability, scalability, and interpretability of the model.

The majority of the reviewed articles indicate that continuous learning of the modern Machine Learning architecture is beneficial in detecting fraud, as well as anticipating the changing strategies of attacks. The change to real time analytics and self-healing networks suggests that telecom industry is becoming more reliant on autonomous intelligence as opposed to fixed detection rules. In the meantime, the ethical AI will focus on the privacy of user data and bias control.

Universities, telecom providers, and cybersecurity experts are necessary to work together to assure further development. It is necessary to combine AI innovation with safe data management, and industry expertise. Such a strategy will ensure the future fraud detecting system is transparent and self-optimizing that will also assist in securing the world communication network.

7 Future Work

The current evolution of the telecommunication systems towards 6G, IoT, and edge intelligence requires more adaptable and autonomous fraud detection solutions. Future studies ought to concentrate on the development of self-learning models that are able to work in a decentralized setting, handle streaming data in real time, and dynamically modify their parameters as the behavior of the network evolves. Federated learning and privacy-preserving analytics can be combined to help telecom operators cooperate in detecting fraud without revealing customer details.

The other avenue worth pursuing is the usage of explainable AI (XAI) and causal inference models to ensure that fraud detection system is more transparent and trustworthy. Integrating ML and blockchain based audit trails would serve as a potential means of enhancing data integrity and accountability in telecom networks as well. In addition, the creation of synthetic and realistic datasets will be required to benchmark the models in controlled and complex environments. Long term, future telecom fraud detection systems must go beyond reactive systems and towards predictive, context-sensitive and self-healing systems, which are in a position to forecast impending threats in advance. The next digital decade will be based on such smart and ethical automation, which will form the basis of secure communication networks.

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

Anakal, S., Maka, K., Tadkal, A., Humanabad, S., Anakal, S., & Laxmikant, E. (2023). Phishing Website Detection Using Machine Learning Methods. *2023*

International Conference on Integrated Intelligence and Communication Systems (ICIICS), 1–5. https://doi.org/10.1109/ICIICS59993.2023.10420933

Boukari, B. E., Ravi, A., & Msahli, M. (2021). Machine Learning Detection for SMiShing Frauds. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–2. https://doi.org/10.1109/CCNC49032.2021.9369640

Das, S., Saha, S., Vijayalakshmi, S., & Jaiswal, J. (2022). An Effecient Approach to Detect Fraud Instagram Accounts Using Supervised ML Algorithms. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 760–764. https://doi.org/10.1109/ICAC3N56670.2022.10074364

Doraiswamy, M. V., & Adakane, P. K. (2025). AI Powered Threat Detection in Cybercrime Using Supervised ML Models. *2025 12th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP)*, 1–6. https://doi.org/10.1109/ICETETSIP64213.2025.11156267

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

Lin, J., Chen, T., Wang, P., & Wu, C. (2022). Governance framework for voice spam detection and interception of telecom network. *2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, 1151–1156. https://doi.org/10.1109/IMCEC55388.2022.10019885

Mahmoud, H. H. H., & Ismail, T. (2020). A Review of Machine learning Use-Cases in Telecommunication Industry in the 5G Era. *2020 16th International Computer Engineering Conference (ICENCO)*, 159–163. https://doi.org/10.1109/ICENCO49778.2020.9357376

Mir, K. H., Kumar, R., Rai, S., Hassan, A., Sarkar, T., & Moharana, B. (2025). Real-Time Anomaly Detection in Telecommunications: Advanced Data Mining Techniques for Fraud Identification. *2025 3rd International Conference on Disruptive Technologies (ICDT)*, 1578–1583. https://doi.org/10.1109/ICDT63985.2025.10986461

Nezhadsistani, N., & Stiller, B. (2024). ML-Based Anomaly Detection in 6G Networks: A Survey on the Current Status, Challenges, and Future Directions. *2024 3rd International Conference on 6G Networking (6GNet)*, 75–83. https://doi.org/10.1109/6GNet63182.2024.10765631

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

Pang, G., Shen, C., Cao, L., & Hengel, A. V. D. (2022). Deep Learning for Anomaly Detection: A Review. *ACM Computing Surveys*, *54*(2), 1–38. https://doi.org/10.1145/3439950

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

Prabhu Rajasekar, K., & Vezhaventhan, D. (2024). Artificial Intelligence Based Fraud Detection, Data Security and Privacy for Telecommunication Systems. *2024 4th International Conference on Sustainable Expert Systems (ICSES)*, 402–406. https://doi.org/10.1109/ICSES63445.2024.10763168

Putina, A., Bahri, M., Salutari, F., & Sozio, M. (2022). AutoAD: An Automated Framework for Unsupervised Anomaly Detection. *2022 IEEE 9th International Conference on Data Science and Advanced Analytics (DSAA)*, 1–10. https://doi.org/10.1109/DSAA54385.2022.10032396

Reypnazarov, E., Allamuratova, Z., Babazhanova, T., & Dauletmuratova, R. (2025). AI-Driven Fraud Detection in Telecommunication Billing Systems. *2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM)*, 1990–1994. https://doi.org/10.1109/EDM65517.2025.11096687

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

Toma, T., Hassan, S., & Arifuzzaman, M. (2021). An Analysis of Supervised Machine Learning Algorithms for Spam Email Detection. *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, 1–5. https://doi.org/10.1109/ACMI53878.2021.9528108

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