NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

Machine learning models for fraud detection in telecommunication networks: A PRISMA – based review

Harshitha Pisupati
Karnataka campus
Rashtriya Raksha University
Shivamogga, India
0009-0004-0251-3210

Pudin Lakavath
School of Forensic Science
National Forensic Sciences University
Goa, India
lakavathpudin.1234@gmail.com

Sravana Durga Pisupati
Independent Researcher
Chennai, India
sravanipisupati@gmail.com

Abstract — ***The high growth rate of the telecommunication networks in the last two decades has changed the world connections, digital transactions, and socio–economic interactions to great extent. The development of mobile users, internet services, and digital payments is making telecommunication infrastructure to be more important aspect of modern society. However, with the rapid digitalisation, advanced fraud schemes have also been able to target users and operators with ease. Telecommunication encompasses within its scope a wide range of organised crimes such as subscription fraud, SIM swap fraud, international revenue share fraud, Wangiri fraud etc causing significant loss to service providers. Conventional systems of detection based on rules are not sufficient to combat the emerging and dynamic fraud schemes and requires more data driven approaches. Machine - learning (ML) techniques have become a powerful method in identifying sophisticated fraud indicators in large scale telecommunication data comprising of call detail records (CDRs) and transactional logs. The models of supervised learning which include Logistic regression, support vector machine, Decision tree, and ensemble models like Random Forest algorithms and XG Boost have shown better results in detection. In the recent times, the deep learning methos has been employed to learn anomalies in telecom data. Although there has been a rise in the number of studies in this field, there is a lack of comparability across studies. This PRISMA – based systematic review evaluates the findings from few of the selected studies to assess the machine learning models, performance outcomes and research gaps in telecom fraud detection.***

Keywords— Anomaly detection, Deep learning, Fraud detection, Machine Learning, PRISMA, Systematic review Telecommunication Fraud.

I. INTRODUCTION

The rapid expansion of telecommunication networks and digital financial integration has transformed global communication systems, becoming essential for economic and social activities [1]. However, this growth has also led to more sophisticated telecom fraud involving unauthorised exploitation of services and identities for financial gain as telecommunications intertwine with banking and E commerce. The complexity and scale of fraud incidents are increasing [2].

Telecommunication fraud includes various frauds such as SIM Swap frauds, International Revenue Share Frauds (IRSF), Wangiri scams, subscription fraud, spam calls, voice phishing, and SIM box bypass fraud. These frauds exploit vulnerabilities in subscriber verification and routing protocols. Traditional detection systems with static patterns are often inadequate against the evolving strategies employed by fraudsters, which hinders the real time anomaly detection [3].

The growing volume, velocity and variety of telecom data complicate fraud detection for telecom operators who generate large amounts of both structured and unstructured data, such as call detail records and network traffic logs [4]. Advanced analytical techniques, particularly machine learning are essential for extracting insights from this high dimensional data, as ML can identify patterns, detect anomalies and predict fraudulent behaviour more accurately and scalably than traditional methods [5].

Supervised learning models, ensemble techniques, deep learning architectures and graph-based frameworks are being utilised in telecom fraud detection for improved automated pattern recognition and behavioural profiling. However, issues such as class imbalance concept drift real time processing needs data privacy laws and the scarcity of public data sets hinder effective implementation [6]. This paper conducts a PRISMA based systematic review of machine learning models in telecom fraud detection, aiming to synthesise research trends, evaluate model performance, identify trends and weaknesses and highlight research gaps for future studies, thus contributing to enhanced fraud detection frameworks in telecommunication networks.

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

II. Methodology

This study uses a systematic approach to review according to PRISMA (Preferred reporting of items in systematic reviews and meta-analysis) 2020 to be transparent, reproducible, and to have a rigorous methodology in the selection and analysis of literature on the subject.

A. Search Strategy

The complete search of the literature was performed in various electronic databases such as Scopus, IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar and Web of Science. Only journal publications which are peer - reviewed and conference papers released between 2020 and 2025 were included in the search results. Keywords combinations used for the literature search were given in **FIGURE 1**. The search was refined with the help of Boolean operators (AND, OR) so that it could cover all the possible relevant studies.

B. Criteria for Inclusion and Exclusion

To ensure methodological rigor and relevance to the study subject, studies were included based on predefined inclusion criteria. Journal articles which are peer reviewed and conference papers including the specific topics about telecommunication fraud detection were selected. Articles depending on machine learning or AI were only considered.

1. Telecommunication fraud detection
2. Machine learning telecom fraud
3. SIM swap fraud detection
4. Call detail record fraud
5. Anomaly detection telecom
6. Telecom fraud classification

Fig. 1. Keyword Combinations used for Literature Search

Studies were excluded if they were only focused on banking or credit card frauds without reference to telecommunication systems. Articles, editorials, opinion papers and non-peer – reviewed papers were also omitted. Furthermore, studies lacking a clear methodology were excluded. Duplicate records identified during screening process were eliminated to prevent repetitions and to ensure data integrity.

C. Study Selection Process

The PRISMA 2020 recommendations were followed in the selection of the study [7]. 150 studies were found after a thorough search of the selected databases. There were 118 studies for screening after 32 duplicate records were found and eliminated during the identification phase. These 118 records titles and abstracts were examined during the screening phase in accordance with predetermined inclusion and exclusion criteria. Due to their lack of relevance to telecom enabled fraud detection, 76 research where consequently eliminated.
Subsequently, 42 full text articles made the eligibility requirements. 24 publications were eliminated at the eligibility stage for various reasons, including non-telecom specificity, duplicate publishing versions, lack of reported performance indicators and the absence of ML methods in methodology. Ultimately, the systematic review contained 18 studies that satisfied all eligibility requirements. The PRISMA flow diagram **(FIGURE 2)** depicts the identification, screening, eligibility, and inclusion phases of the entire study selection process.

III. Overview of Telecommunication Fraud

Telecommunication fraud refers to deliberate misuse of a telecommunication service and network infrastructure intentionally to achieve unauthorised financial gains. As mobile communication, VoIP and digital connectivity continue to grow and thrive at a very high pace, telephone networks are now the main target of more advanced schemes of frauds.
The subscriber identity verification, billing, international routing systems and digital authentication processes have vulnerabilities that are exploited by fraudsters. The integration of telecom services and banking, e-commerce and other digital payment systems has only intensified the level of threats and hence fraud detection is one of the key priorities of telecom operators in all countries of the world [8].
In telecom networks, the fraud environment is dynamic and constantly changing, which is represented by both conventional and technologically developed fraud. Common forms of in the form of SIM swap fraud, where the offender obtain a duplicate SIM card to take control of victim's mobile number telecom[9]; International revenue share fraud (IRSF), which involves fraud may be artificially generating high volumes of international

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

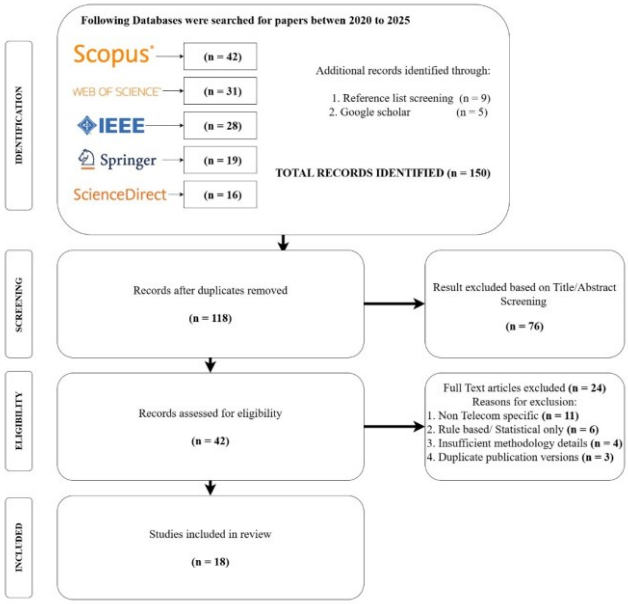


Fig. 2. PRISMA flow diagram employed for the systematic review

premium rate calls [10]; Wangiri fraud, also known as 'one ring scam', where victims are lured into calling back premium numbers [11]; subscription fraud etc.

The most common source of telecom fraud detection systems is the call detail records (CDRs) [12]. A CDR is a structured data regarding communication events such as identifiers of the caller and receiver, the duration of the call, timestamps, the type of the call, routing information, and, in some cases, location information based on cell tower identifiers. The records are also useful in behavioural information, and thus it is possible to identify abnormal calling patterns and suspicious activity. Other than CDR telecom operators may make use of subscriber profile data, sim registration data, Internet protocol detail records, device identifiers including IMEI number, recharge history and network traffic history. Effective fraud detection relies on extracting these features from the heterogeneous data sets to detect anomalies, behaviour deviations and emerging fraud patterns [13].

Telecom fraud detection faces challenges despite advancements in machine learning due to class imbalance, evolving fraud patterns and the high volume of data. To address these challenges, there is a need for adaptive learning techniques, continuous model updates, scalable, big data architectures, and explainable AI frameworks to maintain efficiency and regulatory compliance [14].

IV. MACHINE LEARNING TECHNIQUES IN DETECTION OF TELECOM FRAUD

The use of machine learning algorithms is now the focus of the contemporary telecom fraud detection mechanism because it can acquire sophisticated patterns based on extensive network data of call detail records, subscriber records and traffic records. Certain methods allow incorporating a fraudulent detection of anomalous behaviour, categorising fraudulent transactions and adjusting to changing strategy of fraud. Telecom fraud detection ML models can be broadly divided into supervised learning, ensemble methods, deep learning methods and unsupervised or semi supervised learning methods [12][15].

A. Supervised Learning models

Supervised learning models are extensively used in telecom fraud detection, since it uses labelled data sets in which the past records get labelled as fraudulent or legitimate. These models acquire knowledge of decision limits between normal and suspicious behaviour [16]. Logistic regression is a typical example of a baseline classifier because it is simple and interpretable and is particularly applied when the task at hand is binary fraud detection [17]. Decision trees have a rule-based classification, which is appreciated due to its transparency and the ability to visualise it [18]. Random forest is a collection of decision trees enhances the accuracy of the production and decreases the overfitting since several decision paths are combined [19]. SVM work well in high dimensional space and can detect the best separating hyperplanes between the classes of the fraud and non-fraud [20]. The K nearest neighbours (KNN) algorithm is a transaction classifier that involves similarity measures and is applicable in the detection of local anomalies of behaviour [21]. Naïve bayes, which is a probabilistic inference model, is computationally inexpensive and is effective in telecom data of large scale, even though it is founded on the assumption that the features are independent [22].

B. Ensemble learning methods

Ensemble learning approaches improve fraud detection by merging several base learners to provide more reliable productions. Gradient boosting improves classification accuracy by continuously creating models that fixes the error of earlier models. A highly tuned boosting technique, Extreme gradient boosting, XGBoost, provides parallel processing, regularisation and enhance performance on structured telecom data. Adaboost is very helpful for Imbalance fraud datasets since it concentrates on giving misclassified cases higher weights. Ensemble methods are particularly effective in telecom fraud detection due to their ability to handle non-linear relationships and complex interaction effects among features [23].

C. Deep learning techniques

Deep learning techniques are being employed more in telecom fraud detection because they can handle complex data and behavioural patterns. While Convolutional Neural Networks adapt to analyse the structure of telecom data by extracting

spatial information, Artificial Neural Networks model nonlinear relationships from call data records. Sequential call behaviours are the focus of recurrent neural networks, while long term interdependence in communication patterns is captured by LSTM Networks, which also detect evolving fraud schemes. In real time fraud monitoring systems where behavioural sequences are crucial, these models work very well.[24].

Together, these machine learning techniques provide a comprehensive analytical framework for telecom fraud detection, enabling improved accuracy, adaptability and scalability in model telecommunication networks.

V. Results and Comparative Analysis

After analysing 18 papers, the systematic review concluded that the most common methods for detecting telecom fraud are supervised and ensemble learning. According to [25], Random Forest outperform the logistic regression and XGBoost in banking card fraud detection, achieving virtually perfect accuracy (0.99) and recall (1.0000). Similarly, decision trees (99.89%), Random Forest (99.84%), and XGBoost (99.81%) demonstrated higher accuracy rates in Wangiri fraud detection [26]. Similar findings were published by [27], where Random Forest achieved 99.85% accuracy and XGBoost achieved 97.37% accuracy in Wangiri fraud detection. All things considered, these investigations demonstrate how well ensemble tree-based techniques work with structured telecom data sets.

According to [28], authors discovered that Random Forest achieved an accuracy of 0.92 outperforming SVM and XGBoost in effectiveness, highlighting the value of ensemble models. In a study on spam call detection, authors showed that combining traditional classifiers with AdaBoost produced better results with Naive Bayes + AdaBoost reaching 96% accuracy, outperforming SVM and Decision Tree pairs [29]. Similarly, in a study on credit card fraud detection data sets, they found that XGBoost (Accuracy = 0.97) and Random Forest (Accuracy = 0.96) performed better than SVM and Decision Tree in this study [30].

Deep learning approaches have shown mixed yet promising results in fraud detection. A study [31] noted moderate performance with CNN, while another noted hybrid CNN + XGBoost model gave improved results [32]. In text-based fraud detection [33], they achieved over 97% precision and recall with RoBERTa based models, and the study [34], demonstrated strong accuracy in voice phishing detection using LLM-based frameworks. Unsupervised methods such as K-Means and DBSCAN, applied by [35] achieved reasonable performance but generally did not surpass supervised and ensembled models. However, performance varied across fraud types. In a study [36], authors reported low accuracy in IRSF detection, highlighting the influence of dataset complexity and feature engineering on results. Overall, that results indicate that the most dependable models for structured telecom fraud detection are Random Forest and XGBoost, whereas deep learning and LLM based methods work well for unstructured text and voice-based frauds.

TABLE I. COMPARATIVE ANALYSIS OF RECENT STUDIES ON USE OF MACHINE LEARNING TECHNIQUES IN TELECOM ENABLED FRAUD DETECTION

Sl. no	Author and Year	Fraud type	Models used	Model category	Accuracy	Precision	Recall	Reference
1	Liu Guanyu, 2024	Telecom banking card fraud	Logistic Regression	Supervised and ensemble	0.95862	0.964	0.948	[25]
			Random Forest		0.999993	0.999	1.000	
			XGBoost		0.997983	0.998	0.998	
2	Hu et al (2022)	Telecom Fraud	BTG	Graph machine learning	88.23%	89.53%	84.05%	[37]
3	Jabbar & Suharjito (2020)	Telecom Fraud via CDR	K – Means DBSCAN	Unsupervised Unsupervised	97.23 90.39	98.11 99.38	96.37 89.89	[35]
4	Tong et al. (2025)	Telecom Fraud	GDFGAT	Graph neural networks	93.28	93.51	90.97	[38]

5	Li et al. (2025)	Telecom Fraud	CNN	Deep learning	78.59	16.88	78.50	[31]
6	Li et al. (2024)	Telecom fraud text	RoBERTa-MHARC	Deep Learning/NLP	NA	97.90	97.47	[33]
7	Djomadji et al. (2023)	SIM Box Bypass Fraud	Random Forest	Supervised	0.92	0.88	0.96	[28]
			SVM		0.69	0.89	0.53	
			XGBoost		0.81	0.71	0.82	
8	Guo & Wang (2020)	Telecom fraud on cellular data	CNNcombine (1D CNN + XGBoost)	Hybrid Deep Learning	90.39	81.55	71.60	[32]
9	Potnuru Divya (2024)	Spam calls	SVM along with AdaBoost	Supervised and ensemble	93% (SVM)	92% (SVM)	91% (SVM)	[29]
			Naïve Bayes along with AdaBoost		96%	95%	94%	
			Random forest along with AdaBoost		94%	93%	92%	
			Decision trees along with AdaBoost		90%	89%	88%	
10	Balouchi et al (2024)	Wangiri Fraud	Logistic regression	Supervised learning models	99.46	99.46	99.46	[26]
			Decision trees		99.89	99.89	99.89	
			Random Forest		99.84	99.84	99.84	
			XGBoost		99.81	99.81	99.81	
			Multi- Layer perceptron (MLP)		99.78	99.78	99.78	
11	Sharma et al. (2020)	Credit card fraud	Random Forest	Supervised learning models	98	82	90	[39]
			Logistic Regression		94	54	92	
			SVM		95	76	800	
			Neural networks		99	93	88	
12	Bakumenko et. Al (2025)	Financial anomalies	Logistic Regression	Supervised learning models	0.9979	0.7241	1.0000	[40]
			Random Forest		0.9961	0.6000	0.8571	
			XGBoost		0.9917	0.3830	0.8571	
			SVM		0.9982	0.8889	0.7619	
			Neural networks		0.9841	0.2561	1.0000	
13	Park et al. (2024)	Voice phishing	Vanilla LLM	LLM based framework	0.9650	0.9524	0.9790	[34]
			Domain expert LLM		0.9720	0.9655	0.9790	
			Expert guided LLM		0.9720	0.9787	0.9650	
14	Ravi et al. (2022)	Wangiri Fraud	Random Forest	Supervised learning models	99.85	99.71	99.83	[27]
			XGBoost		97.37	99.74	92.37	
			Naïve bayes		56.24	43.12	98.04	
15	Ding and Zhou (2024)	Telecom fraud (text – based)	LLM with Multi role Multi-layer Prompting	LLM	NA	88.3	85.1	[41]
16	Apostu et al (2020)	Telephone network frauds (IRSF)	Random Forest	Supervised Learning models	23.01	23.19	23.01	[36]
			Logistic Regression		17.76	8.7	17.76	
17	Gupta et al (2025)	Fraud phone calls	XGBoost	Supervised learning models	96.7	47.3	81.8	[42]

18	Chen et al (2025)	Credit card fraud	SVM	Supervised learning and ensemble models	0.94	0.90	0.85	[30]
			Decision tree		0.91	0.88	0.83	
			Random Forest		0.96	0.92	0.89	
			XGBoost		0.97	0.94	0.91	
			AdaBoost		0.92	0.89	0.84	
			MLP		0.95	0.91	0.87	
			ANN		0.96	0.93	0.90	

VI. CONCLUSION

The supervised ensemble learning models, Random Forest and XG boost perform well on structured data sets like call detail records, according to this PRISMA based systematic study that examines machine learning approaches for telecom fraud detection. These models can adapt to many forms of fraud, including Wangiri and SIM box bypass fraud, and perform well in terms of classification, accuracy and resistance to overfitting. Additionally, unstructured data may be processed using deep learning algorithms such as CNNs and LSTMs. Hybrid models combining ensemble and deep learning techniques were used for detection. However, the effectiveness is dependent on feature engineering, class imbalance and data set quality.

Data imbalance, the absence of publicly available datasets, privacy issues and real time deployment are among the main challenges in telecom fraud detection, according to the research. It is challenging to directly compare research due to the inconsistency of assessment measures and the data collection properties. The study concludes that ensembled tree-based models, which are currently the most dependable, are the best at detecting structured telecom fraud. Future research should concentrate on creating adaptive, explainable and hybrid learning models to deal with evolving fraud trends.

Additionally, creating scalable and effective fraud detection systems in contemporary communication networks would require a combination of machine learning, real time analytics and data governance or regulatory compliance.

VII. REFERENCES

[1] J. He, Y. Mu, C. Wang, and Y. Mao, "Impact of digital infrastructure construction on financial development: Evidence from the 'broadband China' Strategy," *Heliyon*, vol. 10, no. 15, p. e35262, Aug. 2024, doi: 10.1016/j.heliyon.2024.e35262.

[2] A. R. Căciulescu, R. Rughiniș, D. Țurcanu, and A. Radovici, "Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy," *Risks*, vol. 12, no. 12, p. 200, Dec. 2024, doi: 10.3390/risks12120200.

[3] K. Liu, "Research on the Types, Characteristics and Countermeasures of Telecom Fraud," *International Journal of Humanities, Social Sciences and Education*, vol. 8, no. 12, pp. 124–129, 2022, doi: 10.20431/2349-0381.0812014.

[4] A. T. - and Dr. C. S. -, "Exploring The Three V's: Volume, Velocity, and Variety in Telco Big Data Analytics," *International Journal For Multidisciplinary Research*, vol. 6, no. 5, Sep. 2024, doi: 10.36948/ijfmr.2024.v06i05.9692.

[5] T. A. Khan, J. Tulsi, M. Alam, K. Kadir, K. M. Ali, and M. S. Mazliham, "Analysis and visualization of fraud detection patterns through data mining and classification using MLP and hybrid deep learning model," *Egyptian Informatics Journal*, vol. 32, p. 100829, Dec. 2025, doi: 10.1016/j.eij.2025.100829.

[6] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, "Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications," *Data Science and Management*, Aug. 2025, doi: 10.1016/j.dsm.2025.08.002.

[7] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *J. Clin. Epidemiol.*, vol. 134, pp. 178–189, Jun. 2021, doi: 10.1016/j.jclinepi.2021.03.001.

[8] Md Habibul Arif, "Machine Learning Models for Cybersecurity Risk Analysis in U.S. Critical Infrastructure Systems," *Journal of Information Systems Engineering and Management*, vol. 11, no. 1s, pp. 1336–1362, Jan. 2026, doi: 10.52783/jisem.v11i1s.14284.

[9] M. Kim, J. Suh, and H. Kwon, "A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures," in *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*, IEEE, Aug. 2022, pp. 240–245. doi: 10.1109/BCD54882.2022.9900510.

[10] L. Ferreira *et al.*, "International revenue share fraud prediction on the 5G edge using federated learning," *Computing*, vol. 105, no. 9, pp. 1907–1932, Sep. 2023, doi: 10.1007/s00607-023-01174-w.

[11] A. A. Mawgoud, A. Abu-Talleb, and B. S. Tawfik, "A Holistic Neural Networks Classification for Wangiri Fraud Detection in Telecommunications Regulatory Authorities," 2021, pp. 175–183. doi: 10.1007/978-3-030-69717-4_19.

[12] M. A. Jabbar and S. Suharjito, "Fraud Detection Call Detail Record Using Machine Learning in Telecommunications Company," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 4, pp. 63–69, Jul. 2020, doi: 10.25046/aj050409.

[13] M. Okmi, L. Y. Por, T. F. Ang, W. Al-Hussein, and C. S. Ku, "A Systematic Review of Mobile Phone Data in Crime Applications: A Coherent Taxonomy Based on Data Types and Analysis Perspectives, Challenges, and

Future Research Directions," *Sensors*, vol. 23, no. 9, p. 4350, Apr. 2023, doi: 10.3390/s23094350.

[14] A. Patel and S. K. Malve, "Machine Learning for Fraud Detection in Digital Payment Systems: Challenges and Solutions," *International Journal of Innovations in Science Engineering And Management*, pp. 89–96, Jul. 2025, doi: 10.69968/ijisem.2025v4i389-96.

[15] A. A. Compagnino *et al.*, "An Introduction to Machine Learning Methods for Fraud Detection," *Applied Sciences*, vol. 15, no. 21, p. 11787, Nov. 2025, doi: 10.3390/app152111787.

[16] B. A. Yehya and N. Salhab, "Telecommunications Fraud Machine Learning-based Detection," in *2023 4th International Conference on Data Analytics for Business and Industry (ICDABI)*, IEEE, Oct. 2023, pp. 656–661. doi: 10.1109/ICDABI60145.2023.10629612.

[17] B. Chugh, N. Malik, and D. Gupta, "Firefly Optimization-Based Logistic Regression Classifier for Credit Card Fraud Detection," *Journal of Circuits, Systems and Computers*, vol. 34, no. 14, Sep. 2025, doi: 10.1142/S0218126625502044.

[18] A. P. Kirilenko, "Decision Trees," 2026, pp. 79–109. doi: 10.1007/978-3-031-89689-7_4.

[19] H. A. Salman, A. Kalakech, and A. Steiti, "Random Forest Algorithm Overview," *Babylonian Journal of Machine Learning*, vol. 2024, pp. 69–79, Jun. 2024, doi: 10.58496/BJML/2024/007.

[20] W. Tang, "Application of support vector machine system introducing multiple submodels in data mining," *Systems and Soft Computing*, vol. 6, p. 200096, Dec. 2024, doi: 10.1016/j.sasc.2024.200096.

[21] Y. Liao and V. R. Vemuri, "Use of K-Nearest Neighbor classifier for intrusion detection," *Comput. Secur.*, vol. 21, no. 5, pp. 439–448, Oct. 2002, doi: 10.1016/S0167-4048(02)00514-X.

[22] Z. Umarova, "Use of the Naive Bayes Classifier Algorithm in Machine Learning for Student Performance Prediction," *International Journal of Information and Education Technology*, vol. 14, no. 1, pp. 92–98, 2024, doi: 10.18178/ijiet.2024.14.1.2028.

[23] A. Mohammed and R. Kora, "A comprehensive review on ensemble deep learning: Opportunities and challenges," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 757–774, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.014.

[24] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, "Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications," *Data Science and Management*, Aug. 2025, doi: 10.1016/j.dsm.2025.08.002.

[25] G. Liu, "Leveraging Machine Learning for Telecom Banking Card Fraud Detection: A Comparative Analysis of Logistic Regression, Random Forest, and XGBoost Models," *Computers and Artificial Intelligence*, vol. 1, no. 1, pp. 13–27, Nov. 2024, doi: 10.70267/1cc7aw07.

[26] A. Balouchi *et al.*, "Wangiri Fraud Detection: A Comprehensive Approach to Unlabeled Telecom Data," *Future Internet*, vol. 18, no. 1, p. 15, Dec. 2025, doi: 10.3390/fi18010015.

[27] A. Ravi, M. Msahli, H. Qiu, G. Memmi, A. Bifet, and M. Qiu, "Wangiri Fraud: Pattern Analysis and Machine-Learning-Based Detection," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6794–6802, Apr. 2023, doi: 10.1109/JIOT.2022.3174143.

[28] 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.

[29] P. Divya, "Spam Call Detection Using Machine Learning," 2024. [Online]. Available: www.ijrpr.com

[30] Y. Chen, "A Comparative Study of Machine Learning Models for Credit Card Fraud Detection," *Academic Journal of Natural Science*, vol. 2, no. 4, pp. 11–18, Dec. 2025, doi: 10.70393/616a6e73.333530.

[31] J. Li, J. Dang, Y. Wang, and J. Yang, "Image-Based Telecom Fraud Detection Method Using an Attention Convolutional Neural Network," *Entropy*, vol. 27, no. 10, Oct. 2025, doi: 10.3390/e27101013.

[32] K. Guo and W. Wang, "Research on Telecom Fraud Detection Model Based on Cellular Network Data," *Journal of Networking and Telecommunications*, vol. 2, no. 1, p. 12, Jun. 2020, doi: 10.18282/jnt.v2i1.835.

[33] 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 (Switzerland)*, vol. 14, no. 24, Dec. 2024, doi: 10.3390/app142411628.

[34] H. Park, J. Lee, S. Han, and H. Byun, "Enhanced Voice Phishing Detection Using an LLM-Based Framework for Data Augmentation and Classification," *IEEE Access*, vol. 13, pp. 152530–152545, 2025, doi: 10.1109/ACCESS.2025.3603007.

[35] M. Abdul Jabbar and Suharjito, "Fraud detection call detail record using machine learning in telecommunications company," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 4, pp. 63–69, 2020, doi: 10.25046/aj050409.

[36] Apostu Sergiu, "Using Machine learning algorithms to detect frauds in Telephone networks," *The Annals of "Dunarea de Jos" University of Galati Fascicle III Electrotechnics Electronics Automatic Control and Informatics*, vol. 43, no. 3, 2020, doi: DOI:10.35219/eeaci.2020.3.03.

[37] X. Hu, H. Chen, S. Liu, H. Jiang, G. Chu, and R. Li, "BTG: A Bridge to Graph machine learning in telecommunications fraud detection," *Future Generation Computer Systems*, vol. 137, pp. 274–287, Dec. 2022, doi: 10.1016/j.future.2022.07.020.

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

[38] A. Tong, B. Chen, Z. Wang, J. Gao, and C. K. Lam, "GDFGAT: Graph attention network based on feature difference weight assignment for telecom fraud detection," *PLoS One*, vol. 20, no. 5 May, May 2025, doi: 10.1371/journal.pone.0322004.

[39] P. Sharma, S. Banerjee, D. Tiwari, and J. C. Patni, "Machine learning model for credit card fraud detection-A comparative analysis," *International Arab Journal of Information Technology*, vol. 18, no. 6, pp. 789–796, Nov. 2021, doi: 10.34028/iajit/18/6/6.

[40] A. Bakumenko, K. Hlavackova-Schindler, C. Plant, and N. C. Hubig, "Advancing Anomaly Detection: Non-Semantic Financial Data Encoding with Large Language Models," *IEEE Access*, vol. 13, pp. 146757–146771, 2025, doi: 10.1109/ACCESS.2025.3600967.

[41] J. Ding and H. Zhou, "Telecom Fraud Detection Based on Large Language Models: A Multi-Role, Multi-Layer Prompting Strategy," *Applied Sciences (Switzerland)*, vol. 16, no. 1, Jan. 2026, doi: 10.3390/app16010544.

[42] S. Gupta SATI, "R E S E A R C H P A P E R Journal of Global Research in Electronics and Communication An Intelligent System for Identifying Fraud Phone Calls Using Machine Learning Algorithms," 2025. [Online]. Available: www.jgrec.info