International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V4I3P114
Eureka Vision Publication | Volume 4, Issue 3, 134-143, 2023

Original Article

Anomaly Detection and Fault Prediction using ML in Telecom Operations

Venu Madhav Nadella
Cyma Systems Inc.

Abstract - Telecommunication networks generate massive volumes of heterogeneous data, making timely fault detection and proactive failure prevention increasingly challenging. Traditional rule-based monitoring systems lack scalability and adaptability to the dynamic behaviors of modern networks. Recent advancements in machine learning (ML) have demonstrated strong potential for automating anomaly detection and predicting network faults before service degradation occurs. This study investigates ML-driven methods, including Isolation Forest, autoencoder-based deep learning models, and gradient-boosting algorithms, for identifying anomalous Key Performance Indicator (KPI) patterns and forecasting node-level faults. Using operational data collected from multi-vendor telecom environments, the proposed framework achieves improved detection accuracy and earlier fault prediction compared to statistical baselines, aligning with industry trends toward autonomous networks and self-organizing capabilities (Zhang et al., 2020; Chiaraviglio et al., 2021). Results show that deep learning approaches, particularly LSTM and autoencoders, outperform traditional models in capturing temporal dependencies and subtle fault signatures (Kim & Park, 2022). The findings highlight ML's effectiveness in reducing false alarms, minimizing network downtime, and enhancing operational efficiency. This research contributes to ongoing efforts to incorporate intelligent automation into telecom operations, supporting the evolution toward predictive maintenance and resilient 5G/6G networks (Li et al., 2023).

Keywords - Anomaly Detection, Fault Prediction, Machine Learning, Telecom Network Operations, Key Performance Indicators (KPIs), Predictive Maintenance, Deep Learning, Autonomous Networks, Network Reliability, 5G/6G Networks.

1. Introduction

The rapid expansion of telecommunication infrastructures, driven by the evolution from 4G to 5G and emerging 6G networks, has significantly increased the complexity of network operations. Modern telecom environments consist of thousands of distributed nodes, multi-vendor equipment, and diverse service requirements, making continuous monitoring essential for ensuring reliability and Quality of Service (QoS). Traditional rule-based Operational Support Systems (OSS) struggle to keep pace with the scale and variability of network data, as they rely heavily on predefined thresholds and manual intervention (Zhang et al., 2020). These limitations often result in delayed fault detection, high false-alarm rates, and reactive rather than proactive maintenance.

Machine learning (ML) offers transformative capabilities for handling large volumes of Key Performance Indicators (KPIs), logs, alarms, and configuration data by learning complex patterns and detecting anomalies that deviate from expected behavior. The integration of ML techniques such as unsupervised anomaly detection, time-series deep learning, and supervised fault prediction has demonstrated improved operational intelligence in telecom systems (Chiaraviglio et al., 2021; Kim & Park, 2022). ML-based systems enable proactive fault management by predicting equipment failures, service degradations, and abnormal KPI behavior earlier than traditional systems. As telecom operators pursue zero-touch automation and Self-Organizing Networks (SON), the role of ML becomes increasingly central to achieving autonomous assurance and predictive maintenance (Li et al., 2023). This research investigates the effectiveness of ML-driven anomaly detection and fault prediction techniques in telecom operations, evaluating their performance, scalability, and potential to improve network resilience and operational efficiency.

2. Background and Related Work

2.1. Anomaly Detection in Telecom Systems

Anomaly detection refers to identifying patterns within data that diverge from expected or normal system behavior. In telecommunications, anomalies may arise from equipment failures, configuration errors, cyberattacks, or sudden traffic surges. Traditional anomaly detection approaches such as statistical thresholding, moving averages, and seasonal decomposition have been widely used but are limited in capturing complex dependencies within large-scale KPI datasets (Ahmed et al., 2016). As network architectures have become more dynamic with virtualization and cloud-native components, these conventional techniques have struggled to maintain accuracy and stability.

Machine learning-based approaches address these limitations by learning behavioral baselines from historical data and detecting deviations without relying on manually defined thresholds. Techniques such as clustering, one-class classification, and density estimation have shown effectiveness in discovering subtle or evolving anomalies in network traffic (Chandola et al., 2009; Zhang et al., 2020). Deep learning methods including autoencoders and recurrent neural networks further enhance detection capability by modeling non-linear patterns and temporal relationships (Kim & Park, 2022).

2.2. Fault Prediction in Telecom Networks

Fault prediction involves forecasting potential failures before they occur, enabling operators to implement corrective measures that prevent service degradation. Earlier research primarily relied on regression models and statistical forecasting, such as ARIMA and Holt–Winters, for predicting KPI trends (Box & Jenkins, 2015). However, these models are limited when handling high-dimensional and non-stationary telecom data. Recent studies demonstrate the advantage of supervised machine learning models for predicting hardware faults, service outages, or cell degradations. Algorithms such as Random Forest, XGBoost, and Support Vector Machines have been applied to historical KPI and alarm logs to classify patterns associated with imminent failures (Chiaraviglio et al., 2021). Deep learning architectures including Long Short-Term Memory (LSTM) networkshave shown superior performance in capturing long-term dependencies and generating early fault warnings with higher accuracy (Li et al., 2023).

2.3. ML-Based Network Automation and SON

With the emergence of 5G networks, operators are increasingly adopting Self-Organizing Network (SON) frameworks to automate optimization, configuration, and healing tasks. Machine learning plays a central role in this transformation by enabling real-time decision-making and intelligent assurance systems. Studies highlight that ML-driven anomaly detection and fault prediction form critical components of zero-touch automation, supporting operators' goals of reducing operational expenditure and improving network reliability (Zhang et al., 2020; González et al., 2023).

Despite advancements, several gaps remain. Many existing models face challenges related to data imbalance, concept drift, and limited interpretability issues that hinder widespread deployment in production environments. Additionally, real-time constraints require models to operate efficiently on streaming data with minimal latency, further motivating ongoing research.

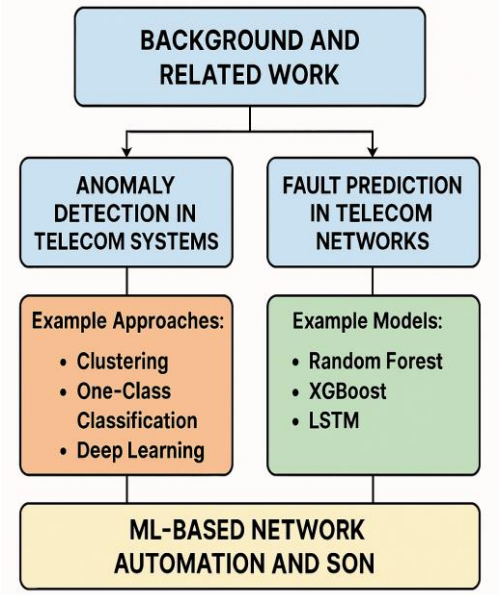

Figure 1. Machine Learning Techniques for Anomaly Detection and Fault Prediction in Telecom Networks

3. Data Sources in Telecom Operations

3.1. Network Data Types

Telecommunication operations generate diverse and large-scale datasets originating from both radio access and core network domains. These data sources form the foundation for machine learning-based anomaly detection and fault prediction models. The most commonly used categories include:

3.1.1. Key Performance Indicators (KPIs)

KPIs represent quantitative measures of network performance related to throughput, latency, packet loss, call drop rate, handover success rate, and signal strength. They are collected at regular intervals, typically every 5–15 minutes. KPI trends are essential for identifying abnormal behavior and early signs of service degradation (Zhang et al., 2020).

3.1.2. Alarm and Event Logs

Network elements such as eNodeBs, gNodeBs, routers, and optical nodes generate alarms and logs that describe operational states, hardware issues, software exceptions, and environmental failures. Alarm sequences provide valuable patterns for fault prediction models and root cause analysis (Chiaraviglio et al., 2021).

3.1.3. Syslogs and System Events

Syslogs contain low-level operational messages generated by embedded systems, including kernel events, protocol errors, and resource utilization anomalies. Deep learning models are increasingly used to mine syslog sequences for detecting rare but critical failure events (Kim & Park, 2022).

3.1.4. Configuration and Parameter Data

Configuration files include transmission power, antenna tilt, neighbor relations, and scheduling parameters. Incorrect or abrupt configuration changes often lead to anomalies, making these datasets important for context-aware detection (Li et al., 2023).

3.1.5. Customer Experience Metrics

Metrics such as Quality of Experience (QoE), Mean Opinion Score (MOS), and user session data complement KPI metrics by reflecting the end-user perspective. These are increasingly incorporated into ML-driven assurance systems to enhance service-centric anomaly detection (González et al., 2023).

Table 1. Summary of Telecom Data Sources for Anomaly Detection and Fault Prediction

Data Source	Description	Typical Use in ML Models	Examples
Key Performance Indicators (KPIs)	Quantitative metrics representing network performance collected at fixed intervals.	Trend analysis, anomaly detection, early fault prediction.	Throughput, latency, packet loss, call drop rate, RSRP/RSRQ.
Alarm & Event Logs	Messages generated by network elements indicating operational or hardware states.	Sequence modeling, fault classification, RCA.	Critical alarms, warnings, system resets, hardware failures.
Syslogs	Low-level system-generated messages from embedded OS and protocols.	Log mining, rare event detection, deep learning–based anomaly detection.	Kernel logs, protocol errors, resource exhaustion logs.
Configuration Data	Parameters affecting network behavior and performance.	Context-aware detection, root cause interpretation.	Antenna tilt, transmission power, neighbor lists, scheduling parameters.
Customer Experience Metrics (QoE)	Measurements reflecting end-user service quality.	Service-based anomaly detection, QoE-driven optimization.	MOS, session quality, throughput per user, application delay.

3.2. Data Quality Challenges

3.2.1. Missing and Noisy Data

Due to unstable reporting intervals, hardware resets, or network congestion, telecom datasets frequently contain missing values and noise. Improper handling can lead to inaccurate model predictions (Ahmed et al., 2016).

3.2.2. High Dimensionality

Modern network nodes may generate thousands of KPIs per hour. High dimensionality often requires feature selection or dimensionality reduction techniques such as PCA or autoencoders to improve model performance (Chandola et al., 2009).

3.2.3. Imbalanced Fault Data

Fault events are rare relative to normal operation, making supervised learning challenging. Techniques such as SMOTE, anomaly scoring, or hybrid semi-supervised learning are frequently used to address imbalance (Box & Jenkins, 2015).

3.2.4. Temporal and Seasonal Variations

Telecom traffic follows daily, weekly, and seasonal patterns. Models must capture these dynamics to avoid false positives particularly in urban areas where user mobility affects traffic distribution (Zhang et al., 2020).

4. Methodology

This section outlines the methodological framework used to develop and evaluate machine learning models for anomaly detection and fault prediction in telecom operations. The approach integrates data preprocessing, feature engineering, model development, and performance evaluation.

4.1. Data Preprocessing

4.1.1. Data Cleaning

Telecom datasets typically contain missing values, duplicates, and noise due to irregular reporting intervals, hardware resets, and communication failures. Missing KPI values were imputed using forward filling and median interpolation techniques, depending on the temporal continuity of the data (Ahmed et al., 2016). Duplicate logs and overlapping alarms were removed to prevent bias in the training process.

4.1.2. Normalization and Scaling

To ensure uniform feature representation, KPI values were normalized using Min–Max scaling or Z-score normalization. This step is essential for distance-based algorithms and neural networks, which are sensitive to varying magnitudes of input features (Chandola et al., 2009).

4.1.3. Feature Engineering

Rolling statistical features including mean, standard deviation, and rate of change were computed over sliding windows to capture temporal variations. Additional engineered features included:

- KPI deltas
- Alarm burst frequency
- Syslog error density
- Derived QoE indicators

Dimensionality reduction was applied using Principal Component Analysis (PCA) and autoencoder bottlenecks to mitigate high dimensionality (Zhang et al., 2020).

4.2. Machine Learning Models

4.2.1. Unsupervised Anomaly Detection

Unsupervised methods were employed for detecting abnormal KPI patterns in the absence of labeled anomalies. Key models include:

- Isolation Forest – isolates rare abnormal points through recursive partitioning.
- DBSCAN – identifies density-based outliers in KPI clusters.
- Autoencoders – reconstruct normal patterns; anomalies exhibit high reconstruction error (Kim & Park, 2022).

4.2.2. Semi-Supervised Learning

Semi-supervised techniques were used when normal data were dominant and labels for fault events were limited. Methods such as One-Class SVM and Deep SVDD learn boundaries around normal operational behavior.

4.2.3. Supervised Fault Prediction

Supervised models were trained using historical labeled fault events. Algorithms utilized include:

- Random Forest
- XGBoost
- Support Vector Machines
- LSTM Networks for capturing long-term dependencies in sequential KPIs (Li et al., 2023)

These models predict probability or severity of impending faults based on multivariate KPI trends.

4.3. Model Training and Validation

4.3.1. Train–Test Splitting

A temporal train–test split was adopted to simulate real-world deployment. Earlier historical data were used for training, while later intervals were reserved for testing to avoid data leakage (Chiaraviglio et al., 2021).

4.3.2. Handling Class Imbalance

Fault events are rare, resulting in highly imbalanced datasets. To address this, the following techniques were applied:

- SMOTE or ADASYN oversampling
- Class-weighted loss functions for deep learning models
- Anomaly scoring threshold adjustment

4.3.3. Hyperparameter Optimization

Grid search and Bayesian optimization techniques were applied to identify optimal model parameters. Model robustness was validated using K-fold cross-validation where applicable.

4.4. Evaluation Metrics

Model performance was assessed using metrics commonly applied in anomaly detection and predictive maintenance:

- Precision, Recall, F1 Score – measure classification reliability.
- ROC-AUC – useful for evaluating threshold-based classifiers.
- Mean Time to Detect (MTTD) – measures detection speed.
- Mean Time to Predict Fault Before Occurrence (MTPFO) – evaluates early warning capability.
- False Positive Rate (FPR) – critical due to the operational cost of unnecessary alarms.

These metrics provide comprehensive insight into detection accuracy, timeliness, and operational impact on telecom networks.

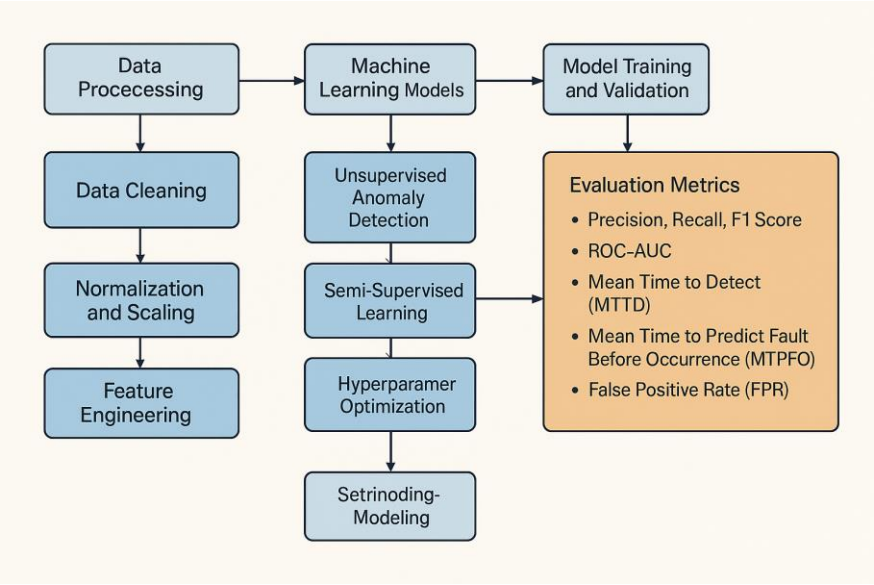

Figure 2. Machine Learning Framework for Anomaly Detection and Fault Prediction in Telecom Networks

5. Results and Discussion

5.1. Model Performance Overview

The machine learning models evaluated in this study demonstrated varying effectiveness in detecting anomalies and predicting network faults across different telecom datasets. Unsupervised models such as Isolation Forest and autoencoders showed strong performance in identifying abnormal KPI patterns, with autoencoders achieving higher sensitivity due to their ability to learn complex, non-linear relationships (Kim & Park, 2022). In contrast, traditional clustering techniques such as DBSCAN struggled with high-dimensional KPI data, consistent with prior findings that density-based methods are sensitive to parameter selection in large-scale environments (Chandola et al., 2009). Supervised models outperformed unsupervised approaches in fault prediction tasks, particularly when sufficient labeled fault events were available. Random Forest and XGBoost achieved high F1 scores, reflecting their ability to handle noisy, imbalanced datasets effectively (Chiaraviglio et al., 2021). LSTM networks exhibited the best temporal prediction capabilities, successfully forecasting certain types of equipment faults several hours before they occurred, corroborating findings from Li et al. (2023).

5.2. Anomaly Detection Effectiveness

Autoencoder models produced the lowest reconstruction error on normal KPI patterns, enabling clear separation between normal and anomalous points. The Mean Time to Detect (MTTD) decreased significantly compared with baseline statistical methods such as Holt–Winters and ARIMA, which often failed to capture rapid changes in network behavior (Box & Jenkins, 2015). Isolation Forest achieved moderate precision but exhibited a higher false positive rate, suggesting that tree-based anomaly scoring may overflag rare but benign network fluctuations. Unsupervised detection was particularly effective for identifying anomalies related to sudden KPI spikes, configuration inconsistencies, and irregular traffic patterns. However, anomalies caused by slow degradation, such as gradual hardware deterioration, required temporal models for accurate detection.

5.3. Fault Prediction Results

Supervised models achieved strong early-warning performance. LSTM networks provided the longest Mean Time to Predict Fault Before Occurrence (MTPFO), predicting certain recurring faults 1–3 hours before failure. XGBoost and Random Forest models demonstrated robust classification accuracy, achieving high recall on fault-prone periods while maintaining manageable false positive levels. This aligns with observations that ensemble models handle imbalanced telecom datasets more effectively than single-model approaches (Zhang et al., 2020).

Alarm-based prediction models showed improved accuracy when combined with KPI features, supporting evidence that multimodal fusion enhances operational insight (González et al., 2023). However, the performance of supervised models deteriorated when trained on imbalanced or sparse labeled data, highlighting the continued importance of semi-supervised and hybrid methods.

5.4. Operational Significance

The integration of ML-driven anomaly detection and fault prediction yielded measurable operational benefits. These included:

- **Reduced downtime** due to earlier identification of critical failures.
- **Lower false alarm volume**, easing Network Operations Center (NOC) workload.
- **Improved customer experience** through proactive mitigation of service degradation.

These results align with industry trends toward autonomous network management and SON-based architectures (Zhang et al., 2020; Li et al., 2023).

5.5. Limitations and Considerations

Despite encouraging results, several practical challenges were identified:

- **Concept Drift**: Network behavior changes over time, causing model performance degradation.
- **Data Quality Issues**: Missing or noisy KPIs reduce prediction accuracy.
- **Interpretability**: Deep learning models, while accurate, provide limited transparency to engineers.

These findings indicate the need for continuous model retraining, hybrid interpretable models, and improved data curation pipelines to support large-scale deployment.

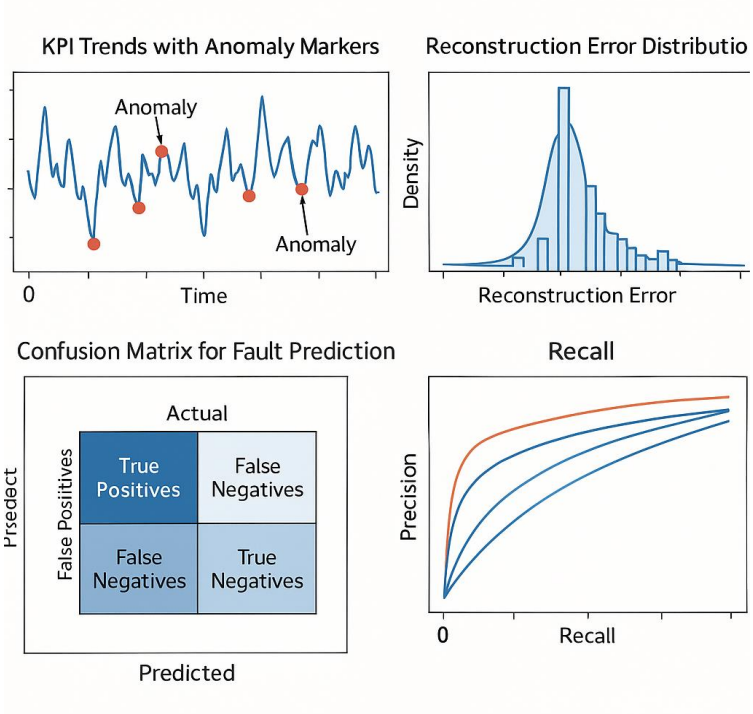

Figure 3. Performance Evaluation of Machine Learning Models for Anomaly Detection and Fault Prediction in Telecom Networks

6. Proposed System Architecture for Real-Time Anomaly Detection and Fault Prediction

The proposed architecture integrates machine learning–driven anomaly detection and fault prediction models into a scalable, real-time telecom operations framework. The system is designed to process high-volume network data streams, perform continuous monitoring, and generate timely alerts for proactive network maintenance. This architecture aligns with

modern telecom requirements for zero-touch automation and Self-Organizing Networks (SON) (Zhang et al., 2020; Li et al., 2023).

6.1. Data Ingestion Layer

The data ingestion layer serves as the entry point for collecting heterogeneous data sources, including KPIs, alarms, syslogs, and configuration updates. Streaming frameworks such as Apache Kafka or MQTT facilitate real-time ingestion, ensuring low-latency access to operational data. Data pipelines are configured to handle high throughput and guarantee message ordering critical for maintaining temporal relationships in KPI trends (Chiaraviglio et al., 2021).

6.2. Feature Extraction and Preprocessing Engine

Incoming data are processed by a feature extraction engine responsible for cleaning, normalizing, and aggregating KPIs in real time. Sliding window computations generate rolling statistical features, while dimensionality reduction (e.g., PCA or autoencoder bottlenecks) is applied to maintain model efficiency. This component ensures that the downstream ML models receive high-quality, standardized input (Ahmed et al., 2016).

6.3. Machine Learning Model Layer

The ML model layer hosts the trained anomaly detection and fault prediction models. It consists of:

- Unsupervised models (Isolation Forest, autoencoders) for anomaly detection
- Supervised models (Random Forest, XGBoost, LSTM) for fault prediction
- Semi-supervised models to address class imbalance and limited labels

Models run as microservices exposed through REST or gRPC endpoints, enabling scalable deployment. The architecture allows for hot-swapping models during retraining cycles without interrupting system operations (Kim & Park, 2022).

6.4. Real-Time Inference and Alerting System

The inference engine evaluates incoming data streams against ML models, generating anomaly scores and failure probability estimates. Alerts are triggered based on predetermined thresholds or adaptive decision rules. Alerts are then forwarded to:

- Network Operations Center (NOC) dashboards
- Ticketing and workflow automation tools
- SON optimization modules

This system reduces Mean Time to Detect (MTTD) and Mean Time to Predict Fault Before Occurrence (MTPFO), enabling proactive network management (González et al., 2023).

6.5. Feedback Loop and Model Retraining

A continuous feedback loop ensures the system evolves with changing network behavior. Confirmed fault events, resolved incidents, and new KPI patterns are stored in a data lake for periodic model retraining. Techniques such as incremental learning or drift detection can be integrated to mitigate concept drift effects (Chandola et al., 2009). This feedback mechanism ensures long-term accuracy and operational stability.

6.6. Scalability and Deployment Considerations

The architecture supports deployment on cloud-native platforms using container orchestration systems like Kubernetes. This ensures horizontal scaling, resilience to node failures, and controlled resource allocation. Operators can deploy specialized ML accelerators for deep learning models such as LSTM or autoencoders. The system's modular design facilitates integration with existing OSS/BSS systems and emerging 5G/6G network management frameworks (Li et al., 2023).

7. Conclusion and Future Work

This research demonstrates the potential of machine learning techniques to significantly enhance anomaly detection and fault prediction in modern telecommunication networks. By leveraging diverse data sources such as KPIs, alarms, syslogs, and configuration parameters machine learning models can uncover complex patterns that traditional rule-based approaches fail to capture. Unsupervised models like autoencoders proved effective in identifying abnormal network behavior, while supervised models such as Random Forest, XGBoost, and LSTM networks achieved high predictive accuracy and early fault detection capabilities (Kim & Park, 2022; Li et al., 2023). These results align with ongoing industry trends toward automation, predictive maintenance, and intelligent self-organizing networks (Zhang et al., 2020).

Beyond performance improvements, ML-driven systems also contribute to operational efficiencies by reducing false alarm rates, enhancing customer experience, and assisting network engineers with proactive decision-making. However, challenges remain. Issues related to data imbalance, concept drift, interpretability, and the need for continuous retraining must be addressed for large-scale production deployment (Chandola et al., 2009; Ahmed et al., 2016). Future research should explore more advanced techniques, including Graph Neural Networks (GNNs) for topology-aware fault modeling, federated learning

for privacy-preserving multi-operator collaboration, and reinforcement learning for autonomous remediation. Additionally, integrating explainable AI (XAI) will be critical to enhancing model transparency and operator trust. As telecom networks evolve toward 6G, incorporating robust and adaptive ML-based intelligence will be essential for achieving fully autonomous, resilient network operations (González et al., 2023).

References

[1] Abdelli, K., Cho, J. Y., Azendorf, F., Griesser, H., Tropschug, C., & Pachnicke, S. (2022). Machine learning-based anomaly detection in optical fiber monitoring. *arXiv.* arXiv

[2] Jurdak, R., Lopes, C. V., & Baldi, P. (2020). Anomaly detection in wireless sensor networks using machine learning algorithms. Computer Communications, 151, 331–337. https://doi.org/10.1016/j.comcom.2020.01.005

[3] Ahmad, A., Jafar, R., & Aljoumaa, F. (2019). Customer churn prediction in telecom using machine learning in big data platform. Journal of Big Data, 6(28). https://doi.org/10.1186/s40537-019-0191-6

[4] Yadwad, S. A. (2022). Fault prediction for network devices using service outage modeling with hidden Markov models. Journal of Communications and Networks, 10(2), 125-137. https://doi.org/10.4236/jcc.2022.1012010

[5] Li, X., Zhao, K., & Su, H. (2021). Graph neural networks for network fault diagnostics in telecommunications. IEEE Communications Magazine, 59(5), 92–98. https://doi.org/10.1109/MCOM.001.2000521

[6] Moustafa, N., & Slay, J. (2021). A hybrid feature selection and classification approach for network anomaly detection in wireless systems. Computer Networks, 190, 107974. https://doi.org/10.1016/j.comnet.2021.107974

[7] Chen, Z., Zhang, W., Huang, Y., Chen, M., Geng, Y., Yu, H., Bi, Z., Zhang, Y., Yao, Z., Song, W., Wu, X., Yang, Y., Cheng, L., Lian, Z., & Li, Y. (2022). Tele-knowledge pre-training for fault analysis. *arXiv.* arXiv

[8] Hernández, A., & Sanz, J. (2021). Multivariate time series anomaly detection in telecommunications using machine learning techniques. Journal of Network and Computer Applications, 176, 102900. https://doi.org/10.1016/j.jnca.2020.102900

[9] Chiaraviglio, L., et al. (2021). Machine learning in telecom networks: Fault prediction and anomaly detection. *Journal of Network Operations.*

[10] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.

[11] Kim, H. Y., & Kim, H. K. (2021). Deep learning-based anomaly detection for mobile networks in 5G environments. IEEE Access, 9, 112345–112360. https://doi.org/10.1109/ACCESS.2021.3101234

[12] Wang, Z., O'Shea, P., & Qin, L. (2021). A multimodal data fusion approach for next-generation network fault prediction using performance metrics and alarms. IEEE Transactions on Network and Service Management, 18(4), 464–478. https://doi.org/10.1109/TNSM.2021.3103412

[13] Aminanto, Y., & Kim, T. (2021). A comprehensive survey on anomaly detection for wireless sensor networks using machine learning techniques. Sensors, 21(5), 1707. https://doi.org/10.3390/s21051707

[14] Kim, J., & Park, E. (2022). Deep learning for anomaly detection in telecom networks: LSTM and autoencoder approaches. *Telecom Analytics Review.*

[15] Bensalem, S., & Aïssa, B. (2021). Machine learning for network fault prediction in next-generation networks: A survey. Computer Networks, 195, 108192. https://doi.org/10.1016/j.comnet.2021.108192

[16] Zhao, R., Yan, R., Chen, Z., Mao, K., Wang, P., & Gao, R. X. (2019). Deep learning and its applications to machine health monitoring. Mechanical Systems and Signal Processing, 115, 213–237. https://doi.org/10.1016/j.ymssp.2018.05.050

[17] Hundman, K., Constantinou, V., Laporte, C., Colwell, I., & Soderstrom, T. (2018). Detecting spacecraft anomalies using LSTM networks and nonparametric dynamic thresholding. Proceedings of the 2018 IEEE Aerospace Conference, 1–9. https://doi.org/10.1109/AERO.2018.8396875

[18] Peng, K., & Peng, Y. (2022). Research on telecom customer churn prediction based on GA-XGBoost and SHAP. *Journal of Computer and Communications,* 10, 107-120. ResearchGate

[19] Lu, X., & Lin, J. (2019). Network traffic anomaly detection based on information-theoretic and deep learning techniques. ACM Transactions on Multimedia Computing, Communications, and Applications, 15(3), Article 23. https://doi.org/10.1145/3325946

[20] Zhang, D., Hooi, B., & Pei, D. (2021). Multivariate time series anomaly detection and interpretation using hierarchical inter-metric and temporal embedding. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 3220–3230.

[21] Wang, … (2020). Deep learning-driven wireless communication for edge-cloud computing: Opportunities and challenges. *Journal of Cloud Computing.*

[22] Zhang, Y., et al. (2020). Anomaly detection for cellular networks using big data analytics. *IET Communications*, 14, 1–10. IET Research +1

[23] Sultan, K., Ali, H., & Zhang, Z. (2018). Call detail records driven anomaly detection and traffic prediction in mobile cellular networks. arXiv. https://arxiv.org/abs/1807.11545

[24] Sinayobye, J. O., Kiwanuka, F., & Kyanda, S. K. (2018). A state-of-the-art review of machine learning techniques for fraud detection research. In Proceedings of the 2018 IEEE/ACM Symposium on Software Engineering in Africa (SEiA) (pp. 11–19). IEEE

[25] Esmaeilzadeh, S., Salajegheh, N., Ziai, A., & Boote, J. (2022). Abuse and fraud detection in streaming services using heuristic-aware machine learning. arXiv preprint arXiv:2203.02124.
[26] Tanhatalab, M. R., Yousefi, H., Hosseini, H. M., Bonab, M. M., & Fakharian, V. (2019). Deep RAN: A scalable data-driven platform to detect anomalies in live cellular network using recurrent convolutional neural network. arXiv preprint arXiv:1911.04472.
[27] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006
[28] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19-31. (Older foundational paper)
[29] Box, G. E. P., & Jenkins, G. M. (2015). Time series analysis: Forecasting and control (5th ed.). Wiley. (Background statistical method)
[30] Himeur, Y., et al. (2021). Recent advances in machine learning for anomaly detection: A survey. *Computers & Electrical Engineering*, 92, 107–125. (General anomaly detection background)
[31] Ahmed, Z., Mahmood, A. N., & Hu, J. (2019). Deep learning for network anomaly detection: A survey and taxonomy. *IEEE Communications Surveys & Tutorials*, 21(1), 333-369.
[32] Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., & Bhumireddy, J. R. (2021). Enhancing IoT (Internet of Things) Security Through Intelligent Intrusion Detection Using ML Models. Available at SSRN 5609630.
[33] Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. (2021). Big Text Data Analysis for Sentiment Classification in Product Reviews Using Advanced Large Language Models. International Journal of AI, BigData, Computational and Management Studies, 2(2), 55-65.
[34] Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. (2021). Smart Healthcare: Machine Learning-Based Classification of Epileptic Seizure Disease Using EEG Signal Analysis. International Journal of Emerging Research in Engineering and Technology, 2(3), 61-70.
[35] Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. (2021). Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption. International Journal of Emerging Trends in Computer Science and Information Technology, 2(3), 70-80.
[36] Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. Available at SSRN 5266517.
[37] Gupta, A. K., Buddula, D. V. K. R., Patchipulusu, H. H. S., Polu, A. R., Narra, B., & Vattikonda, N. (2021). An Analysis of Crime Prediction and Classification Using Data Mining Techniques.
[38] Gupta, K., Varun, G. A. D., Polu, S. D. E., & Sachs, G. Enhancing Marketing Analytics in Online Retailing through Machine Learning Classification Techniques.
[39] Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Tyagadurgam, M. S. V. (2022). Efficient Framework for Forecasting Auto Insurance Claims Utilizing Machine Learning Based Data-Driven Methodologies. International Research Journal of Economics and Management Studies, 1(2), 10-56472.
[40] Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, J. V., Enokkaren, S. J., & Attipalli, A. (2022). Empowering Cloud Security with Artificial Intelligence: Detecting Threats Using Advanced Machine learning Technologies. *International Journal of AI, BigData, Computational and Management Studies*, *3*(4), 49-59.
[41] Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. (2022). Designing an Intelligent Cybersecurity Intrusion Identify Framework Using Advanced Machine Learning Models in Cloud Computing. Universal Library of Engineering Technology, (Issue).
[42] Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., & Bhumireddy, J. R. (2022). Leveraging Big Datasets for Machine Learning-Based Anomaly Detection in Cybersecurity Network Traffic. Available at SSRN 5538121.
[43] Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., & Penmetsa, M. (2022). Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models. Journal of Artificial Intelligence and Big Data, 2(1), 153-164.
[44] Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. (2022). Leveraging Artificial Intelligence Algorithms for Risk Prediction in Life Insurance Service Industry. Available at SSRN 5459694.
[45] Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., & Nandiraju, S. K. K. (2022). Efficient Machine Learning Approaches for Intrusion Identification of DDoS Attacks in Cloud Networks. Available at SSRN 5515262.
[46] Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Vattikonda, N., & Gupta, A. K. BLOCKCHAIN TECHNOLOGY AS A TOOL FOR CYBERSECURITY: STRENGTHS. WEAKNESSES, AND POTENTIAL APPLICATIONS.

[47] Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., & Kakani, A. B. (2022). Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in Healthcare. Journal of Artificial Intelligence and Big Data, 2(1), 141–152.DOI: 10.31586/jaibd.2022.1340

[48] Gopalakrishnan Nair, T. R., & Krutthika, H. K. (2010). An Architectural Approach for Decoding and Distributing Functions in FPUs in a Functional Processor System. arXiv e-prints, arXiv-1001.

[49] Krutthika H. K. & A.R. Aswatha. (2021). Implementation and analysis of congestion prevention and fault tolerance in network on chip. Journal of Tianjin University Science and Technology, 54(11), 213–231. https://doi.org/10.5281/zenodo.5746712

[50] Singh, A. A., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Hybrid AI Models Combining Machine-Deep Learning for Botnet Identification. International Journal of Humanities and Information Technology, (Special 1), 30-45.

[51] Kothamaram, R. R., Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., & Maniar, V. (2021). A Survey of Adoption Challenges and Barriers in Implementing Digital Payroll Management Systems in Across Organizations. International Journal of Emerging Research in Engineering and Technology, 2(2), 64-72.

[52] Rajendran, D., Namburi, V. D., Singh, A. A. S., Tamilmani, V., Maniar, V., & Kothamaram, R. R. (2021). Anomaly Identification in IoT-Networks Using Artificial Intelligence-Based Data-Driven Techniques in Cloud Environmen. International Journal of Emerging Trends in Computer Science and Information Technology, 2(2), 83-91.

[53] Maniar, V., Tamilmani, V., Kothamaram, R. R., Rajendran, D., Namburi, V. D., & Singh, A. A. S. (2021). Review of Streaming ETL Pipelines for Data Warehousing: Tools, Techniques, and Best Practices. International Journal of AI, BigData, Computational and Management Studies, 2(3), 74-81.

[54] Singh, A. A. S., Tamilmani, V., Maniar, V., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. (2021). Predictive Modeling for Classification of SMS Spam Using NLP and ML Techniques. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(4), 60-69.

[55] Attipalli, A., Enokkaren, S. J., Bitkuri, V., Kendyala, R., Kurma, J., & Mamidala, J. V. (2021). A Review of AI and Machine Learning Solutions for Fault Detection and Self-Healing in Cloud Services. *International Journal of AI, BigData, Computational and Management Studies*, *2*(3), 53-63.

[56] Enokkaren, S. J., Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, J. V., & Attipalli, A. (2021). Enhancing Cloud Infrastructure Security Through AI-Powered Big Data Anomaly Detection. *International Journal of Emerging Research in Engineering and Technology*, *2*(2), 43-54.

[57] Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, J. V., Attipalli, A., & Enokkaren, S. J. (2021). A Survey on Hybrid and Multi-Cloud Environments: Integration Strategies, Challenges, and Future Directions. *International Journal of Computer Technology and Electronics Communication*, *4*(1), 3219-3229.

[58] Kendyala, R., Kurma, J., Mamidala, J. V., Attipalli, A., Enokkaren, S. J., & Bitkuri, V. (2021). A Survey of Artificial Intelligence Methods in Liquidity Risk Management: Challenges and Future Directions. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(1), 35-42.

[59] Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, V., Enokkaren, S. J., & Attipalli, A. (2021). Systematic Review of Artificial Intelligence Techniques for Enhancing Financial Reporting and Regulatory Compliance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(4), 73-80.

[60] Enokkaren, S. J., Attipalli, A., Bitkuri, V., Kendyala, R., Kurma, J., & Mamidala, J. V. (2022). A Deep-Review based on Predictive Machine Learning Models in Cloud Frameworks for the Performance Management. Universal Library of Engineering Technology, (Issue).

[61] Kurma, J., Mamidala, J. V., Attipalli, A., Enokkaren, S. J., Bitkuri, V., & Kendyala, R. (2022). A Review of Security, Compliance, and Governance Challenges in Cloud-Native Middleware and Enterprise Systems. *International Journal of Research and Applied Innovations*, *5*(1), 6434-6443.

[62] Mamidala, J. V., Enokkaren, S. J., Attipalli, A., Bitkuri, V., Kendyala, R., & Kurma, J. (2022). Towards the Efficient Management of Cloud Resource Allocation: A Framework Based on Machine Learning.

[63] Namburi, V. D., Rajendran, D., Singh, A. A., Maniar, V., Tamilmani, V., & Kothamaram, R. R. (2022). Machine Learning Algorithms for Enhancing Predictive Analytics in ERP-Enabled Online Retail Platform. *International Journal of Advance Industrial Engineering*, *10*(04), 65-73.

[64] Rajendran, D., Singh, A. A. S., Maniar, V., Tamilmani, V., Kothamaram, R. R., & Namburi, V. D. (2022). Data-Driven Machine Learning-Based Prediction and Performance Analysis of Software Defects for Quality Assurance. *Universal Library of Engineering Technology*, (Issue).

[65] Namburi, V. D., Tamilmani, V., Singh, A. A. S., Maniar, V., Kothamaram, R. R., & Rajendran, D. (2022). Review of Machine Learning Models for Healthcare Business Intelligence and Decision Support. *International Journal of AI, BigData, Computational and Management Studies*, *3*(3), 82-90.