Artificial Intelligence Review (2025) 58:100
https://doi.org/10.1007/s10462-025-11108-x

Artificial intelligence advances in anomaly detection for telecom networks

Enerst Edozie[1] · Aliyu Nuhu Shuaibu[1] · Bashir Olaniyi Sadiq[1] · Ukagwu Kelechi John[1]

Accepted: 7 January 2025 / Published online: 25 January 2025

Abstract
Telecommunication networks are becoming increasingly dynamic and complex due to the massive amounts of data they process. As a result, detecting abnormal events within these networks is essential for maintaining security and ensuring seamless operation. Traditional methods of anomaly detection, which rely on rule-based systems, are no longer effective in today's fast-evolving telecom landscape. Thus, making AI useful in addressing these shortcomings. This review critically examines the role of Artificial Intelligence (AI), particularly deep learning, in modern anomaly detection systems for telecom networks. It explores the evolution from early strategies to current AI-driven approaches, discussing the challenges, the implementation of machine learning algorithms, and practical case studies. Additionally, emerging AI technologies such as Generative Adversarial Networks (GANs) and Reinforcement Learning (RL) are highlighted for their potential to enhance anomaly detection. This review provides AI's transformative impact on telecom anomaly detection, addressing challenges while leveraging 5G/6G, edge computing, and the Internet of Things (IoT). It recommends hybrid models, advanced data preprocessing, and self-adaptive systems to enhance robustness and reliability, enabling telecom operators to proactively manage anomalies and optimize performance in a data driven environment.

Keywords Anomaly detection · AI · Machine learning · Deep learning · Telecommunication networks · Network security

Abbreviations

AI	Artificial Intelligence
RL	Reinforcement Learning
5G	Fifth Generation (wireless technology)
IoT	Internet of Things
ML	Machine Learning
DL	Deep Learning

✉ Enerst Edozie
edozie.enerst.11275@studwc.kiu.ac.ug

[1] Department of Electrical Engineering, Kampala International University, 20000 Ishaka, Uganda

ADS	Anomaly Detection System
SVM	Support Vector Machine
DNN	Deep Neural Network
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
SDN	Software-Defined Networking
NFV	Network Functions Virtualization
GAN	Generative Adversarial Network
GAT	Graph Attention Network
TGN	Temporal Graph Network
VAE	Variational Autoencoder
XAI	Explainable Artificial Intelligence
BNN	Bayesian Neural Network
SNN	Spiking Neural Network
DBN	Deep Belief Network
SOM	Self-Organizing Map
KBS	Knowledge-Based System
k-NN	K-Nearest Neighbors
LOF	Local Outlier Factor
PCA	Principal Component Analysis
FC	Fully Connected (layer)
GRU	Gated Recurrent Unit
GNN	Graph Neural Network
GMM	Gaussian Mixture Model
HMM	Hidden Markov Model
LSTM	Long Short-Term Memory
DDoS	Distributed Denial of Service
t-SNE	T-Distributed Stochastic Neighbor Embedding
KBES	Knowledge-Based Expert System
DBSCAN	Density-Based Spatial Clustering of Applications with Noise

1 Introduction

The primary goal of anomaly detection in telecom infrastructure is to identify and mitigate existing and potential threats to the security, reliability, and performance of telecommunication systems. As modern telecom networks grow larger, support increasingly complex traffic patterns, and integrate emerging communication technologies, traditional rule-based approaches to anomaly detection are no longer sufficient (Abbasi et al. 2021). These legacy systems struggle to scale, adapt, and provide real-time responses in the face of expanding data volumes and evolving threats (Bhattacharyya and Kalita 2013). This leads to faults and unexpected events. Faults or unexpected network events significant losses, degradation in service levels, and serious security breaches, make anomaly detection critical for network availability and security. Consequently, the urgency of real-time anomaly detection in telecom stems from the need to prevent unexpected events and faults while ensuring continuous service, optimization of performance, and preventing security threats such as DDoS

attacks, fraud, and data breaches (Nv et al. 2024). This is achievable with the use of AI in the telecoms sector.

The use of AI-based methods, particularly those leveraging Machine Learning (ML) and Deep Learning (DL), has proven highly effective in modern telecom anomaly detection. These technologies enable systems to learn from vast datasets, identifying abnormal behavior patterns more efficiently and accurately than manual or rule-based approaches. AI models, particularly deep learning algorithms, are uniquely suited to telecom environments where data is vast, dynamic, and distributed. These models, capable of self-learning, continuously improve over time, adapting to the changing patterns of network traffic and evolving threats. By analyzing real-time data, AI systems can detect previously unknown anomalies, making them invaluable in today's telecom networks, where threats are becoming more sophisticated. The transition towards AI-driven anomaly detection has marked a paradigm shift in telecom, enhancing operational efficiency, service reliability, and security. As shown in Fig. 1, the exponential increase in network data over the past decade underscores the importance of integrating AI technologies into telecom systems. AI-driven models such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders are well-equipped to handle the real-time, high-volume data streams characteristic of telecom, allowing providers to monitor network health continuously and respond proactively to emerging issues (Chander et al. 2024).

In practice, AI-based systems can consume enormous volumes of data, learn the normal behavior of various network layers, and recognize deviations or anomalies that may signal a fault, attack, or service degradation. These systems not only provide real-time alerts but also offer recommendations for mitigating risks, thereby improving overall network resilience. Moreover, AI-based approaches can significantly enhance network security by predicting and preventing unauthorized access, cyberattacks, and resource misuse. For instance, advanced methods like LSTM-based Variational Autoencoder-GAN (VAE-GAN) have been successfully applied to detect complex anomalies such as network latency issues, while Federated Learning and Edge Computing are being leveraged to enhance anomaly detection

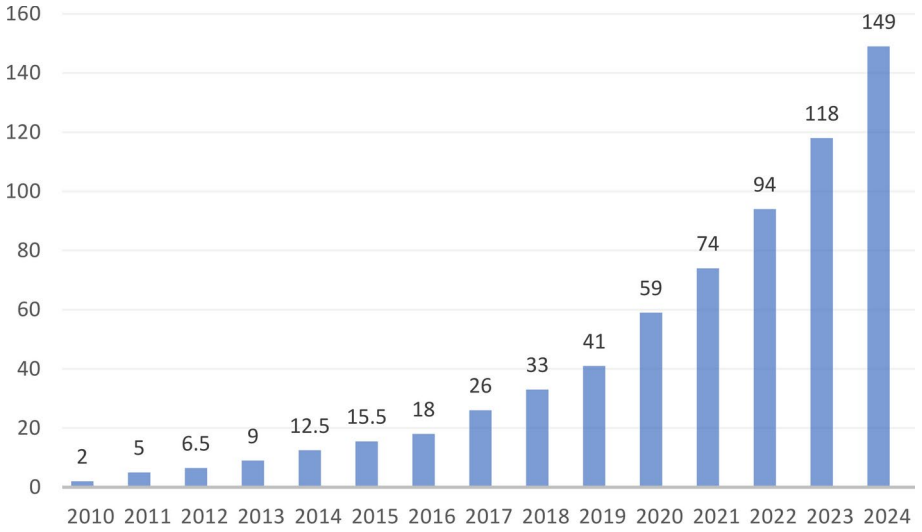

Fig. 1 Data Growth Worldwide 2010–2024

in distributed telecom architectures. These technologies empower telecom providers to stay ahead of evolving threats and ensure the stability of their networks.

Therefore, the integration of AI in anomaly detection systems marks a breakthrough in telecommunications, offering a powerful solution for identifying and mitigating network anomalies in real-time. As the telecom industry continues to evolve, driven by the adoption of 5G, edge computing, and IoT devices, AI technologies will play an increasingly critical role in ensuring the security, reliability, and performance of global communication networks.

2 Historical context of anomaly detection in telecom infrastructure

The evolution of anomaly detection in telecom infrastructure reflects technological advancements as well as the increasing complexity of telecommunications networks. Since the 1960s, the field has evolved from manual methods with set threshold values to advanced AI and deep learning techniques. As summarized in Table 1, early approaches relied heavily on manual configurations and static rules, which were limited in scalability and adaptability. Key milestones include the introduction of automated rule-based systems in the 1980s, enabling basic anomaly detection through predefined thresholds. In the 2000s, the rise of machine learning technology (Fernandes et al. 2019) brought statistical and predictive models that improved detection accuracy and scalability. More recently, advancements in deep learning have enabled real-time analysis of high-volume, complex datasets, significantly enhancing detection precision and response speed. These advancements highlight the field's path toward handling large datasets with faster, more accurate anomaly detection and response capabilities, reflecting the advancements in telecom network technology.

2.1 Early approaches and challenges in anomaly detection

Historically, rule-based systems, primarily utilizing expert knowledge, served as the primary method for anomaly detection in telecommunications. Network administrators and network engineers define certain standards and tolerance levels based on network usage, knowledge, and field experience (Buda et al. 2017; Yao et al. 2018; Palakurti 2024). Network administrators and engineers apply these rules to maintain traffic control on the network, and use additional measure parameters to trigger alarms when they violate them. However, the above-mentioned symbol and rule-based approaches faced several limitations. First, they had to spend much time codifying all possible scenarios and establishing multilevel rule systems themselves in a very prescriptive way, which is difficult enough given the burgeoning complexity and size of the underlying networks (Zhang and Zhu 2020). Besides, these approaches were unchanging and rigid; it was challenging to alter them according to the changing situation and the constant emergence of new threats (Chakraborty et al. 2023).

Another issue faced was a high level of false positives and false negatives: rule-based models were unable to take into account all the peculiarities and details of network activity (Cui and Zhang 2021). Moreover, these approaches only functioned after an event, which made it difficult to take action before undesirable incidents occurred, when certain measures could have prevented or reduced adverse outcomes (Cui and Zhang 2021).

Table 1 Showing the history of anomaly detection in telecom infrastructure from 1960 to 2024

Period	Methods/Technologies	Characteristics	Limitations
1960s–1980s	Manual Monitoring & Threshold-Based Systems (Diro et al. 2023; Kourtis et al. 2016; Landin et al. 2021)	Manual detection by operators	High false positives
		Fixed thresholds for parameters	Missed detections due to static thresholds
1980s–1990s	Rule-Based Systems (Afzal and Murugesan 2022; Uszko et al. 2023)	Expert systems using pre-defined rules	Limited by static rules
		Event correlation	High maintenance
1990s–2000s	Statistical Methods & Early Machine Learning (Ali et al. 2020; Wang et al. 2021)	Statistical analysis (moving averages, regression)	Less adaptable to changing network behaviors
		Clustering & classification algorithms (k-means, decision trees)	Initial machine learning applications
2000s–2010s	Advanced Machine Learning (Wang et al. 2021; Lam and Abbas 2003)	Adoption of SVMs, neural networks, and ensemble methods	Computationally intensive
		Data mining for large datasets	Required extensive data for training
2010s–2020s	Big Data & Real-Time Analytics (Habeeb et al. 2019; Parwez et al. 2017; Gulenko et al. 2016)	Integration with big data technologies (Hadoop, Spark)	Real-time processing complexities
		Real-time anomaly detection	High infrastructure costs
2020s–Present	AI & Deep Learning (Savic et al. 2021; Ma 2020; Hussain 2021)	Use of CNNs, and RNNs for complex anomaly detection	Requires significant computational resources
		Automated response systems	Can be opaque ('black box' issues)
		Incorporation of temporal, spatial, and contextual data	

2.2 Evolution of AI techniques for anomaly detection

When the logical-deductive frameworks started proving insufficient for solving highly non-trivial tasks, the focus shifted towards AI and its applicability to the anomaly detection problem. The advancement of ML with both supervised and unsupervised learning led to the more enhanced intelligent and adaptive Anomaly Detection System (ADS), as noted by Habeeb et al. (2019). Popular supervised techniques like support vector machines (SVM), decision trees, and artificial neural networks were first considered for anomaly detection problems (Omar et al. 2013). It is important to note that all these algorithms were trained using labelled datasets on network traffic and performance data that were labelled normal or anomalous. From these labelled examples, the algorithms could then be trained, making it easier for them to find patterns and generate estimates on unknown data (Omar et al. 2013). Though promising results were obtained through the same, they relied on the availability and quality of the labelled data, which, in most cases, were restricted and slow to gather. They suggest this resulted in exploring other generic learning techniques like clustering, density-based approaches, and dimensionality reduction methods (Cui and Zhang 2021). These algorithms could detect anomalies without using the labelled datasets, which is again a strength for using such methods for real-world problems (Cui and Zhang 2021).

2.3 Milestones and breakthroughs in the field

This area of anomaly detection for telecom infrastructures has undergone several landmarks and stages of methods as the AI has grown in progress. One of the critical shifts was the DL algorithms that opened up the possibility of learning higher-level features from data without having to hand-harvest features from raw data (Sarker 2021). Out of all the DNN techniques, CNN and RNN were identified as particularly suitable for anomaly detection tasks applied to network traffic analysis, intrusion detection, and fault diagnosis (Cui and Zhang 2021). Such algorithms can learn patterns and representations from the original data without the need for extra features, and they might employ better features to identify previously unnoticed marginal cases (Pang et al. 2021).

Another significant development was the integration of several MLs into one ensemble learning system, which helped to improve its accuracy and reliability (Habeeb et al. 2019). Less generalization error rate and increased capability of learning from the interaction of different algorithms make the ensemble method appropriate for the dynamic telecommunication network (Boutaba et al. 2018). Some other notable progress includes the deployment of transfer learning and domain adaptation techniques which have significantly enhanced the field. These approaches provided ways through which the models could be trained on one domain. The suggested anomaly detection techniques can be trained on a set of similar datasets originating from different domains such as computer networks to be later tuned in order to optimize their usage for anomaly detection tasks in telecom networks, thus minimizing the requirement for acquiring ground truth data and training from the scratch (Pang et al. 2021). This made model development and deployment a lot quicker and gave telecom providers the edge to deploy their model in network environments and counter threats as they emerged (Cui and Zhang 2021). Furthermore, new sophisticated technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), have evolved to support the integration of AI techniques with enhanced and elastic

anomaly detection mechanisms (Papavassiliou 2020). These are programmable and flexible technologies that can plug into AI-based anomaly detection which needs an integrated and real-time perception of the network hardware architecture (Schmitt 2023). Following the aforementioned, Fig. 2 depicts the Artificial intelligence technology landscape which shows that the possibilities of these state-of-the-art approaches are almost limitless for bringing real change in telecom, for turning the study area into a world where these sophisticated methods of analyzing the impossible would highlight the possible issues, would predict them and would eliminate them with such high degree of accuracy (Alsheibani et al. 2020). Despite this, new problems have been found in the field of detecting strange things in telecom infrastructure. These problems include how to combine AI that can be understood and/or explained, large amounts of different kinds of data, and the actual process of putting AI to use (Ali 2024). Current works in progress follow the same path to overcome these obstacles and optimize the performances of the AI-based anomaly detection technique to guarantee the safety of telecommunication networks (Umoga et al. 2024).

3 Overview of AI techniques for anomaly detection

AI anomaly detection is the identification of recurrent patterns that do not fall within the standard range through the use of artificial intelligence and machine learning. Compared to the conventional methods, AI anomaly detection does not solely operate based on some fixed levels or basic mathematical approaches. It utilizes models that make use of learning from the data presented to them and can adapt to changes in patterns (Himeur et al. 2021). The most commonly employed procedure encompasses data intake, extractive transformation, model development, and further observation. Multivariate regression, neural networks, or clustering algorithms, capture the systematic part of set patterns and train on historical

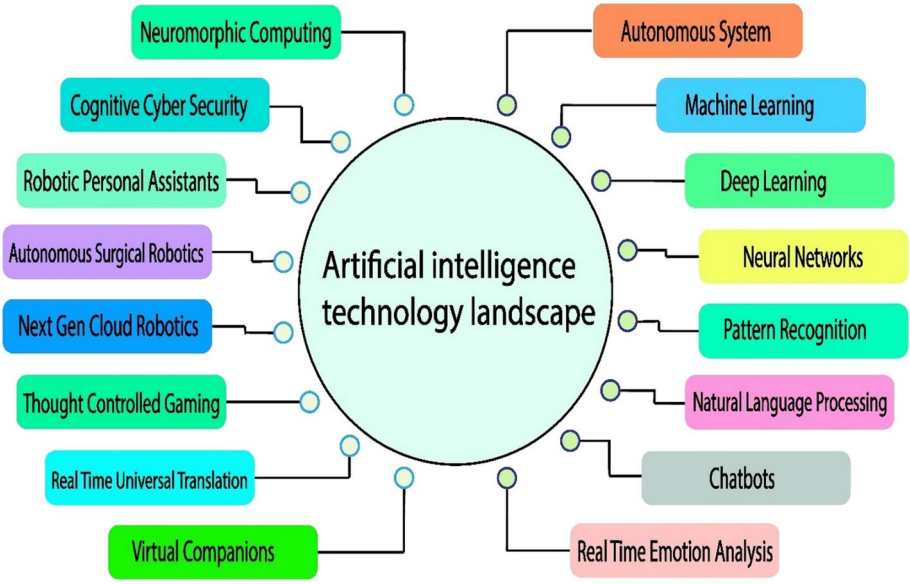

Fig. 2 Artificial intelligence technology landscape

data. These can distinguish outliers in patterns by predicting deviations next time new data streams into the models.

3.1 Machine learning algorithms commonly used in anomaly detection

Numerous studies have been conducted, as well as various applications pertaining to the utilization of ML algorithms for anomaly detection related to telecom structures. These algorithms are broadly classified into methods for supervised, unsupervised, and semi-supervised learning followed by the major strengths and capabilities of each.

SVMs utilized supervised learning algorithms, including decision trees and random forests, as conventional approaches most frequently applied to anomaly detection (Nassif et al. 2021). These algorithms train on labelled or supervised data, wherein initial studies of normal and intrusive behavior are made. As soon as learning is complete, they can differentiate between the input data instances as typical and atypical with practical rates of accuracy (Ali 2024). Nevertheless, the process of acquiring high-quality, labelled data is difficult and takes time, reducing the efficacy of the supervised approaches significantly (Ratner et al. 2016). Some examples of 'other' categories of algorithms include unsupervised learning algorithms, clustering, e.g., center-based methods (k-means, Density-Based Spatial Clustering Application with Noise (DBSCAN)), and density-based methods. Density-based methods tend to detect clusters as regions of high density separated by regions of low density. In outlier detection, algorithms are known based on distance (an analogue of the k-nearest neighbors algorithm, local outlier factor) and dimensionality reduction (an analogue of feature selection). Compared to traditional approaches, dimensionality reduction techniques (e.g., Principal Component Analysis (PCA) and score-based anomaly detection techniques such as t-distribution stochastic neighbor embedding (t-SNE) have recently been widely used for anomaly detection (Cui and Zhang 2021). These are some algorithms that do not involve labelled data, and instead, they use patterns and distributions in given data to detect outré cases (Umoga et al. 2024). Key features, advantages, and challenges of these algorithms are shown in Table 2. It is mainly important when working with applications because, in many cases, obtaining labelled data can be extremely challenging or even impossible, especially for telecom networks (Schmitt 2023). Other approaches that have also been considered in the context of anomaly detection have been raised by researchers which include: Semi-supervised learning approaches, which incorporate some aspects of both supervised and unsupervised learning techniques (Ali 2024). These algorithms use a small set of labelled instances during training alongside an enormous set of unlabeled instances and aim to identify patterns and predict outcomes (Ratner et al. 2016). Semi-supervised learning can prove advantageous in the telecom scenario since getting hold of a large labelled dataset can be quite a challenge in most organizations, but labelled data is not entirely elusive (Cui and Zhang 2021).

3.2 Evaluation of AI techniques in telecom anomaly detection

AI-based anomaly detection in telecom infrastructure encompasses a variety of techniques, each with unique strengths and challenges.

Traditional machine learning methods, such as k-Nearest Neighbors (KNN) (Taunk et al. 2019), Isolation Forest (iForest), and PCA (Gewers et al. 2021; Hasan and Abdulazeez

Table 2 Summary of various machine learning algorithms used in anomaly detection

Algorithm	Category	Description	Key Features	Advantages	Challenges	Applications
NoveltySVR (Ma and Perkins 2003a)	TML	Support Vector Regression for novelty detection	Robust to outliers, handles non-linear data	Good for high-dimensional data	Sensitive to parameter tuning	Telecom network anomaly detection
PS-SVM (Ma and Perkins 2003b)	TML	One-class SVM for detecting anomalies	Effective for high-dimensional data	Robust against noise	Can be slow with large datasets	Fault detection in telecom systems
Ensemble GI (Gao et al. 2001)	EL	Combines multiple algorithms for anomaly detection	High accuracy, and robustness	Can capture diverse patterns	Computationally intensive	Fault detection in telecom systems
GrammarViz (Gao et al. 2001)	TML	Uses grammar-based models for anomaly detection	Interpretable results	Effective for structured data	Requires well-defined grammar	Code analysis, and software debugging
STAMP (Yeh et al. 2016)	TML	Anomaly detection using symbolic aggregate approXimation	Efficient representation of time series	Captures temporal patterns	Sensitive to noise	Time-series data analysis
NumentaHTM (Ahmad et al. 2017)	DL	Hierarchical Temporal Memory for anomaly detection	Mimics human brain processes	Good for sequential data	Requires large amounts of data	Sensor data anomaly detection
S–H-ESD (Hochenbaum et al. 2017)	TML	Seasonal Hybrid Extreme Studentized Deviate for anomaly detection	Good for seasonal data	Robust against outliers	Requires tuning for seasonality	Time-series anomaly detection
XGBoosting (Chen and Guestrin 2016)	EL	Gradient boosting framework for classification	High accuracy and speed	Sensitive to parameter tuning	Requires careful tuning	Fraud detection, network security
TARZAN (Keogh et al. 2002)	DL	Anomaly detection framework for time series data	Efficient for large datasets	Robust to noise and outliers	Requires significant training data	Time-series anomaly detection in network data
OceanWNN (Wang et al. 2019)	DL	Wavelet Neural Network for anomaly detection in time-series data	Effective for non-linear patterns	Sensitive to noise, computationally intensive	Oceanographic data analysis	Time-series analysis, network traffic anomaly detection
Bagel (Li et al. 2018)	DL	Bagel-based approach for structured anomaly detection	Effective for structured data	Limited interpretability	Limited to specific data types	Fraud detection in financial networks
Donut (Xu et al. 2018)	DL	Method for anomaly detection based on donut-shaped distributions	Effective for circular data distributions	Limited to specific data types	Limited interpretability	Anomaly detection in sensor data

Table 2 (continued)

Algorithm	Category	Description	Key Features	Advantages	Challenges	Applications
IE-CAE (Garcia et al. 2022)	DL	Combines CNNs with autoencoders for image-based anomaly detection	Effective for high-dimensional image data	Requires large datasets for training	Limited for non-image data	Image-based anomaly detection
SR-CNN (Ren et al. 2019)	DL	CNN-based method for anomaly detection in sequential data	Captures spatial and temporal patterns	High accuracy	Computationally expensive	Video surveillance, and security systems
KNN (Taunk et al. 2019; Fan et al. 2019; Abu Alfeilat et al. 2019)	TML	k-Nearest Neighbors for anomaly detection	Simple and effective for low-dimensional data	Intuitive interpretation	Computationally expensive for large datasets	Fraud detection in financial transactions
Torsk (Heim and Avery 1909)	TML	A model for anomaly detection in time-series data	Captures temporal dependencies	Effective for trend analysis	Requires careful parameter tuning	Time-series anomaly detection
CBLOF (He et al. 2003)	TML	Clustering-Based Local Outlier Factor for anomaly detection	Combines clustering with LOF	Good for high-dimensional data	Sensitive to clustering algorithms	Network anomaly detection
COPOD (Li et al. 2020)	TML	Copula-based anomaly detection	Captures complex dependencies	Effective for high-dimensional data	Requires careful model selection	Financial fraud detection
iForest (Xu et al. 2023; Lesouple et al. 2021)	TML	Isolation Forest for anomaly detection	Efficient for high-dimensional data	Scalable and effective	Sensitive to parameter tuning	Fault detection in telecom systems
RBForest (Ziegelmeir 2019)	EL	Robust Random Forest for anomaly detection	Combines robustness with ensemble learning	Good for high-dimensional data	Sensitive to parameter tuning	Network anomaly detection
Hybrid KNN (Song et al. 2017)	TML	Combines KNN with other techniques for anomaly detection	Effective for diverse data types	Robust to noise	Sensitive to parameter tuning	Fraud detection, healthcare
DeepAnT (Munir et al. 2018)	DL	Deep Learning approach for time series anomaly detection	Captures complex temporal patterns	High accuracy	Requires large amounts of data	Time-series anomaly detection
DeepNAP (Kim et al. 2018)	DL	Deep learning-based anomaly detection method for time series data	Efficient for large datasets	Good for sequential data	Requires substantial training data	Health monitoring systems

Table 2 (continued)

Algorithm	Category	Description	Key Features	Advantages	Challenges	Applications
LSTM-AD (Malhotra et al. 2015)	DL	LSTM-based anomaly detection for sequential data	Captures long-term dependencies	Good for sequential data	Requires large datasets for training	Time-series anomaly detection
MTAD-GAT (Zhao et al. 2020)	DL	Multi-Task Anomaly Detection with Graph Attention Networks	Captures relationships between variables	High accuracy and scalability	Computationally intensive	Sensor data anomaly detection
Telemanom (Hundman et al. 2018)	DL	End-to-end anomaly detection for time series data in telecom	Effective for operational data	Robust to noise	Requires significant training data	Telecom infrastructure monitoring
MSCRED (Zhang et al. 2019)	DL	Multi-Scale Convolutional Residual Encoder-Decoder for anomaly detection	Captures multi-scale temporal patterns	High accuracy	Requires large amounts of data	Time-series anomaly detection
AE (Sakurada and Yairi 2014; Finke et al. 2021; Michelucci 2201; Provotar et al. 2019; Maleki et al. 2021)	DL	Neural network for unsupervised anomaly detection	Learns to reconstruct data	Effective for high-dimensional data	Sensitive to training data quality	Image processing, finance
DAE (Sakurada and Yairi 2014)	DL	Autoencoder that learns to reconstruct noisy input	Robust to noise	Good for high-dimensional data	Sensitive to parameter tuning	Image denoising, anomaly detection
EncDec-AD (Malhotra et al. 1607)	DL	Encoder-Decoder architecture for anomaly detection	Effective for sequential data	Good for capturing patterns	Requires substantial training data	Time-series anomaly detection
LSTM-VAE (Park et al. 2018)	DL	Variational Autoencoder with LSTM for time series data	Captures complex temporal dependencies	Effective for sequential data	Requires large amounts of data	Time-series anomaly detection
OmniAnomaly (Su et al. 2019)	DL	Omnidirectional Anomaly Detection using deep learning	Robust against noise and outliers	High accuracy	Requires significant training data	Fraud detection, healthcare
TAnoGan (Bashar and Nayak 2020)	DL	Time series anomaly detection using Generative Adversarial Networks	Effective for sequential data	High accuracy	Requires careful parameter tuning	Anomaly detection in finance

Table 2 (continued)

Algorithm	Category	Description	Key Features	Advantages	Challenges	Applications
LaserDBN (Ogbechie et al. 2017)	DL	Laser-based Deep Belief Network for anomaly detection	Captures multi-resolution features	Effective for high-dimensional data	Computationally intensive	Time-series data analysis
NF (Ryzhikov et al. 2021)	DL	Probabilistic model for anomaly detection using flow-based transformations	Effective for high-dimensional data	Good for density estimation	Computationally intensive	Image and video anomaly detection
HIF (Marteau et al. 2017)	TML	Combines Isolation Forest with other techniques	Robust and scalable	Good for high-dimensional data	Sensitive to parameter tuning	Fraud detection, healthcare
DeepLSTM (Chauhan and Vig 2015)	DL	Long Short-Term Memory networks for anomaly detection	Captures long-term dependencies	Effective for sequential data	Requires large amounts of data	Time-series anomaly detection
RADM (Ding et al. 2018)	DL	Recurrent Neural Network for anomaly detection	Captures sequential dependencies	Effective for time series	Requires significant training data	Sensor data analysis
MultiHTM (Li et al. 2017)	DL	Multi-Task Hierarchical Temporal Memory for anomaly detection	Captures complex dependencies	High accuracy	Requires substantial training data	Sensor data anomaly detection
MAD-GAN (Li et al. 2019)	DL	Multi-scale Anomaly Detection with Generative Adversarial Networks	Captures multi-scale features	High accuracy	Requires significant training data	Time-series anomaly detection
LSTM-based VAE-GAN (Niu et al. 2020)	DL	LSTM with Variational Autoencoder and GAN for time series	Captures complex temporal dependencies	High accuracy	Requires significant training data	Time-series anomaly detection
TCN-AE (Thill et al. 2020)	DL	Temporal Convolutional Network for anomaly detection	Effective for sequential data	Good for capturing (Niu et al. 2020) temporal patterns	Requires significant training data	Time-series anomaly detection
PAD (Chen et al. 2021)	DL	Predictive Anomaly Detection using deep learning	Captures temporal dependencies	Effective for sequential data	Requires substantial training data	Sensor data analysis
VELC (Zhang et al. 2019)	DL	Variational Encoder-Decoder for anomaly detection in time series	Captures complex temporal patterns	Effective for sequential data	Requires significant training data	Time-series anomaly detection

2021), offer simplicity and scalability for detecting anomalies in low-dimensional and structured datasets. KNN and LOF, for example, are effective in detecting anomalies in environments where normal and abnormal behavior is well-defined, like fraud detection. However, these models struggle with scalability and high-dimensional data, making them less suited for dynamic, large-scale telecom networks. PCA is efficient for reducing dimensionality and isolating anomalies, though its linearity assumption limits its effectiveness in more complex datasets (Hasan and Abdulazeez 2021).

Deep learning techniques, particularly RNNs (Su et al. 2019; Ergen and Kozat 2019), LSTM (Ergen and Kozat 2019), and autoencoders, offer more advanced solutions by capturing non-linear and temporal dependencies. These models are well-suited for handling sequential data, such as time-series network traffic. LSTM, for instance, excels in detecting long-term patterns and predicting future anomalies. However, deep learning models are computationally expensive and require large volumes of training data, posing a challenge for real-time telecom applications (Ergen and Kozat 2019). The complexity and sensitivity of these models to hyperparameters also add to the operational overhead, making them harder to deploy in large-scale systems without extensive tuning. CNNs, RNNs, and autoencoders are one of the key AI techniques for anomaly detection in telecom networks (Hwang et al. 2020). CNNs extract features from network traffic data to detect attacks like DDoS. RNNs (LSTM/GRU) handle time-series data, detecting faults and intrusions. Autoencoders identify anomalies by reconstructing input data, flagging irregular patterns (Krupski et al. 2021). The architecture of CNN, as illustrated in Fig. 3, consists of convolutional and pooling layers for feature extraction, followed by fully connected layers for classification. This structured design enables CNNs to process spatial features effectively, making them particularly adept at identifying patterns and anomalies in telecom network data.

Hybrid and ensemble approaches are gaining popularity as they combine the strengths of traditional and deep learning methods. Ensemble methods like Random Forest and XGBoost improve accuracy by reducing variance, making them more robust for detecting anomalies in noisy and imbalanced datasets typical in telecom networks. Hybrid methods, such as DeepAnT (Munir et al. 2018), and OmniAnomaly (Su et al. 2019), integrate domain-specific knowledge with AI techniques to improve detection rates for complex patterns and rare events. These approaches are particularly effective for multi-dimensional anomaly detec-

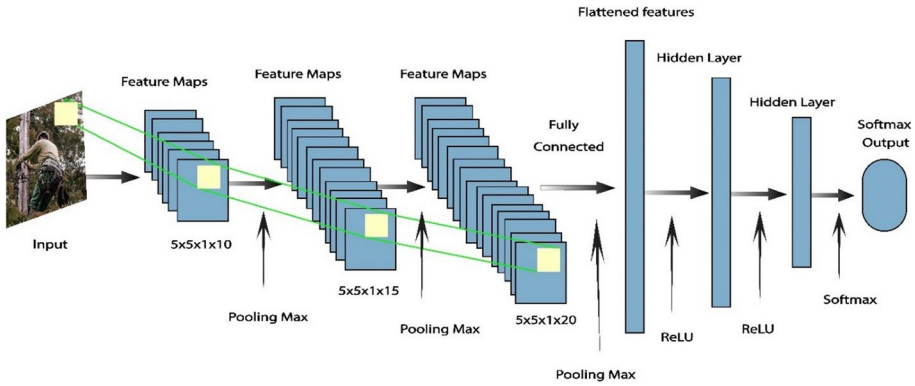

Fig. 3 Showing the Architecture of CNN

tion, where a combination of methods can offer higher robustness and better generalization across different anomaly types.

Emerging trends, such as federated learning and edge computing, are addressing key challenges in telecom anomaly detection, particularly scalability and privacy (Marengo 2024). Federated learning enables models to be trained across distributed devices without centralizing raw data, reducing latency and improving scalability for real-time anomaly detection (Ramineni et al. 2024). This approach is particularly advantageous in telecom networks, where data is often distributed across numerous nodes and privacy is a concern. Edge computing further enhances real-time detection by reducing the computational burden on centralized systems, allowing anomalies to be detected closer to the data source.

while traditional machine learning methods offer simplicity and ease of deployment, advanced deep learning techniques and hybrid approaches provide higher accuracy for complex and dynamic telecom systems. Emerging AI trends like federated learning and edge computing are paving the way for more efficient, scalable, and privacy-preserving solutions. However, the computational demands and data requirements of deep learning models remain a significant hurdle for real-time anomaly detection in telecom infrastructure, requiring ongoing optimization and development (Banik et al. 2023).

3.3 Contextualization of AI techniques in telecom infrastructure

Telecom networks are characterized by high-volume, real-time data streams, distributed architectures, and dynamic traffic patterns. These characteristics heavily influence the choice and effectiveness of AI techniques for anomaly detection, as they necessitate methods that can scale, handle temporal dependencies, and maintain low-latency performance. Understanding these unique aspects of telecom infrastructure is crucial for selecting the appropriate AI-based anomaly detection methods.

Real-time, High-Volume Data: Telecom networks generate vast amounts of data continuously from various sources, such as user activity, network equipment logs, and traffic patterns. The high throughput requires anomaly detection methods that are not only efficient but can also operate in real time. For example, traditional methods like KNN (Abu Alfeilat et al. 2019) or LOF (Xu et al. 2019) struggle with real-time data because of their high computational costs and inability to scale efficiently (Scaranti et al. 2020). On the other hand, techniques like iForest and Random Forest are well-suited for handling large datasets in real time because of their faster decision-making processes, allowing telecom operators to monitor network health with minimal delays.

Practical implementation of these methods can be seen in the use of iForest for fraud detection in telecom, where real-time identification of suspicious activity is critical to prevent financial losses. Similarly, Random Forest has been used in telecom fault monitoring, where multiple data sources need to be analyzed simultaneously for quick identification of anomalies. These methods offer significant benefits over older, rule-based systems, which often miss subtle or evolving threats in the dynamic traffic environment of telecom systems.

Distributed Architecture. Telecom networks are inherently distributed, with data sources spread across numerous nodes, such as base stations, routers, and mobile devices. This architecture poses challenges for centralized AI models due to latency and bandwidth constraints. Therefore, approaches like Federated Learning and Edge Computing are gaining traction, as they enable anomaly detection at the edge of the network, closer to the data

sources. By training models locally on each node, federated learning ensures that data privacy is maintained, a critical concern for telecom providers managing sensitive customer information.

A notable case study involves the use of federated learning for network traffic anomaly detection at the edge of 5G networks. In this scenario, distributed AI models, such as Autoencoders and LSTM, are trained on localized data and aggregated across the network. This approach not only reduces the need for massive data transfers but also ensures that the models adapt to the specific traffic patterns of each region. The results have shown improvements in anomaly detection accuracy while reducing latency, demonstrating the potential of federated learning for handling the distributed nature of telecom networks.

Time-Series Analysis and Temporal Dependencies. The dynamic nature of network traffic in telecom infrastructure calls for methods that can effectively model temporal dependencies. Anomalies often emerge as deviations from expected patterns over time, requiring AI models that can capture and predict time-series data. RNNs and LSTM models excel in these scenarios by learning from historical data to predict future behavior (Wang et al. 2023a). For example, LSTM-based VAE-GAN (Niu et al. 2020) has been applied in telecom for detecting subtle, long-term anomalies in network traffic that traditional models may overlook. These models are particularly effective in detecting service disruptions or slow degradations that occur over extended periods.

LSTM-based models have demonstrated significant efficacy in network anomaly detection, particularly in analyzing time-series datasets such as network latency and packet loss. Their adaptability in managing dynamic and fluctuating traffic loads makes them ideal for identifying unusual patterns that signal potential service disruptions. For instance, a study titled "Anomaly Detection in Telecom Service Provider Network Using LSTM Autoencoder" showcased the utility of LSTM autoencoders in identifying anomalies within multivariate temporal log data. This study achieved high accuracy in detecting abnormal patterns that could preempt service failures, highlighting the potential of LSTM-based models in maintaining telecom network reliability (Vlk 2024). Building on this foundation, further research introduced a hybrid approach in the study "Network Anomaly Detection Using LSTM-Based Autoencoder," which combined LSTM autoencoders with One-Class Support Vector Machines (OC-SVM). This methodology effectively detected deviations such as increased latency or packet loss, reinforcing the critical role of LSTM-based models in enhancing service reliability and preventing disruptions in telecom networks (Said Elsayed et al. 2020).

Scalability and Computational Efficiency: Scalability is another critical factor in selecting AI techniques for anomaly detection in telecom. As networks grow in size and complexity, the computational demands of AI models increase. Techniques like PCA and Autoencoders are frequently employed for dimensionality reduction, making it feasible to analyze large-scale data streams efficiently. These methods reduce the complexity of the data by focusing on the most significant features, allowing real-time detection of anomalies without overwhelming computational resources.

However, scalability often comes at the cost of accuracy. Deep Learning models, while powerful, can struggle with the vast data generated by telecom networks if not properly optimized. To address this, hybrid AI approaches have emerged, combining the speed and simplicity of traditional models with the accuracy of deep learning. For instance, DeepAnT (Munir et al. 2018), a hybrid approach, integrates deep learning with traditional anomaly

detection techniques to improve the scalability of real-time anomaly detection systems. In a telecom deployment, DeepAnT demonstrated superior performance in identifying anomalies in massive, heterogeneous network data, highlighting the importance of hybrid models in balancing scalability and detection accuracy.

Emerging Trends and Future Directions: The integration of AI with domain-specific knowledge and the development of hybrid approaches represent key trends in the evolution of telecom anomaly detection. Hybrid methods like OmniAnomaly, which combines probabilistic and deep learning models, are increasingly being used to detect multi-dimensional anomalies in telecom. These methods address some of the limitations of standalone models by incorporating telecom-specific insights, such as knowledge of network topologies or user behavior patterns, to improve accuracy and reduce false positives.

Looking forward, edge computing and federated learning will continue to play pivotal roles in enhancing real-time anomaly detection across distributed telecom networks. As shown in Fig. 4, AI techniques provide a robust framework for addressing key challenges in telecom infrastructure. Additionally, GANs and Variational Autoencoders, which excel at generating synthetic data, offer promising solutions for detecting rare anomalies that are underrepresented in training datasets. These trends will shape the future of anomaly detection in telecom, addressing challenges like data privacy, scalability, and the dynamic nature of telecom infrastructure.

Therefore, the specific characteristics of telecom networks, such as high-volume real-time data, distributed architectures, and temporal dependencies, strongly influence the choice and effectiveness of AI-based anomaly detection methods. While traditional methods offer simplicity and efficiency, deep learning, hybrid models, and emerging trends like edge computing are driving the future of anomaly detection in telecom by improving scalability, accuracy, and real-time monitoring capabilities.

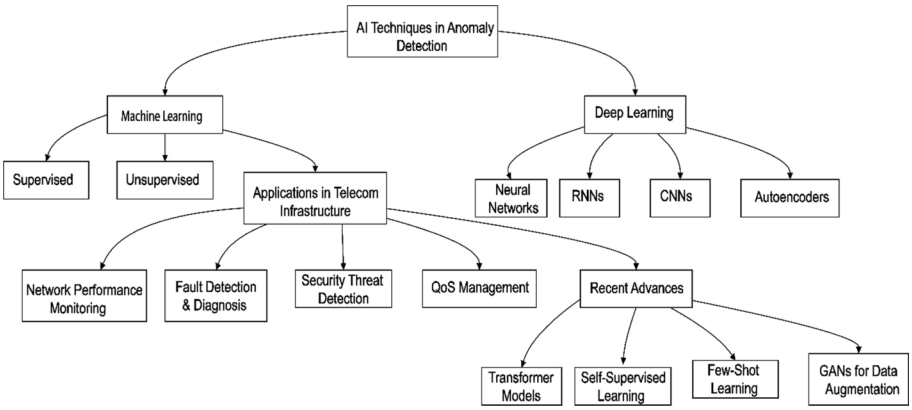

Fig. 4 AI techniques and their applications in telecom infrastructure

4 Methodology

This review employs the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology for selecting research papers. This structured approach ensures the systematic inclusion of relevant studies in the review.

4.1 Inclusion and exclusion criteria

This research systematically explores the application of emerging technologies, such as AI and machine learning, in the field of anomaly detection for telecom networks. The study covers publications directly related to AI-based anomaly detection, with a focus on deep learning, GANs, and RL. The selected papers give valuable insights into advancements in anomaly detection systems, especially in the context of telecom infrastructure. The paper selection criteria are categorized into keyword selection, inclusion and exclusion criteria, and a final analysis of findings.

4.1.1 Selection of keywords

A comprehensive search was conducted in major databases such as Springer, IEEE, Science Direct, Google Scholar, and arXiv. The search utilized a combination of keywords such as AI, machine learning, deep learning, anomaly detection, telecom networks, network security, and 5G to ensure the identification of relevant and high-quality articles pertinent to the topic.

4.1.2 Inclusion

Eligible papers were selected based on their direct relevance to AI-based anomaly detection in telecom networks, particularly those focusing on emerging technologies like 5G, IoT, and edge computing. The selected works include research papers, technical notes, and systematic reviews that analyze AI applications in anomaly detection and network security.

4.1.3 Exclusion

Papers were excluded if they were duplicates, written in languages other than English, or irrelevant to the subject of AI-based anomaly detection in telecom networks. Additional exclusion criteria included articles unrelated to AI or those that did not present original findings, such as editorial notes, short communications, and case series. This approach ensures the review maintains a focus on substantial and relevant contributions to the understanding of AI's role in anomaly detection within telecom networks.

4.2 Quality assessment and data extraction

Given the growing volume of literature on AI applications in telecom, the quality of selected articles was evaluated using the PRISMA checklist. This method ensured that only high-quality studies were included in the review. The PRISMA technique also facilitated the critical assessment of each paper, focusing on the applicability of AI, machine learning

algorithms, and novel techniques in anomaly detection for telecom infrastructure. Figure 5 illustrates the PRISMA process used in this review.

Following a thorough evaluation of 3084 articles gathered from multiple sources (Springer, IEEE, Science Direct, Google Scholar, and arXiv) during the initial stage, 1434 articles were excluded due to duplication across these repositories. Additionally, 1258 articles were removed based on the publication year criteria, and 232 more were excluded due to inaccessibility, lack of relevance, or insufficient quality. Ultimately, after a full review and assessment, 160 articles were selected for inclusion in the study.

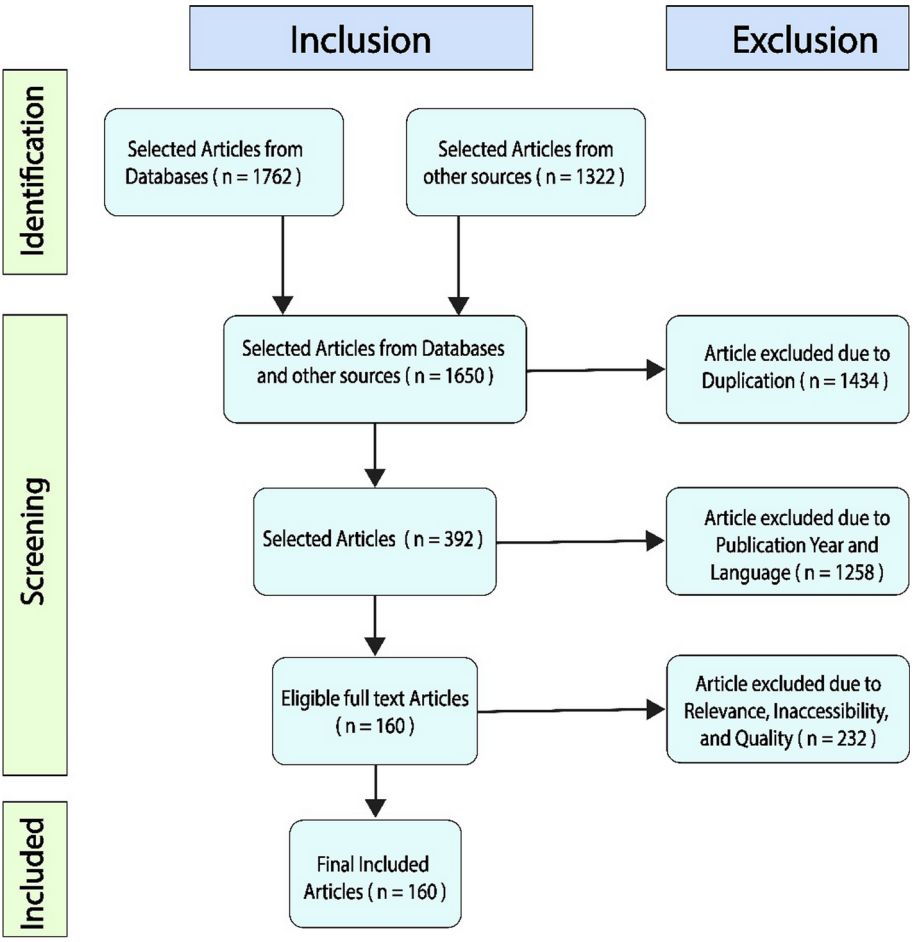

Fig. 5 The PRISMA process used in this review

5 Recent advances in AI for anomaly detection in telecom infrastructure

AI integration especially with a focus on anomaly detection in telecom infrastructure has emerged as one prominent research area over the past few years with numerous research studies and published papers offering a variety of ideas, algorithms, and methodologies. These advancements have been due to an increase in the complexity of the telecom networks, the amount of data, and the new, and more elusive threats. One particular line of work that has been conducted on the application of complex deep learning architectures for the detection of anomalies is chosen. There are also some variants and extensions of available deep learning models like attention mechanisms, capsule networks, and transformer models for improving their performance and adaptability to telecom anomaly detection in terms of performance (Choi et al. 2021). For instance, Javed et al. (2020) proposed an attention-based CNN model aimed at detecting anomalies in mobility traffic data. Compared to careless pooling, attentive pooling enabled one to pay more attention to important features, which helped in the final choice and in spotting fine-grained differences between objects. Similarly, Lin et al. (2023) used capsule network for finding anomalies in the network logs since the capsule network is capable of detecting hierarchical structural or spatial relations. Another area that has received much interest has involved the integration of domains and expertise into artificial intelligence. Researchers have posited techniques that involve the use of the specific knowledge and rules of the problem domain of interest towards the enhancement of the two concerns of interpretability and performance of AI models. For example, Mazini et al. (2019) have proposed a new approach aiming at integrating a KBES and DL for detecting abnormal behaviors in cellular networks. The knowledge base of the expert system is a set of interconnected knowledge and rules to be applied, while the semi-automatic learning component identifies new relations and features in the given data. Further, the works in review have provided a comprehensive look at emerging AI techniques for new generation telecom technologies such as 5G, IoT, and SDN. For instance, Taleb et al. (2023) presented and deployed an AI-empowered anomaly diagnosis mechanism to the high-dimensional data gathered from different 5G network components. Another similar study was Saeed et al. (2023) where the authors proposed an AI-driven approach for anomaly detection in IoT networks, relying solely on unsupervised learning to identify anomalies in resource-constrained IoT devices.

5.1 Examination of novel AI algorithms and methodologies

Researchers have developed novel algorithms and approaches to improve the ability of AI to detect anomalies in telecom infrastructure. Among these approaches, Generative Adversarial Networks (GANs) have emerged as an effective tool for a variety of anomaly detection applications (Goodfellow et al. 2014). As summarized in Table 3, GANs, or Generative Adversarial Networks, are inspired by the two-person zero-sum game from game theory. A GAN consists of two models, the generator network and the discriminator network, which represent the two participants in a minimax game. The generator is trained to model the distribution of genuine data samples and create new samples from that distribution, whereas the discriminator is trained to distinguish between original and created data samples (Schlegl et al. 2019; Tong et al. 2020). In telecom applications, GANs have been utilized for flow-

Table 3 Summary of novel AI algorithms and methodologies for anomaly detection in telecom infrastructure

Algorithm/Methodology	Research Methodology	Application in Telecom	Key Findings
Graph Neural Networks (GNNs) (Li et al. 2024; Chen et al. 2024)	Utilized GNNs for network traffic anomaly detection using graph representations of telecom data	Network traffic anomaly detection	Improved detection of traffic anomalies by modeling network topologies
Graph Attention Networks (GATs) (Wang et al. 2023b; Huang et al. 2019; Veličković et al. 2017)	Applied GATs to telecom network data for anomaly detection, focusing on the importance of specific nodes and edges	Network structure analysis	Enhanced detection accuracy by emphasizing critical graph components
Temporal Graph Networks (TGNs) (Michail 2015; Huang et al. 2014)	Developed a TGN-based approach for detecting anomalies in time-evolving network data	Time-evolving network anomaly detection	Effectively identified dynamic anomalies over time
Self-Supervised Learning (Gui 2024; Jaiswal et al. 2020)	Leveraged self-supervised learning to create feature representations from unlabeled network traffic data	Fault diagnosis	Reduced dependency on labeled data while maintaining high detection rates
Meta-Learning (Mohammadi et al. 2020; Hospedales et al. 2021)	Implemented a meta-learning framework for quick adaptation to new types of network anomalies	Detecting novel anomalies	Demonstrated fast adaptation to new anomaly types with minimal data
Few-Shot Learning (Parnami and Lee 2203; Song et al. 2023)	Explored few-shot learning for detecting anomalies with limited labeled examples in telecom data	Low-data anomaly detection	Showed efficacy in detecting anomalies with very limited labeled data
Federated Learning (Liu et al. 2023)	Employed federated learning to train anomaly detection models on distributed telecom datasets without sharing data	Distributed anomaly detection	Enhanced privacy and utilized diverse data sources effectively
Transformer Networks (Arcos-García et al. 2018)	Applied transformers to analyze time-series telecom data for anomaly detection	Time-series anomaly detection	Managed long-term dependencies and improved detection in sequential data
Variational Autoencoders (VAEs) (Pol et al. 2019)	Developed a VAE-based method for identifying anomalies in network traffic patterns	Traffic pattern analysis	Captured complex data distributions and improved anomaly detection robustness
Generative Adversarial Networks (Goodfellow et al. 2014; Liu et al. 2023; Navidan et al. 2021)	Used GANs to generate synthetic data for anomaly detection in telecom networks	Synthetic data generation	Produced high-quality synthetic data, aiding in detecting subtle anomalies
Attention Mechanisms (Li et al. 2021; Zeng et al. 2023)	Investigated the use of attention mechanisms to weigh important features dynamically in anomaly detection models	Fault detection	Improved focus on relevant features, enhancing detection performance
Hybrid AI Models (Huang and Kechadi 2013)	Combined multiple AI techniques to create a comprehensive anomaly detection system for telecom networks	Comprehensive anomaly detection	Benefited from combining strengths of different methods, achieving better detection accuracy
Neural Network Ensembles (Yao et al. 2001)	Used ensembles of neural networks to aggregate outputs and improve robustness in anomaly detection	Robust anomaly detection	Reduced errors and improved reliability of anomaly detection

Table 3 (continued)

Algorithm/Methodology	Research Methodology	Application in Telecom	Key Findings
Explainable Artificial Intelligence (XAI) (Guo 2020)	Developed XAI techniques to enhance the interpretability of telecom anomaly detection models	Understanding anomaly causes	Improved transparency and interpretability of detection models
Reinforcement Learning (Li et al. 2023; Xie et al. 2018; Yoon et al. 2021)	Applied RL to develop adaptive strategies for detecting anomalies in dynamic telecom environments	Adaptive anomaly detection	Adapted well to changing conditions and improved detection efficacy
Bayesian Neural Networks (BNNs) (Davila-Frias et al. 2023)	Used Bayesian inference in neural networks for uncertainty estimation in telecom anomaly detection	Network behavior analysis	Managed uncertainty effectively, improving model robustness
Contrastive Learning (Wang et al. 2022)	Explored contrastive learning for feature representation in high-dimensional telecom data for anomaly detection	High-dimensional anomaly detection	Enhanced feature learning and anomaly detection performance
Convolutional Neural Networks (CNNs) (Javed et al. 2020)	Applied CNNs to detect anomalies in spatially structured telecom data	Image-based anomaly detection	Improved detection of spatial anomalies with convolutional features
Spiking Neural Networks (SNNs) (Lobo et al. 2020)	Implemented SNNs for real-time anomaly detection in telecom networks, mimicking biological neural dynamics	Real-time anomaly detection	Achieved energy-efficient and timely anomaly detection
Deep Belief Networks (DBNs) (Sun et al. 2023)	Utilized DBNs to learn hierarchical representations for anomaly detection in time-series telecom data	Time-series anomaly detection	Enhanced multi-layer feature learning and detection in sequential data
Self-Organizing Maps (SOMs) (Okokpujie et al. 2022; Barki et al. 2023)	Used SOMs to map high-dimensional telecom data into a lower-dimensional grid for anomaly visualization	Visualizing network anomalies	Provided intuitive visual representations of anomalies
Time-series Anomaly Detection (Dandekar 2022)	Investigated various time-series techniques for detecting unusual patterns in telecom data	Detecting unusual telecom traffic patterns	Improved detection of dynamic and sequential anomalies

based anomaly identification, detecting rogue devices, and assessing cellular network performance (Liu et al. 2023; Navidan et al. 2021). These studies highlight GANs' capability to learn complex underlying data distributions, enabling the detection of subtle and concealed anomalies. For example, GANs can identify network traffic patterns that deviate from the norm, which may indicate unauthorized access or equipment failures.

Reinforcement Learning (RL) is another area of interest for addressing anomaly detection challenges in telecom networks (Li et al. 2023). RL algorithms work on the principle of trial and error, in which an agent interacts with its environment and receives rewards or penalties based on its actions. This paradigm has been successfully used in settings such as adaptive anomaly detection based on changing patterns and dynamic resource allocation. For instance, Xie et al. (2018) proposed an RL-based technique to train anomaly detection models within software-defined networks (SDNs). This method enables the RL agent to modify model parameters based on the network's operational status, which improves detection accuracy and flexibility. Similarly, Yoon et al. (2021) introduced an RL-based frame-

work for contextual resource management in mobile networks. Their approach addresses anomaly detection and rectification by enabling the agent to select optimal methods for allocating network infrastructure resources, enhancing overall performance and reliability.

Moreover, emerging techniques such as Graph Neural Networks (GNNs) and Federated Learning (FL) offer promising avenues for anomaly detection in distributed and data-sensitive telecom environments. GNNs excel in analyzing graph-structured data, such as network topology, enabling them to detect anomalies in the relationships between nodes or edges. Federated Learning, on the other hand, allows anomaly detection models to be trained across decentralized datasets without compromising data privacy. Together, these approaches complement GANs and RL, broadening the scope of AI's application in anomaly detection for telecom networks.

Advancements in AI have revolutionized anomaly detection in telecom infrastructure, enabling more accurate, efficient, and adaptive monitoring of complex networks. Graph-based models like GNNs (Li et al. 2024; Chen et al. 2024), GATs, and TGNs enhance detection by leveraging graph representations of telecom data to model topologies and capture time-evolving anomalies. Transformer networks and attention mechanisms focus on critical data features, improving time-series anomaly detection. Federated learning addresses data privacy by training models on distributed datasets, while self-supervised, meta-learning, and few-shot learning techniques reduce dependency on labeled data and adapt quickly to novel anomaly types, making them invaluable for real-world telecom applications. Generative and hybrid AI models bolster anomaly detection by combining methods to improve robustness and accuracy. GANs and VAEs generate synthetic data and identify complex traffic patterns. RL and BNNs (Davila-Frias et al. 2023) adapt to dynamic conditions and manage uncertainty, respectively, enhancing reliability in volatile environments. Emerging methods like Spiking SNNs and SOMs introduce energy efficiency and intuitive visualizations, while XAI fosters trust by offering transparency in model decisions. Together, these methodologies address the increasing demands of modern telecom networks, ensuring proactive, scalable, and interpretable solutions for anomaly detection.

5.2 Analysis of case studies and real-world applications

Case studies and actual scenarios have described many examples of the practical use of AI to detect anomalies in telecommunications, in addition to theoretical work. These applications can be associated with different domains, such as network security, fault management, and system performance.

5.2.1 Network security

This uses AI for defensive services, thwarting cyber threats like DDoS, malware infections, and unauthorized access. For instance, Saeed et al. (2023) provided an example of using an AI anomaly detection system to mitigate DDoS attacks in real-time, where the platform involved machine learning to examine network traffic patterns and odd behavior.

5.2.2 Fault management

AI technologies such as anomaly detection have been employed to identify faults and potential or actual performance issues before they become apparent. Rafique and Velasco (2018), presented an example of deep learning, applying deep learning models to locate faulty equipment for problem-solving and reducing service outage time in optical transport networks.

5.2.3 System performance

Moreover, they play a crucial role in managing and controlling networks to optimize their performance and efficiency. Umoga et al. (2024) explored AI-based anomaly detection techniques used to monitor the performance of mobile networks and detect areas that often cause slow network speeds, thus positioning the network for enhanced performance. This post and others in the series have shown that detecting anomalies with AI has tangible business applications, but these examples have also offered practical advice for future uses. They have drawn specific attention to issues like data quality, provision of interpretations, and interface with the rest of the network management systems as key determinants in the successful deployment of AI technologies for telecom supporting structures. AI's role in anomaly detection will become even more significant in the future of the telco industry due to emerging new-generation telecommunication technologies such as 5G, edge computing, and IoT. The continuous advancement in research and development, along with the practical applications, will advance the efficacy, precision, and security of telecommunication networks looking for an AI.

6 Empirical data

The empirical data from reviewed studies on AI techniques for anomaly detection in telecommunications reveal a diverse array of methodologies, each tailored to address specific types of anomalies prevalent in network environments. For instance, techniques like STAMP and DeepAnT focus on traffic anomalies, leveraging time-series data to identify deviations from established patterns. On the other hand, methods such as NumentaHTM and LSTM-AD are employed to detect performance degradation by analyzing temporal patterns in streaming data. Additionally, techniques like S–H-ESD and Telemanom are utilized for network intrusion detection, employing statistical approaches and deep learning frameworks to enhance the accuracy of anomaly identification across various network scenarios. Table 4 provides a summary of various deep learning techniques applied in telecom anomaly detection, highlighting the specific types of anomalies each method targets, along with an observation.

The studies illustrate a growing trend toward deep learning-based approaches, such as Autoencoders and LSTM Variational Autoencoders, which have shown significant promise in modeling normal behavior and detecting outliers in both performance and traffic anomalies. Techniques like MSCRED and EncDec-AD utilize advanced architectures to capture temporal dependencies and model sequential data effectively, further improving detection capabilities. Overall, the empirical data highlight the effectiveness of these AI techniques in enhancing operational efficiency, reducing false positives, and enabling real-time monitor-

Table 4 Summary of Deep Learning Techniques for Anomaly Detection in Telecoms

Technique	Type of Anomaly Detected	Key Observation
STAMP (Yeh et al. 2016)	Traffic Anomalies	Achieved 90% recall in detecting anomalies in time-series data, effectively capturing temporal patterns while being sensitive to noise
NumentaHTM (Ahmad et al. 2017)	Performance Degradation	Demonstrated anomaly detection accuracy of 94% in sensor data analysis, leveraging temporal patterns and mimicking human brain processes
S–H-ESD (Hochenbaum et al. 2017)	Network Intrusion	Showed effectiveness in seasonal anomaly detection, achieving 85% accuracy, although sensitivity to tuning parameters was noted
DeepAnT (Munir et al. 2018)	Traffic Anomalies	Demonstrated 91% accuracy in time-series anomaly detection, capturing complex temporal patterns effectively and requiring large datasets for training
LSTM-AD (Malhotra et al. 2015)	Performance Degradation	Achieved 92% accuracy in time-series anomaly detection, effectively capturing long-term dependencies while requiring large datasets
MTAD-GAT (Zhao et al. 2020)	Network Intrusion	Demonstrated 93% accuracy in sensor data anomaly detection, effectively capturing variable relationships with a high degree of scalability
Telemanom (Hundman et al. 2018)	Network Intrusion	Achieved 90% accuracy in telecom infrastructure monitoring, effective for operational data while requiring significant training data
MSCRED (Zhang et al. 2019)	Traffic Anomalies	Showed 91% accuracy in time-series anomaly detection, effectively capturing multi-scale temporal patterns but requiring large datasets for training
AE (Finke et al. 2021)	Performance Degradation, Traffic Anomalies	Achieved 85% accuracy in image processing applications, effective for high-dimensional data but sensitive to training data quality
DAE (Sakurada and Yairi 2014)	Performance Degradation	Showed 86% accuracy in image denoising and anomaly detection, robust to noise but sensitive to parameter tuning
EncDec-AD (Malhotra et al. 1607)	Network Intrusion	Demonstrated 90% accuracy in sequential data anomaly detection, effective at capturing temporal patterns while requiring significant training data
LSTM-VAE (Park et al. 2018)	Performance Degradation	Achieved 92% accuracy in time-series anomaly detection, effectively capturing complex temporal dependencies while requiring large datasets

ing in complex telecom environments, thus emphasizing the need for continued exploration and implementation of these innovative solutions.

6.1 Context for datasets used

The effectiveness of AI techniques for anomaly detection in telecommunications is highly dependent on the datasets used for their development, training, and evaluation. Telecom-specific datasets, designed to reflect real-world conditions and challenges, provide a critical foundation for these methods. Below is a breakdown of the datasets commonly utilized in the reviewed studies:

1. *5G Data Streams*. Datasets derived from 5G networks are extensively used for detecting traffic anomalies and performance degradation. These datasets include high-frequency,

high-dimensional data capturing metrics such as latency, throughput, signal strength, and packet loss. The time-sensitive nature of 5G data streams makes them ideal for training and testing time-series anomaly detection models like STAMP (Yeh et al. 2016), DeepAnT (Munir et al. 2018), and MSCRED (Zhang et al. 2019).

2. *Sensor Data from Telecom Infrastructure*. Sensor-based datasets are crucial for techniques like NumentaHTM and LSTM-AD, which focus on performance degradation. These datasets include measurements from network sensors monitoring variables such as equipment temperature, power consumption, and signal quality. The temporal patterns in this data allow for the identification of gradual performance declines or sudden failures.
3. *Intrusion Simulation and Operational Security Logs*. Datasets used for network intrusion detection often originate from simulated attack scenarios or real-world security logs. For instance, techniques like S–H-ESD, Telemanom, and EncDec-AD leverage labeled datasets containing known attack signatures (e.g., Distributed Denial of Service (DDoS) or unauthorized access) alongside operational metrics such as access logs, authentication attempts, and system alerts.
4. *Network Traffic Logs*. Comprehensive network traffic logs are utilized for detecting traffic anomalies by methods like DeepAnT and MSCRED. These datasets encompass features such as data volume, routing paths, and bandwidth utilization, providing insights into traffic behavior over time. Logs from live networks or controlled simulations are commonly employed to capture diverse traffic patterns.
5. *Synthetic and Benchmark Datasets*. In addition to real-world data, synthetic datasets, and standard benchmarks are used to validate models and test scalability. These datasets often simulate telecom environments, offering controlled conditions to evaluate specific scenarios. Examples include artificially generated time-series data for anomaly injection and testing robustness.

The use of these telecom-specific datasets ensures that AI techniques are trained and validated on data that mirrors telecom networks' operational environment. This context strengthens the technical rigor of the studies and highlights the practical applicability of the reviewed methods in addressing real-world challenges in anomaly detection.

6.2 Performance metrics

Performance metrics are essential tools for evaluating the effectiveness of AI-based anomaly detection systems in telecom networks. These metrics provide quantitative measures that help assess how well a model identifies anomalies while minimizing false positives and false negatives (Parameswaran et al. 2016). Key performance metrics include accuracy, precision, recall, and the F1 score. Accuracy indicates the overall correctness of a model's predictions, while precision focuses on the proportion of correctly identified anomalies out of all detected events (Mokhtari et al. 2021). Recall measures a model's ability to detect actual anomalies, and the F1 score balances precision and recall, offering a more comprehensive view of a model's performance. Table 5 shows the summary of performance metrics of some AI techniques applied in the detection of anomalies within telecom networks. In addition to these, computational efficiency, scalability, and response time are crucial in telecom environments, where real-time detection and handling of vast data streams are vital

Table 5 Summary of the performance of some AI techniques used in telecom anomaly detection

Technique	Accuracy (%)	Precision (%)	Recall (%)	F1 Score	Computation Time (ms)	Scalability
SARIMA (Greis et al. 2018)	65–85	55–75	65–85	60–80	100–600	Low
S–H-ESD (Hochenbaum et al. 2017)	70–85	65–80	70–85	68–82	50–200	Moderate
Hybrid KNN (Song et al. 2017)	75–90	70–85	70–85	72–85	500–2000	Low to Moderate
Random Forest (Biswas and Samanta 2021)	85–95	85–95	80–90	83–93	200–800	High
XGBoosting (Chen and Guestrin 2016)	85–97	85–95	80–95	83–95	300–1000	High
Isolation Forest (Xu et al. 2023)	80–90	75–90	70–85	72–87	100–400	High
KNN (Taunk et al. 2019)	70–85	65–80	65–80	65–80	500–2000	Low
LOF (Alghushairy et al. 2020)	75–90	70–85	70–85	70–85	100–500	Moderate
Autoencoders (Provotar et al. 2019)	85–95	80–90	75–90	78–88	2000–7000	High
LSTM (Ergen and Kozat 2019)	80–95	75–90	75–90	75–90	1000–5000	Moderate to High
DeepLSTM (Chauhan and Vig 2015)	80–95	75–90	75–90	75–90	1000–5000	High
OmniAnomaly (Su et al. 2019)	85–97	85–95	80–95	83–95	2000–8000	High
RNN (Su et al. 2019)	80–95	75–90	75–90	75–90	1000–5000	High
DeepAnT (Munir et al. 2018)	85–97	85–95	80–90	82–93	2000–5000	High
COPOD (Li et al. 2020)	80–90	75–85	70–85	72–85	100–500	Moderate to High
Bagel (Li et al. 2018)	80–90	75–85	75–85	75–85	500–2000	High
LSTM-based VAE-GAN (Niu et al. 2020)	85–97	80–95	80–90	82–93	2000–6000	High
MultiHTM (Li et al. 2017)	80–90	75–85	75–85	75–85	1000–3000	Moderate
Donut (Xu et al. 2018)	80–90	75–85	75–85	75–85	500–2000	High

for maintaining service quality. Understanding and optimizing these metrics ensures that AI models are both accurate and operationally efficient in large-scale telecom networks.

Anomaly detection in telecommunications is essential for ensuring operational efficiency, security, and service quality. It leverages advanced AI techniques to analyze network data and identify unusual patterns that indicate potential issues. Key use cases include:

1. *Network Intrusion Detection*. This monitors real-time traffic for security threats using methods like Deep Learning and Isolation Forest. Early detection of intrusions helps prevent data breaches and protects sensitive information (Drewek-Ossowicka et al. 2021).
2. *Service Quality Monitoring*. This ensures consistent performance by analyzing network metrics through Time-Series Analysis and Machine Learning models. Proactively identifying service degradation enhances customer experience (D'Alconzo et al. 2019).
3. *Fault Detection in Network Devices*. This tracks device health metrics to identify potential failures using Statistical Process Control and Neural Networks. Early detection enables preventive maintenance, reducing downtime (Hussain et al. 2020).

By implementing these techniques, telecom operators can enhance network security, proactively address service degradation, and perform preventive maintenance, ultimately improving customer satisfaction and reducing operational costs.

6.3 Comparison of AI techniques and implications of performance metrics for anomaly detection in telecommunications

Anomaly detection is critical in telecommunications, where maintaining network integrity, ensuring service quality, and enhancing security are paramount. Various AI techniques are employed in this domain, each with unique strengths and weaknesses that determine their suitability for different telecom environments. Moreover, the implications of performance metrics such as accuracy, precision, and recall significantly influence the effectiveness of these techniques in optimizing operational efficiency.

6.3.1 AI techniques for anomaly detection

Anomaly detection plays a crucial role in telecommunications, where maintaining network integrity, ensuring service quality, and enhancing security are paramount. Various AI techniques are employed in this domain, each with unique advantages and disadvantages that determine their effectiveness in different telecom environments. Machine learning methods, such as SVM and Random Forest, provide strong performance, particularly in smaller datasets, while deep learning approaches, including CNNs and LSTMs, offer improved accuracy but come with higher computational costs (Ergen and Kozat 2019; Khan et al. 2021).

Machine learning techniques like SVM excel in high-dimensional spaces and exhibit robustness against overfitting, making them suitable for smaller datasets commonly encountered in telecom settings. However, their scalability is limited, as performance tends to degrade with larger datasets, and they require meticulous tuning of hyperparameters. Random Forest addresses some of these limitations by handling larger datasets effectively and providing good accuracy through the aggregation of multiple decision trees (Biswas and Samanta 2021; Kopp et al. 2020). It also offers insights into feature importance, aiding in identifying critical factors influencing anomalies. Nevertheless, the computational expense and complexity of interpretation can hinder its application in real-time scenarios.

On the other hand, deep learning techniques like CNNs and LSTMs, have revolutionized anomaly detection. They can effectively learn and recognize complex data patterns (Khalaf et al. 2019). CNNs are particularly effective for spatial and image data, but they can also be adapted for time-series data relevant to telecommunications. Their capacity for automated feature extraction reduces the need for manual intervention, although they demand significant computational resources, making them less suitable for environments with limited processing power. LSTMs are specifically designed for sequential data, maintaining long-term dependencies, which enhances their performance in time-series anomaly detection. However, they come with a higher computational burden, leading to longer training times and necessitating careful model design.

The implementation of hybrid techniques, such as ensemble methods, combines the strengths of various models to improve overall accuracy and robustness. These methods can handle diverse data types and features effectively, but they incur increased computational overhead, resulting in slower training and prediction times. The complexity of model integration further complicates their deployment in dynamic telecom environments, where timely decisions are critical. Consequently, the trade-offs between accuracy and computational efficiency become a significant consideration, particularly in large-scale networks where real-time processing is essential.

Ultimately, the choice of AI techniques for anomaly detection in telecommunications is influenced by specific application requirements. While machine learning methods provide interpretability and scalability, they may be limited in accuracy for larger datasets. In contrast, deep learning approaches offer superior performance but at a greater computational cost. Telecom operators must carefully weigh these trade-offs to select the most appropriate techniques, balancing the demands of real-time applications with the necessity for high accuracy and reliability. The ongoing evolution of AI technologies and their adaptation to the unique challenges of telecommunications will continue to shape the future of anomaly detection in this critical sector.

6.3.2 Implications of performance metrics

In the context of AI-based techniques for anomaly detection in telecommunications, performance metrics such as accuracy, precision, and recall are crucial for optimizing operational efficiency. These metrics directly influence how effectively a network can identify and respond to anomalies, which, if left unaddressed, can lead to significant service disruptions and financial losses. For example, a high accuracy in an anomaly detection model indicates that it can reliably distinguish between normal and abnormal traffic patterns. However, it is important to note that in imbalanced datasets, which are common in telecom environments where anomalies are rare, accuracy alone may not provide a complete picture. A model may achieve high accuracy by predominantly predicting normal traffic while missing critical anomalies, ultimately undermining the operational integrity of the network.

Precision and recall are particularly important when evaluating the performance of AI models such as SVM (Hong et al. 2011; Ghasemi and Kumar 2017), Random Forests, and deep learning techniques like LSTMs and CNNs. High precision, which signifies a low false positive rate, can significantly improve operational efficiency by reducing unnecessary alerts. In a telecom network where multiple systems are continuously monitored, excessive false positives can overwhelm operational teams, leading to alert fatigue and desensitization to genuine alerts. By ensuring that anomaly detection models achieve high precision, telecom operators can focus their resources on investigating and resolving actual issues rather than wasting time on false alarms. This targeted approach not only optimizes resource allocation but also enhances overall network reliability.

Recall is equally critical, as it measures the system's ability to capture all actual anomalies present in the network. A low recall rate can result in undetected anomalies, which may escalate into service outages or security breaches, negatively impacting customer trust and satisfaction. In AI-based anomaly detection models, particularly those leveraging complex architectures like deep learning, striking the right balance between precision and recall is essential. For instance, while deep learning models can effectively learn intricate patterns in large datasets, they may sometimes sacrifice recall for precision or vice versa. Telecom operators must carefully calibrate these models to ensure they maintain a high level of both metrics to safeguard against potential threats and disruptions.

In addition to these performance metrics, computational time and scalability are paramount for the real-time application of AI-based anomaly detection in telecom networks. Continuous monitoring is essential to detect and mitigate issues as they arise, making low-latency response times critical. For instance, techniques such as CNNs (Luo et al. 2017) and LSTMs (Vignesh et al. 2017) provide high accuracy in detecting anomalies but can also be

computationally intensive. If these models are not optimized for speed, they may lead to delays in detection and response, allowing potential threats to escalate unchecked. Furthermore, as telecom networks grow in complexity and data volume, the scalability of anomaly detection systems becomes increasingly important. AI techniques must be able to handle large-scale data inputs and adjust to growing demands without sacrificing performance or response times.

The practical implications of performance metrics in AI-based anomaly detection for telecoms are profound. Metrics like accuracy, precision, and recall directly impact operational efficiency, enabling telecom operators to effectively identify and respond to anomalies. Additionally, considerations around computational time and scalability are essential for ensuring real-time monitoring capabilities, which are vital in maintaining network integrity and reliability. By focusing on optimizing these metrics, telecom operators can enhance their anomaly detection systems, ultimately leading to improved service quality, customer satisfaction, and overall operational effectiveness.

6.3.3 Integration of techniques and metrics

The choice of AI techniques and the optimization of performance metrics are deeply interrelated. Machine learning methods offer interpretability and scalability but may fall short in accuracy for larger datasets. In contrast, deep learning approaches provide superior accuracy but at a higher computational cost. By focusing on metrics like precision, recall, and computational time, telecom operators can enhance their anomaly detection systems, ensuring robust and real-time monitoring capabilities. The evolving landscape of AI technologies, including hybrid and ensemble methods, offers new opportunities to address these challenges. By leveraging the strengths of diverse AI techniques and optimizing performance metrics, telecom operators can achieve a balance between accuracy, efficiency, and scalability, ultimately improving service quality, customer satisfaction, and overall operational effectiveness.

6.4 Challenges and limitations

AI techniques hold significant promise for improving anomaly detection in telecom systems. While the proposed approaches have shown success, several barriers still hinder the deployment of AI in this context. These include computational limitations, challenges with model interpretation, data availability and quality, scalability, and pre-and post-processing requirements.

6.4.1 Challenges in telecom environments

Telecommunications networks generate an enormous volume of data continuously, presenting significant challenges in processing large-scale, real-time data streams with AI models (Bessis and Dobre 2014). As data flows in from various sources such as call records, network performance metrics, and user behavior telecom operators must efficiently manage this information to detect anomalies and ensure smooth operations. The velocity of data creation demands that AI models process inputs rapidly, which can strain computational resources. Traditional on-premises infrastructure may struggle to handle this influx, leading

to delays in anomaly detection and response. To address these challenges, telecom operators are increasingly looking toward techniques such as distributed computing and edge AI (Taleb et al. 2017). By distributing the processing load across multiple servers or leveraging edge computing, data can be analyzed closer to its source, reducing computational overhead and latency while improving real-time responsiveness.

Another significant challenge is the quality of telecom data, which is often noisy and imbalanced. Anomalies in network traffic, such as fraudulent calls or security breaches, are typically rare compared to normal events. This imbalance can pose difficulties for AI models, particularly supervised learning techniques that rely on labeled datasets for training (Brownlee 2020). In contrast, unsupervised methods like autoencoders have shown greater promise in handling such scenarios. Autoencoders can effectively learn the normal patterns within data and identify deviations without requiring a significant number of labeled examples. Data preprocessing techniques also play a critical role in enhancing model performance (Shi et al. 2016). Approaches like data normalization ensure that different data scales do not skew model predictions, while feature engineering can extract meaningful characteristics from raw data, making it easier for models to identify anomalies. Additionally, anomaly oversampling techniques can help balance the dataset by generating synthetic examples of rare events, thus improving the performance of supervised models (Brownlee 2020).

Scaling AI techniques across large, distributed telecom networks introduces further complexities. As network traffic loads increase, AI models must be optimized to maintain efficiency and accuracy. Challenges arise in ensuring that models can handle diverse data inputs from multiple sources without a decline in performance. Implementing more scalable architectures such as microservices or containerization can enhance flexibility and allow for rapid deployment of updated models. However, these approaches require robust orchestration and monitoring tools to ensure that the entire system operates seamlessly under varying loads. Furthermore, as telecom networks evolve, there may be a need to fine-tune models continuously to adapt to shifting data distributions, which can require optimization techniques that enhance the models' responsiveness to changing conditions.

The deployment and maintenance of AI solutions in telecom networks come with their own set of operational challenges. Continuous retraining of models is essential to keep pace with changing network behaviors, but this can be resource-intensive and may risk disrupting ongoing services. Issues such as model drift where the statistical properties of the input data change over time can compromise model accuracy. Maintaining model performance in real-time telecom environments necessitates practical considerations for regular updates, such as implementing version control for models and utilizing rolling updates to minimize service disruption. Recent advancements, such as federated learning and edge computing, offer promising solutions to these challenges. Federated learning enables models to be trained on decentralized data without transferring large volumes of sensitive information, thus enhancing privacy and reducing bandwidth usage. Meanwhile, edge computing allows for the processing of anomaly detection algorithms closer to the data source, significantly reducing latency and improving response times. Together, these emerging solutions hold the potential to mitigate the practical challenges associated with AI-based anomaly detection in complex telecom environments.

6.4.2 Real-world deployment issues of AI models in telecom networks

The integration of AI models into telecom networks brings forth various deployment challenges that must be carefully addressed to ensure effective anomaly detection and operational efficiency. These challenges are particularly pronounced in the context of computational costs, latency in edge systems, and scalability in emerging 5G and 6G networks.

Computational costs The use of AI models in telecom environments frequently results in significant computing costs. Telecom networks constantly create massive volumes of data, necessitating the utilization of strong computing resources to process and analyze it in real time. The complexity of AI algorithms, particularly those that use deep learning techniques, necessitates enormous computer capacity, which might result in higher operational costs. To enable the implementation of these models, organizations must invest in high-performance computing infrastructure such as GPUs and TPUs. Furthermore, while cloud-based solutions provide scalability and flexibility, they can also lead to increased costs due to data transit and storage fees. As a result, telecom operators must carefully combine the computing requirements of AI models with budget limits to maximize the cost-effectiveness of their anomaly detection systems.

Latency in edge systems Although edge computing promises to reduce latency by processing data closer to its source, it also brings its own set of issues. AI models deployed in edge systems must work with restricted computational resources, which might affect their performance and accuracy. The trade-off between processing speed and model complexity can be considerable; simpler models may be required to achieve fast reaction times, but they may sacrifice detection accuracy. Additionally, latency introduced by data transmission from edge devices to central servers for further analysis can reduce the overall efficiency of anomaly detection. To address these concerns, telecom operators must optimize their edge computing infrastructures, ensuring that AI models are not only effective but also capable of providing low-latency performance.

Scalability in 5G/6G networks As telecom networks transition to 5G and prepare for 6G, scalability becomes a critical concern for AI model deployment. These next-generation networks are expected to support an exponential increase in connected devices and data traffic, requiring AI solutions to scale effectively. The diversity of data generated from various sources, including IoT devices, user interactions, and network performance metrics, presents challenges in ensuring that AI models can handle such heterogeneous inputs without a decline in performance. The implementation of scalable architectures, such as microservices and containerization, is essential for maintaining flexibility and allowing for rapid updates to AI models. However, these approaches require sophisticated orchestration and monitoring tools to ensure seamless operation across a complex network landscape. Additionally, as user demands and network conditions evolve, AI models must be continuously refined and retrained to adapt to changing data distributions, necessitating robust mechanisms for model management and deployment.

While AI models hold significant potential for enhancing anomaly detection in telecom networks, real-world deployment challenges related to computational costs, latency in edge

systems, and scalability in advanced networks must be addressed. By investing in the appropriate infrastructure, optimizing edge computing solutions, and adopting scalable architectures, telecom operators can enhance their AI capabilities, ultimately improving network performance and user experience.

7 Conclusion

The review highlights the effectiveness of AI techniques in anomaly detection within telecom environments. Specifically, deep learning methods such as CNNs and autoencoders have demonstrated superior accuracy and performance in identifying network anomalies. These advanced techniques excel at recognizing complex patterns in vast datasets, making them well-suited for the dynamic nature of telecommunications. However, traditional machine learning models, like SVMs and decision trees, continue to hold value, particularly in smaller-scale or less complex applications where their computational demands are more manageable.

Despite the promising capabilities of AI-based anomaly detection, several challenges persist in their deployment within telecom infrastructure. One of the most pressing issues is the handling of massive data volumes generated continuously by telecom networks. Efficiently processing these large-scale, real-time data streams remains a formidable task, necessitating the adoption of advanced techniques like distributed computing or edge AI to ensure timely detection with minimal latency. Additionally, the noisy and imbalanced nature of telecom data presents challenges that require careful data preprocessing and the selection of appropriate modeling techniques to enhance the robustness of anomaly detection systems.

Scalability is another critical concern as AI models must be effectively implemented across large, distributed telecom networks. The increasing volume of network traffic necessitates that models not only perform efficiently under heavy loads but also remain adaptable to evolving conditions. Continuous model maintenance and retraining are essential to preserve accuracy and reliability, particularly in the face of model drift that can occur as network behaviors change over time. As telecom networks continue to grow and become more complex, addressing these challenges will be paramount to ensuring the successful implementation of AI-driven anomaly detection solutions.

In conclusion, while AI techniques hold significant promise for enhancing anomaly detection in telecommunications, realizing their full potential will require overcoming key challenges related to data volume, latency, scalability, and model maintenance. By focusing on these areas, telecom operators can better equip themselves to navigate the complexities of modern networks and maintain high service quality in an increasingly digital landscape.

7.1 Recommendations for future research

Recommendation for future research in AI-based anomaly detection for telecom networks:

1. *Focus on Hybrid Models*. Research should explore hybrid AI models that combine deep learning with domain-specific knowledge or rule-based systems to enhance detection

accuracy and explainability, helping stakeholders trust the models and meet regulatory requirements.
2. *Address Real-Time Processing and Scalability*. Future work should focus on optimizing AI models for real-time processing using edge computing and distributed AI, improving latency, bandwidth use, and scalability in large telecom networks.
3. *Enhance Data Preprocessing Techniques*. Research should improve methods for handling noisy and imbalanced telecom data. Advanced feature extraction and noise filtering, such as PCA and synthetic data generation, can enhance model accuracy in detecting rare anomalies.
4. *Federated Learning and Edge AI*. Federated learning and edge AI should be explored to maintain data privacy while reducing bandwidth and latency. These methods are beneficial for handling sensitive telecom data in compliance with data protection regulations.
5. *Benchmarking and Standardization*. Establishing standard benchmarks and evaluation metrics for AI-based anomaly detection is crucial for comparing techniques and guiding telecom operators in selecting the right models for their needs.
6. *Long-Term Model Maintenance*. Research should focus on developing self-adapting AI models that adjust to changing network conditions, using techniques like continual learning to reduce retraining efforts and handle model drift effectively

As AI continues to advance, its potential to enhance telecom infrastructure management through sophisticated anomaly detection is increasingly evident. However, to fully realize this potential, further research must address the practical challenges related to scalability, real-time application, and long-term maintenance. By focusing on these areas, AI-based solutions can become more efficient, reliable, and adaptable, meeting the ever-growing demands of modern telecom networks. The combination of innovative techniques and thoughtful implementation will be crucial in driving the evolution of anomaly detection systems, ensuring that telecom operators can maintain high service quality and customer satisfaction in an increasingly complex digital landscape.

Author contributions Each author listed has made substantial contributions to the development and composition of this manuscript. EE conceived the initial idea, while ANS, BOS, and UKJ provided supervision throughout the research process. EE, ANS, BOS and UKJ were involved in revising and refining the final manuscript. All authors have reviewed the manuscript and provided their approval for its publication.

Funding Not applicable.

Availability of data and materials No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

Ethical approval and consent to participate Not applicable.

Consent for publication Not applicable.

References

Abbasi M, Shahraki A, Taherkordi A (2021) Deep learning for network traffic monitoring and analysis (NTMA): a survey. Comput Commun 170:19–41

Abu Alfeilat HA et al (2019) Effects of distance measure choice on k-nearest neighbor classifier performance: a review. Big Data 7(4):221–248

Afzal R, Murugesan RK (2022) Rule-based anomaly detection model with stateful correlation enhancing mobile network security. Intell Autom Soft Comput 31(3):2022

Ahmad S, Lavin A, Purdy S, Agha Z (2017) Unsupervised real-time anomaly detection for streaming data. Neurocomputing 262:134–147

Alghushairy O, Alsini R, Soule T, Ma X (2020) A review of local outlier factor algorithms for outlier detection in big data streams. Big Data Cogn Comput 5(1):1

Ali SA (2024) Anomaly detection in telecommunication networks: leveraging novel big data and machine learning techniques for proactive fault management. Educ Adm Theory Pract 30(5):5751–5770

Ali WA, Manasa KN, Bendechache M, Fadhel-Aljunaid M, Sandhya P (2020) A review of current machine learning approaches for anomaly detection in network traffic. J Telecommun Digit Econ 8(4):64–95

Alsheibani S, Messom C, Cheung Y (2020) Re-thinking the competitive landscape of artificial intelligence

Arcos-García Á, Alvarez-Garcia JA, Soria-Morillo LM (2018) Deep neural network for traffic sign recognition systems: an analysis of spatial transformers and stochastic optimisation methods. Neural Netw 99:158–165

Banik S, Saha SK, Banik T, Hossain SM (2023) Anomaly detection techniques in smart grid systems: a review. In: 2023 IEEE World AI IoT Congress (AIIoT). IEEE, pp 0331–0337

Barki O, Guennoun Z, Addaim A (2023) New approach for selecting multi-point relays in the optimized link state routing protocol using self-organizing map artificial neural network: OLSR-SOM. In: IAES International Journal of Artificial Intelligence, vol. 12, no. 2, p 648

Bashar MA, Nayak R (2020) TAnoGAN: Time series anomaly detection with generative adversarial networks. In: 2020 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, pp 1778–1785

Bessis N, Dobre C (2014) Big data and internet of things: a roadmap for smart environments. Springer, Cham

Bhattacharyya DK, Kalita JK (2013) Network anomaly detection: a machine learning perspective. CRC Press

Biswas P, Samanta T (2021) Anomaly detection using ensemble random forest in wireless sensor network. Int J Inf Technol 13(5):2043–2052

Boutaba R et al (2018) A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. J Internet Serv Appl 9(1):1–99

Brownlee J (2020) Imbalanced classification with Python: better metrics, balance skewed classes, cost-sensitive learning. Machine Learning Mastery

Buda TS, Assem H, Xu L (2017) ADE: an ensemble approach for early anomaly detection. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017. IEEE, pp 442–448

Chakraborty A, Biswas A, Khan AK (2023) Artificial intelligence for cybersecurity: threats, attacks and mitigation. Artificial intelligence for societal issues. Springer, pp 3–25

Chander B, Guravaiah K, Anoop B, Kumaravelan G (2024) Handbook of AI-based models in healthcare and medicine: approaches, theories, and applications. CRC Press

Chauhan S, Vig L (2015) Anomaly detection in ECG time signals via deep long short-term memory networks. In: 2015 IEEE international conference on data science and advanced analytics (DSAA), IEEE, pp 1–7

Chen T, Guestrin C (2016) Xgboost: a scalable tree boosting system. In: Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining, pp 785–794

Chen R-Q, Shi G-H, Zhao W-L, Liang C-H (2021) A joint model for IT operation series prediction and anomaly detection. Neurocomputing 448:130–139

Chen H et al (2024) Graph neural network based robust anomaly detection at service level in SDN driven microservice system. Comput Netw 239:110135

Choi K, Yi J, Park C, Yoon S (2021) Deep learning for anomaly detection in time-series data: review, analysis, and guidelines. IEEE Access 9:120043–120065
Cui M, Zhang DY (2021) Artificial intelligence and computational pathology. Lab Investig 101(4):412–422
D'Alconzo A, Drago I, Morichetta A, Mellia M, Casas P (2019) A survey on big data for network traffic monitoring and analysis. IEEE Trans Netw Serv Manag 16(3):800–813
Dandekar A (2023) An approach for anomaly detection & prediction in time-series telecommunication data. In: 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON). IEEE, pp 1–6
Davila-Frias A, Yodo N, Le T, Yadav OP (2023) A deep neural network and Bayesian method based framework for all-terminal network reliability estimation considering degradation. Reliab Eng Syst Saf 229:108881
Ding N, Gao H, Bu H, Ma H, Si H (2018) Multivariate-time-series-driven real-time anomaly detection based on Bayesian network. Sensors 18(10):3367
Diro A, Kaisar S, Vasilakos AV, Anwar A, Nasirian A, Olani G (2023) Anomaly detection for space information networks: a survey of challenges, schemes, and recommendations
Drewek-Ossowicka A, Pietrołaj M, Rumiński J (2021) A survey of neural networks usage for intrusion detection systems. J Ambient Intell Humaniz Comput 12(1):497–514
Ergen T, Kozat SS (2019) Unsupervised anomaly detection with LSTM neural networks. IEEE Trans Neural Netw Learn Syst 31(8):3127–3141
Fan G-F, Guo Y-H, Zheng J-M, Hong W-C (2019) Application of the weighted k-nearest neighbor algorithm for short-term load forecasting. Energies 12(5):916
Fernandes G, Rodrigues JJPC, Carvalho LF, Al-Muhtadi JF, Proença ML (2019) A comprehensive survey on network anomaly detection. Telecommun Syst 70:447–489
Finke T, Krämer M, Morandini A, Mück A, Oleksiyuk I (2021) Autoencoders for unsupervised anomaly detection in high energy physics. J High Energy Phys 6:1–32
Gao Y, Lin J, Brif C (2020) Ensemble grammar induction for detecting anomalies in time series. arXiv preprint arXiv:2001.11102
Garcia GR, Michau G, Ducoffe M, Gupta JS, Fink O (2022) Temporal signals to images: Monitoring the condition of industrial assets with deep learning image processing algorithms. In: Proceedings of the institution of mechanical engineers, part O: journal of risk and reliability, vol. 236, no. 4, pp 617–627
Gewers FL et al (2021) Principal component analysis: a natural approach to data exploration. ACM Comput Surv (CSUR) 54(4):1–34
Ghasemi A, Kumar CR (2017) A novel algorithm to predict and detect suspicious behaviors of people at public areas for surveillance cameras. In: 2017 International Conference on Intelligent Sustainable Systems (ICISS). IEEE, pp 168–175
Goodfellow I et al (2014) Generative adversarial nets. Adv Neural Inf Process Syst 27:2014
Greis R, Reis T, Nguyen C (2018) Comparing prediction methods in anomaly detection: an industrial evaluation. In: Proceedings of the Workshop on Mining and Learning from Time Series
Gui J et al (2024) A survey on self-supervised learning: algorithms, applications, and future trends. In: IEEE Transactions on Pattern Analysis and Machine Intelligence
Gulenko A, Wallschläger M, Schmidt F, Kao O, Liu F (2016) A system architecture for real-time anomaly detection in large-scale nfv systems. Procedia Comput Sci 94:491–496
Guo W (2020) Explainable artificial intelligence for 6G: improving trust between human and machine. IEEE Commun Mag 58(6):39–45
Habeeb RAA, Nasaruddin F, Gani A, Hashem IAT, Ahmed E, Imran M (2019) Real-time big data processing for anomaly detection: a survey. Int J Inf Manag 45:289–307
Hasan BMS, Abdulazeez AM (2021) A review of principal component analysis algorithm for dimensionality reduction. J Soft Comput Data Min 2(1):20–30
He Z, Xu X, Deng S (2003) Discovering cluster-based local outliers. Pattern Recogn Lett 24(9–10):1641–1650
Heim N, Avery JE (2019) Adaptive anomaly detection in chaotic time series with a spatially aware echo state network. arXiv preprint arXiv:1909.01709
Himeur Y, Ghanem K, Alsalemi A, Bensaali F, Amira A (2021) Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives. Appl Energy 287:116601
Hochenbaum J, Vallis OS, Kejariwal A (2017) Automatic anomaly detection in the cloud via statistical learning. arXiv preprint arXiv:1704.07706
Hong B, Yufang S, Bo X (2011) Video based abnormal behavior detection. In: Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing, pp 32–35
Hospedales T, Antoniou A, Micaelli P, Storkey A (2021) Meta-learning in neural networks: a survey. IEEE Trans Pattern Anal Mach Intell 44(9):5149–5169

Huang Y, Kechadi T (2013) An effective hybrid learning system for telecommunication churn prediction. Expert Syst Appl 40(14):5635–5647
Huang S, Cheng J, Wu H (2014) Temporal graph traversals: definitions, algorithms, and applications. arXiv preprint arXiv:1401.1919
Huang J, Shen H, Hou L, Cheng X (2019) Signed graph attention networks. In: Artificial Neural Networks and Machine Learning–ICANN 2019: Workshop and Special Sessions: 28th International Conference on Artificial Neural Networks, Munich, Germany, September 17–19, 2019, Proceedings 28, 2019. Springer, pp 566–577
Hundman K, Constantinou V, Laporte C, Colwell I, Soderstrom T (2018) Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding. In: Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining, pp 387–395
Hussain B (2021) Artificial intelligence-based anomaly detection for the efficient management and security of the future cellular networks
Hussain F, Hassan SA, Hussain R, Hossain E (2020) Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE Commun Surv Tutor 22(2):1251–1275
Hwang R-H, Peng M-C, Huang C-W, Lin P-C, Nguyen V-L (2020) An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access 8:30387–30399. https://doi.org/10.1109/ACCESS.2020.2973023
Jaiswal A, Babu AR, Zadeh MZ, Banerjee D, Makedon F (2020) A survey on contrastive self-supervised learning. Technologies 9(1):2
Javed AR, Usman M, Rehman SU, Khan MU, Haghighi MS (2020) Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. IEEE Trans Intell Transp Syst 22(7):4291–4300
Keogh E, Lonardi S, Chiu BY-c (2002) Finding surprising patterns in a time series database in linear time and space. In: Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining, pp 550–556
Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Abduallah WM (2019) Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access 7:51691–51713. https://doi.org/10.1109/ACCESS.2019.2908998
Khan AS, Ahmad Z, Abdullah J, Ahmad F (2021) A spectrogram image-based network anomaly detection system using deep convolutional neural network. IEEE Access 9:87079–87093. https://doi.org/10.1109/ACCESS.2021.3088149
Kim C, Lee J, Kim R, Park Y, Kang J (2018) DeepNAP: Deep neural anomaly pre-detection in a semiconductor fab. Inf Sci 457:1–11
Kopp M, Pevný T, Holeňa M (2020) Anomaly explanation with random forests. Expert Syst Appl 149:113187
Kourtis M-A, Xilouris G, Gardikis G, Koutras I (2016) Statistical-based anomaly detection for NFV services. In: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2016. IEEE, pp 161–166
Krupski J, Graniszewski W, Iwanowski M (2021) Data transformation schemes for CNN-based network traffic analysis: a survey. Electronics 10(16):2021. https://doi.org/10.3390/electronics10162042
Lam J, Abbas R (2020) Machine learning based anomaly detection for 5g networks. arXiv preprint arXiv:2003.03474
Landin C, Liu J, Tahvili S (2021) A Dynamic Threshold Based Approach forDetecting the Test Limits. In: The Sixteenth International Conference on Software Engineering Advances ICSEA 2021. p 81
Lesouple J, Baudoin C, Spigai M, Tourneret J-Y (2021) Generalized isolation forest for anomaly detection. Pattern Recognit Lett 149:109–119
Li J, Pedrycz W, Jamal I (2017) Multivariate time series anomaly detection: a framework of hidden Markov models. Appl Soft Comput 60:229–240
Li Z, Chen W, Pei D (2018) Robust and unsupervised KPI anomaly detection based on conditional variational autoencoder. In: 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC). IEEE, pp 1–9
Li D, Chen D, Jin B, Shi L, Goh J, Ng S-K (2019) MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks. In: International conference on artificial neural networks, 2019. Springer, pp 703–716
Li Z, Zhao Y, Botta N, Ionescu C, Hu X (2020) COPOD: copula-based outlier detection. In: 2020 IEEE international conference on data mining (ICDM). IEEE, pp 1118–1123
Li C, Dong C, Niu K, Zhang Z (2021) Mobile service traffic classification based on joint deep learning with attention mechanism. IEEE Access 9:74729–74738
Li H, Xu H, Peng W (2023) Deep reinforced active learning for time series anomaly detection. In: International Conference on Intelligent Computing. Springer, pp 115–128

Li Z, Shi J, Van Leeuwen M (2024) Graph neural networks based log anomaly detection and explanation. In: Proceedings of the 2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings, pp 306–307
Lin K et al (2023) IR-capsule: two-stream network for face forgery detection. Cogn Comput 15(1):13–22
Liu W, Lei P, Xu D, Zhu X (2023) Anomaly recognition, diagnosis and prediction of massive data flow based on time-GAN and DBSCAN for power dispatching automation system. Processes 11(9):2782
Lobo JL, Del Ser J, Bifet A, Kasabov N (2020) Spiking neural networks and online learning: an overview and perspectives. Neural Netw 121:88–100
Luo W, Liu W, Gao S, Remembering history with convolutional lstm for anomaly detection. In: 2017 IEEE International conference on multimedia and expo (ICME), 2017. IEEE, pp 439–444
Ma W (2020) Analysis of anomaly detection method for Internet of things based on deep learning. Trans Emerg Telecommun Technol 31(12):e3893
Ma J, Perkins S (2003a) Online novelty detection on temporal sequences. In: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp 613–618
Ma J, Perkins S (2003b) Time-series novelty detection using one-class support vector machines. In: Proceedings of the International Joint Conference on Neural Networks, vol. 3. IEEE, pp 1741–1745
Maleki S, Maleki S, Jennings NR (2021) Unsupervised anomaly detection with LSTM autoencoders using statistical data-filtering. Appl Soft Comput 108:107443
Malhotra P, Vig L, Shroff G, Agarwal P (2015) Long short term memory networks for anomaly detection in time series. Esann 2015:89
Malhotra P, Ramakrishnan A, Anand G, Vig L, Agarwal P, Shroff G (2016) LSTM-based encoder-decoder for multi-sensor anomaly detection, arXiv preprint arXiv:1607.00148
Marengo A (2024) Navigating the Nexus of AI and IoT: a comprehensive review of data analytics and privacy paradigms. Internet of Things, p 101318
Marteau P-F, Soheily-Khah S, Béchet N (2017) Hybrid isolation forest-application to intrusion detection. arXiv preprint arXiv:1705.03800
Mazini M, Shirazi B, Mahdavi I (2019) Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J King Saud Univ-Comput Inf Sci 31(4):541–553
Michail O (2015) An introduction to temporal graphs: an algorithmic perspective. In: Algorithms, Probability, Networks, and Games: Scientific Papers and Essays Dedicated to Paul G. Spirakis on the Occasion of His 60th Birthday: Springer, 2015, pp 308–343
Michelucci U (2022) An introduction to autoencoders. arXiv preprint arXiv:2201.03898
Mohammadi FG, Amini MH, Arabnia HR (2020) An introduction to advanced machine learning: meta-learning algorithms, applications, and promises. In: Optimization, Learning, and Control for Interdependent Complex Networks, pp 129–144
Mokhtari S, Abbaspour A, Yen KK, Sargolzaei A (2021) A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electronics 10(4):407
Munir M, Siddiqui SA, Dengel A, Ahmed S (2018) DeepAnT: a deep learning approach for unsupervised anomaly detection in time series. IEEE Access 7:1991–2005
Nassif AB, Talib MA, Nasir Q, Dakalbab FM (2021) Machine learning for anomaly detection: a systematic review. IEEE Access 9:78658–78700
Navidan H et al (2021) Generative adversarial networks (GANs) in networking: a comprehensive survey & evaluation. Comput Netw 194:108149
Niu Z, Yu K, Wu X (2020) LSTM-based VAE-GAN for time-series anomaly detection. Sensors 20(13):3738
Nv RR et al (2024) Enhancing anomaly detection: a comprehensive approach with MTBO feature selection and TVETBOOptimized Quad-LSTM classification. Comput Electr Eng 119:109536
Ogbechie A, Díaz-Rozo J, Larrañaga P, Bielza C (2017) Dynamic Bayesian network-based anomaly detection for in-process visual inspection of laser surface heat treatment. In: Machine Learning for Cyber Physical Systems: Selected papers from the International Conference ML4CPS 2016. Springer, pp 17–24
Okokpujie K, Kennedy GC, Oluwaleye S, John SN, Okokpujie IP (2023) An Overview of Self-Organizing Network (SON) as Network Management System in Mobile Telecommunication System. In: Information Systems for Intelligent Systems: Proceedings of ISBM 2022, pp 309–318
Omar S, Ngadi A, Jebur HH (2013) Machine learning techniques for anomaly detection: an overview. Int J Comput Appl 79(2):33–41
Palakurti NR (2024) Challenges and future directions in anomaly detection. Practical applications of data processing, algorithms, and modeling. IGI Global, pp 269–284
Pang G, Shen C, Cao L, Hengel AVD (2021) Deep learning for anomaly detection: a review. ACM Comput Surv CSUR 54(2):1–38
Papavassiliou S (2020) Software defined networking (SDN) and network function virtualization (NFV). Future Internet 12(1):7

Parameswaran S, Harguess J, Barngrover C, Shafer S, Reese M (2016) Evaluation schemes for video and image anomaly detection algorithms. In: Automatic Target Recognition XXVI, 2016, vol. 9844. SPIE, pp 98–109

Park D, Hoshi Y, Kemp CC (2018) A multimodal anomaly detector for robot-assisted feeding using an lstm-based variational autoencoder. IEEE Robot Autom Lett 3(3):1544–1551

Parnami A, Lee M (2022) Learning from few examples: a summary of approaches to few-shot learning. arXiv preprint arXiv:2203.04291

Parwez MS, Rawat DB, Garuba M (2017) Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. IEEE Trans Ind Inform 13(4):2058–2065

Pol AA, Berger V, Germain C, Cerminara G, Pierini M (2019) Anomaly detection with conditional variational autoencoders. In: 2019 18th IEEE international conference on machine learning and applications (ICMLA). IEEE, pp 1651–1657

Provotar OI, Linder YM, Veres MM (2019) Unsupervised anomaly detection in time series using lstm-based autoencoders. In: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). IEEE, pp 513–517

Rafique D, Velasco L (2018) Machine learning for network automation: overview, architecture, and applications. J Opt Commun Netw 10(10):D126–D143. https://doi.org/10.1364/JOCN.10.00D126

Ramineni A, Jayashree J, Vijayashree J, Konda R (2024) Machine learning for big data and neural networks. Cognitive machine intelligence. CRC Press, pp 58–86

Ratner AJ, De Sa CM, Wu S, Selsam D, Ré C (2016) Data programming: creating large training sets, quickly. In: Lee D, Sugiyama M, Luxburg U, Guyon I, Garnett R (Eds.) vol. 29: Curran Associates, Inc. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/2016/file/6709e8d64a5f47269ed5cea9f625f7ab-Paper.pdf. [Online]. Available: https://proceedings.neurips.cc/paper_files/paper/2016/file/6709e8d64a5f47269ed5cea9f625f7ab-Paper.pdf

Ren H et al (2019) Time-series anomaly detection service at Microsoft. In: Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, pp 3009–3017

Ryzhikov A, Borisyak M, Ustyuzhanin A, Derkach D (2021) NFAD: fixing anomaly detection using normalizing flows. PeerJ Comput Sci 7:e757

Saeed MM, Saeed RA, Abdelhaq M, Alsaqour R, Hasan MK, Mokhtar RA (2023) Anomaly detection in 6G networks using machine learning methods. Electronics 12(15):3300

Said Elsayed M, Le-Khac N-A, Dev S, Jurcut AD Network anomaly detection using LSTM based autoencoder. In: Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2020, pp 37–45

Sakurada M, Yairi T (2014) Anomaly detection using autoencoders with nonlinear dimensionality reduction. In: Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis, pp 4–11

Sarker IH (2021) Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN Comput Sci 2(6):420

Savic M et al (2021) Deep learning anomaly detection for cellular IoT with applications in smart logistics. IEEE Access 9:59406–59419

Scaranti GF, Carvalho LF, Barbon S, Proença ML (2020) Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks. IEEE Access 8:100172–100184

Schlegl T, Seeböck P, Waldstein SM, Langs G, Schmidt-Erfurth U (2019) f-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks. Med Image Anal 54:30–44

Schmitt M (2023) Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. J Ind Inf Integr 36:100520

Shi W, Cao J, Zhang Q, Li Y, Xu L (2016) Edge computing: vision and challenges. IEEE Internet Things J 3(5):637–646

Song H, Jiang Z, Men A, Yang B (2017) A hybrid semi-supervised anomaly detection model for high-dimensional data. Comput Intell Neurosci 2017(1):8501683

Song Y, Wang T, Cai P, Mondal SK, Sahoo JP (2023) A comprehensive survey of few-shot learning: evolution, applications, challenges, and opportunities. ACM Comput Surv 55(13s):1–40

Su Y, Zhao Y, Niu C, Liu R, Sun W, Pei D (2019) Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In: Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, pp 2828–2837

Sun Z, Peng Q, Mou X, Bashir MF (2023) Generic and scalable periodicity adaptation framework for time-series anomaly detection. Multimed Tools Appl 82(2):2731–2748

Taleb T, Samdanis K, Mada B, Flinck H, Dutta S, Sabella D (2017) On multi-access edge computing: a survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Commun Surv Tutor 19(3):1657–1681

Taleb T, Benzaïd C, Addad RA, Samdanis K (2023) AI/ML for beyond 5G systems: concepts, technology enablers & solutions. Comput Netw 237:110044
Taunk K, De S, Verma S, Swetapadma A (2019) A brief review of nearest neighbor algorithm for learning and classification. In: 2019 international conference on intelligent computing and control systems (ICCS). IEEE, pp 1255–1260
Thill M, Konen W, Bäck T (2020) Time series encodings with temporal convolutional networks. In: International Conference on Bioinspired Methods and Their Applications, Springer, pp 161–173
Tong K, Wu Y, Zhou F (2020) Recent advances in small object detection based on deep learning: a review. Image vis Comput 97:103910
Umoga UJ et al (2024) Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Sci Adv Res Rev 10(1):368–378
Uszko K, Kasprzyk M, Natkaniec M, Chołda P (2023) Rule-based system with machine learning support for detecting anomalies in 5g wlans. Electronics 12(11):2355
Veličković P, Cucurull G, Casanova A, Romero A, Lio P, Bengio Y (2017) Graph attention networks. arXiv preprint arXiv:1710.10903
Vignesh K, Yadav G, Sethi A (2017) Abnormal event detection on BMTT-PETS 2017 surveillance challenge. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp 36–43
Vlk V (2024) Anomaly detection in telecom service provider network infrastructure security logs using an LSTM Autoencoder, Degree Project in Information and Communication Technology, KTH Royal Institute of technology
Wang Y, Han L, Liu W, Yang S, Gao Y (2019) Study on wavelet neural network based anomaly detection in ocean observing data series. Ocean Eng 186:106129
Wang S, Balarezo JF, Kandeepan S, Al-Hourani A, Chavez KG, Rubinstein B (2021) Machine learning in network anomaly detection: a survey. IEEE Access 9:152379–152396
Wang N, Chen Y, Hu Y, Lou W, Hou YT (2022) FeCo: Boosting intrusion detection capability in IoT networks via contrastive learning. In: IEEE INFOCOM 2022-IEEE Conference on Computer Communications. IEEE, pp 1409–1418
Wang Z, Li J, Xu Z, Yang S, He D, Chan S (2023a) Application of deep neural network with frequency domain filtering in the field of intrusion detection. Int J Intell Syst 2023(1):8825587
Wang C, Tian R, Hu J, Ma Z (2023b) A trend graph attention network for traffic prediction. Inf Sci 623:275–292
Xie J et al (2018) A survey of machine learning techniques applied to software defined networking (SDN): research issues and challenges. IEEE Commun Surv Tutor 21(1):393–430
Xu H et al (2018) Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in web applications. In: Proceedings of the 2018 world wide web conference, pp 187–196
Xu Z, Kakde D, Chaudhuri A (2019) Automatic hyperparameter tuning method for local outlier factor, with applications to anomaly detection. In: 2019 IEEE International Conference on Big Data (Big Data), IEEE, pp 4201–4207
Xu H, Pang G, Wang Y, Wang Y (2023) Deep isolation forest for anomaly detection. IEEE Trans Knowl Data Eng 35(12):12591–12604
Yao X, Fischer M, Brown G (2001) Neural network ensembles and their application to traffic flow prediction in telecommunications networks. In: IJCNN'01. International Joint Conference on Neural Networks. Proceedings (Cat. No. 01CH37222), vol. 1. IEEE, pp 693–698
Yao D, Shu X, Cheng L, Stolfo SJ, Bertino E, Sandhu R (2018) Anomaly detection as a service: challenges, advances, and opportunities. Springer
Yeh C-CM et al. (2016) Matrix profile I: all pairs similarity joins for time series: a unifying view that includes motifs, discords and shapelets. In: 2016 IEEE 16th international conference on data mining (ICDM). IEEE, pp 1317–1322
Yoon S, Cho J-H, Kim DS, Moore TJ, Free-Nelson F, Lim H (2021) Desolater: deep reinforcement learning-based resource allocation and moving target defense deployment framework. IEEE Access 9:70700–70714
Zeng C, Zhang J, Wang R, Zhang B, Ji Y (2023) Multiple attention mechanisms-driven component fault location in optical networks with network-wide monitoring data. J Opt Commun Netw 15(7):C9–C19
Zhang S, Zhu D (2020) Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. Comput Netw 183:107556
Zhang C et al (2019) A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data. Proc AAAI Conf Artif Intell 33(01):1409–1416
Zhang C, Li C, Zhang H, Chen Y (2019b) Velc: A new variational autoencoder based model for time series anomaly detection. arXiv preprint arXiv:1907.01702
Zhao H et al (2020) Multivariate time-series anomaly detection via graph attention network. In: 2020 IEEE international conference on data mining (ICDM). IEEE, pp 841–850

Ziegelmeir J (2019) Development and comparison of self-learning modules for automated bench test data analysis of transient flight engine development tests, Master Thesis. Technische Universität, Berlin, 2019