International Journal of Artificial Intelligence,
ISSN 0974-0635; Int. J. Artif. Intell.
2026, Volume 24, Issue Number 2 [Published on 29/08/2026]

Investigation of the Effectiveness of Anomaly-Monitoring Methods for Network Intrusions in Ensuring the Information Security of Telecommunication Networks Using Autoencoders

A. Marchuk [1]

[1] V.V. Popovskyy Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics,
61166, 14 Nauky Ave., Kharkiv, UKRAINE
Email : artemmarchuk264@gmail.com

ABSTRACT

Ensuring the cybersecurity of telecommunication networks presupposes the detection of anomalies in traffic as a key element of protection systems. The purpose of the study was to assess the effectiveness of autoencoders for monitoring anomalies in network traffic and increasing the security level of telecommunication systems. The methodology was based on methods of comparative, systems and theoretical-analytical analysis to evaluate the effectiveness and optimise models of anomaly detection in telecommunication networks. It was established that telecommunication systems require adaptive traffic-analysis algorithms, since signature-based methods lose effectiveness in the face of new threats. Z-score and regression analysis are simple but do not take into account non-linearity and correlations between parameters. K-means and Density-Based Spatial Clustering of Applications with Noise are capable of identifying unknown patterns without data labelling, but these algorithms are sensitive to parameters and unstable with large data volumes. The Local Outlier Factor and Isolation Forest algorithms are effective for detecting rare events without prior training, but often generate too many false positives. It was found that autoencoders detect anomalies on the basis of reconstruction error, which makes it possible to identify unknown threats without the need for data labelling. Recurrent autoencoders take temporal dependencies into account, which makes it possible effectively to recognise long-term attacks such as Distributed Denial of Service or Botnet, but such models require significant computational resources. The classical accuracy indicator is insufficient; in Intrusion Detection System environments, Precision, Recall, F1-score, Receiver Operating Characteristic – Area Under the Curve and False Positive Rate are considered the main measures, as these metrics reflect the real effectiveness of attack detection. Combining autoencoders with clustering or statistical methods increases effectiveness, reduces false alerts and forms the basis of adaptive cyber defence. The practical value of the study lies in the possibility of using the results obtained to build high-performance systems for monitoring network traffic that are capable of timely detection of new and hidden cyberthreats.

Keywords: Data processing, machine learning, neural networks, hybrid models, cyberthreats, system scalability.
Mathematics Subject Classification: 68T07, 68M12, 94A62

1. INTRODUCTION

The increase in the number and complexity of cyberattacks represents a serious challenge for the stable functioning of telecommunication networks and information infrastructures. Traditional monitoring systems, which are based mainly on signature-based methods, prove effective only against already known threats and do not provide an adequate level of protection in the event of modified or new attack

scenarios. Methods of statistical analysis partially overcome this limitation; however, the effectiveness decreases significantly in conditions of complex multifactor intrusions. In modern conditions, one of the key problems of cyber defence is ensuring timely and accurate detection of hidden anomalies in real-time mode when processing large volumes of network traffic (Baigereyev et al., 2025; Ginters and Revathy, 2021). In this regard, the application of deep-learning methods, in particular autoencoders, which make it possible to identify atypical patterns without prior data labelling, is becoming increasingly relevant. At the same time, the use of such models is accompanied by a number of challenges related to the high resource intensity of the training process and the need for adaptation to specific operating conditions of telecommunication systems.

Analysis of scientific sources has shown that the problem of anomaly detection in network traffic has been actively studied both in international and in Ukrainian practice. Thus, in the work by Zhang and Fan (2024) it was shown that autoencoders achieved high accuracy in anomaly detection in large datasets. However, the authors noted that computational costs and the duration of the training process complicated the use in real time. In the study by Wang et al. (2024) combined approaches were proposed that integrated autoencoders with classification methods. The results demonstrated increased model accuracy, but the paper indicated that the effectiveness of these methods strongly depended on parameter settings and the characteristics of the input data. In the work by Li (2020) it was proved that hybrid architectures that combined autoencoders with other machine-learning algorithms increased the ability of systems to detect complex attacks, but model accuracy decreased under changing network-environment conditions. Additional results were presented in the study by Aziz et al. (2024), where the use of hybrid models in variable traffic was considered; it was found that these systems could adapt to new attacks, but the scalability in real networks with high load remained problematic. Sun et al. (2020) showed that autoencoders operate effectively even with incomplete or partially corrupted datasets, demonstrating high robustness to information loss. At the same time, the authors noted that without additional optimisation of the architecture and tuning of hyperparameters, model performance gradually decreased when processing large streams of network traffic, especially in real-time mode. In the work, Rahman et al. (2023) confirmed the high accuracy of autoencoders in monitoring network traffic, which made it possible effectively to detect atypical and previously unknown behaviour patterns. However, the researchers emphasised that without optimisation of computational processes and reduction of resource intensity, the implementation of such models in large-scale telecommunication systems remained limited, which reduced the practical applicability in real conditions. Lahasan and Samma (2022) proposed integration of autoencoders with generative adversarial neural networks, which made it possible to increase the accuracy and sensitivity of systems detecting hidden deviations in network traffic. The authors stressed that the proposed approach reduced the number of false positives and improved the quality of data reconstruction; however, model testing was mainly carried out on experimental datasets, and therefore the effectiveness of the method requires verification in real telecommunication-network conditions.

At the same time, Ukrainian researchers have also actively developed the area of anomaly detection in network traffic. Shulha et al. (2025) proposed a generalised model of a system for forecasting and detecting anomalies in cyber infrastructure that combined autoencoders and multilayer perceptrons.

The authors proved that the use of such a hybrid architecture increased the accuracy of classification of atypical events and provided faster adaptation to new types of attacks. In addition, the study showed the possibility of reducing system load through optimisation of model-training processes. Marchenko et al. (2024) demonstrated that deep-learning methods, in particular autoencoders, showed high effectiveness in Internet of Things environments, provided noise and resource constraints were taken into account. The researchers found that adapting training parameters to limited computational resources made it possible to maintain stable performance even under high traffic variability.

Separately, methods for analysing network traffic using the Local Outlier Factor (LOF) and Histogram-Based Outlier Score algorithms were developed, which provided high sensitivity to local anomalies in the data (Sabibolda et al., 2024; Tashtay et al., 2026). The results of such approaches indicated the ability of the algorithms to detect subtle deviations effectively, even in high-dimensional datasets typical of telecommunication networks. Petliak (2025) carried out a systematic analysis of existing anomaly-detection models and highlighted the existence of a trade-off between accuracy and computational costs. The author noted that increasing detection accuracy is accompanied by growth in architectural complexity and training time, which requires the search for an optimal balance between system effectiveness and performance. In a number of practical developments, autoencoders also demonstrated high accuracy and practical suitability for use by network administrators when monitoring traffic in real time (Brescia et al., 2024; 2025). Summarising the results of the studies conducted, it can be stated that autoencoders have shown significant potential in tasks of anomaly detection in network traffic, as the autoencoders are capable of working with unlabelled data and detecting new types of attacks.

However, existing works have revealed a number of unresolved problems: high computational complexity, the need to optimise architectures for specific conditions, limited scalability, and the lack of sufficient research on the effectiveness of hybrid approaches in real telecommunication networks. Issues related to model stability in real-time mode, which is crucial for cyber-defence systems, have also not been sufficiently examined.

The purpose of the study was to assess the effectiveness of applying autoencoders and hybrid models in anomaly-detection tasks in telecommunication networks, taking into account the requirements for accuracy, data-processing speed and resource optimisation. On the basis of the results obtained, the following objectives of the study were defined: to generalise modern approaches to anomaly detection in telecommunication networks and identify trends in the development; to analyse the effectiveness of statistical, clustering and neural-network methods, in particular autoencoders, in terms of accuracy, adaptability and computational complexity; and to determine key criteria for assessing model performance and outline directions for the improvement to increase the reliability of threat-detection systems.

2. MATERIALS AND METHODS

The study had a theoretical-analytical character, which made it possible to generalise the characteristics of classical, deep and hybrid models, compare the architectures, advantages and disadvantages, and

identify patterns in model performance under various operating conditions of telecommunication networks. A structured narrative-comparative research design was used. The research procedure comprised four consecutive stages: identification of relevant publications, screening for direct relevance to network anomaly detection, extraction of comparable methodological and performance characteristics, and qualitative synthesis of the evidence. Sources were considered relevant when they described the operating principles, evaluation metrics, implementation conditions, or practical limitations of anomaly-detection methods in telecommunication, Internet of Things, cloud, or related network environments.

By means of the comparative-analytical method, on the basis of data from sources, approaches to anomaly detection in telecommunication networks were generalised – statistical methods (Z-score, regression analysis), clustering methods (k-means, Density-Based Spatial Clustering of Applications with Noise (DBSCAN)), outlier-detection methods (LOF, Isolation Forest), autoencoders, LSTM autoencoders, hybrid models (autoencoder + clustering). The unit of analysis was an individual anomaly-detection method or model architecture described in the selected sources. The evaluation process was based on a structured comparison matrix that included data-labelling requirements, the ability to model non-linear and temporal dependencies, Precision, Recall, F1-score, ROC-AUC, False Positive Rate (FPR), processing speed, computational complexity, scalability, and reported limitations. The criteria were chosen to ensure a comprehensive and balanced understanding of the effectiveness of cyber-defence systems in telecommunication networks. Because the reviewed studies used different datasets, model architectures, classification thresholds, and experimental settings, their numerical results were not statistically pooled. Instead, the findings were synthesised qualitatively, and the verbal ratings presented in Table 2 were assigned according to the predominance and consistency of the results reported across the selected sources. Additionally, a comparative analysis of anomaly-detection methods according to the advantages and disadvantages – classical, autoencoder-based and hybrid – was carried out in order to determine which approaches provide the best accuracy and stability when analysing telecommunication traffic.

For the purpose of theoretical generalisation of approaches to optimising autoencoders for anomaly detection in telecommunication networks, the method of systems analysis and generalisation of scientific sources was used, which made it possible to identify the main directions of model development, taking into account architecture optimisation and reduction of computational complexity (Mienye & Swart, 2025), increased robustness of models to noise and distortions in telecommunication data (Duque et al., 2024; Choi et al., 2021), and the ability to adapt in real time (Hou et al., 2022; Lin, 2024). The extracted findings were grouped into three analytical domains: architectural and computational optimisation, robustness to noise and data distortions, and adaptability to changing traffic in real time. Conclusions were formulated when convergent tendencies were identified across several sources, whereas inconsistent findings were retained as methodological limitations. The task was to systematise scientific approaches to optimising autoencoders, determine the main trends in the development and outline promising directions for improving the effectiveness of adaptive anomaly-detection systems in telecommunication networks.

3. RESULTS

The increase in the number of attacks in telecommunication networks creates the need to revise traditional approaches to monitoring and analysing network traffic. Traditional signature-based methods provide satisfactory results only in cases of known attack patterns, but are ineffective when confronted with new or modified threats. Current trends in the development of telecommunication systems require algorithms that are capable of adapting to dynamic changes and learning patterns of normal behaviour without constant manual intervention. In this regard, comparison of the effectiveness of different approaches to anomaly detection has become an important component of research in the field of cybersecurity, as it makes it possible to identify the strengths and weaknesses of each method (Aly et al., 2020).

Classical anomaly-detection methods, despite the long history of use, have limitations caused by the increasing complexity of network-traffic structure. Statistical approaches such as the standard-deviation method Z-score and regression analysis are based on identifying deviations from the mean value and on the assumption of a normal distribution of the data. These models make it possible quickly to identify simple anomalies that differ from typical values, and therefore remain useful in environments with relatively stable behaviour. The main advantage is the simplicity of interpretation of results and low computational requirements, which makes it possible to implement such models even on basic equipment. However, in complex systems with numerous interrelated parameters such methods lose accuracy because correlations between features are not taken into account (Choi et al., 2021; Hashimov et al., 2019).

Moreover, regression models cannot effectively describe the non-linear processes inherent in real network traffic, which reduces the effectiveness in situations where the behaviour of users or devices changes over time. Problems of statistical methods are also related to the impossibility of efficient use in cases of high-dimensional data, where classical approaches require preliminary simplification or reduction of features to several indicators (Stamov et al., 2023). Such simplifications often lead to the loss of important information, which negatively affects detection accuracy. Therefore, statistical models are used mainly as auxiliary tools for rapid preliminary analysis or as part of hybrid systems, where such models provide a preliminary assessment of the network state before applying more complex algorithms (Garg et al., 2020; Kondratenko and Kondratenko, 2014, Sokoliuk et al., 2021).

Clustering methods are considered more flexible, among which the most widespread are k-means and DBSCAN. These methods do not require labelled data and make it possible to detect unknown patterns by grouping similar elements into clusters. This creates the possibility of identifying new types of attacks without prior knowledge of the characteristics (Aly et al., 2020). The basis of the effectiveness of clustering algorithms is the ability to determine similarity between objects according to specified metrics, which makes it possible automatically to separate potentially anomalous observations. However, such methods are highly sensitive to parameter choice, in particular the number of clusters or search radius. Even a slight change in these parameters may alter the analysis result, which limits the practical stability. An additional disadvantage of clustering algorithms is the complexity of the use in large networks with uneven traffic distribution. Under such conditions, algorithms like k-means often create clusters of irregular shape or merge heterogeneous data, leading to incorrect conclusions. DBSCAN is more robust to noise but requires complex parameter tuning and does not always operate correctly when traffic density varies (Carrara et al., 2021). Despite this, clustering methods remain useful as part of combined

detection systems, where these methods are used for preliminary processing and segmentation of data, thereby reducing the load on more complex models (Hou et al., 2022; Gospodinova, 2022).

Outlier-detection methods, in particular LOF and Isolation Forest, make it possible to operate without labelled samples and to detect rare or unknown deviations. These models identify anomalies by the level of "isolation" of individual observations, which makes it possible to find atypical events even without prior training of the model on examples. LOF analyses the local density of the point's neighbourhood and determines the degree of deviation from neighbouring objects, whereas Isolation Forest uses an ensemble of decision trees to isolate observations with uncharacteristic values. The main advantage of these methods is the universality and ability to work with different types of data. However, these methods often generate numerous false positives, which reduces the practical value in systems with high traffic intensity (Hou et al., 2022). Classical approaches remain effective only in cases where the traffic structure is stable and the number of variables is limited. In modern networks, where data are characterised by high dynamics and high dimensionality, these methods lose the ability to describe processes accurately. This determines the shift towards more complex machine-learning models that are capable of automatically forming an understanding of patterns without prior specification of analytical relationships (Bodi et al., 2021; Choi et al., 2021).

One of the most promising directions in this context has been autoencoders (Figure 1). The autoencoders operate on the principle of reconstructing the input data: the model compresses the information into a compact latent representation and then attempts to restore it. The difference between the original and reconstructed data is used as an anomaly indicator. If the reconstruction error exceeds a certain threshold, the system considers the observation to be a deviation. This approach is effective because it does not require prior labelling and makes it possible to detect new threats that have not yet existed in signature databases (Ball et al., 2023; Kadenko et al., 2024).

```
latent_dim = 64

class Autoencoder(Model):
  def __init__(self, latent_dim):
    super(Autoencoder, self).__init__()
    self.latent_dim = latent_dim
    self.encoder = tf.keras.Sequential([
      layers.Flatten(),
      layers.Dense(latent_dim, activation='relu'),
    ])
    self.decoder = tf.keras.Sequential([
      layers.Dense(784, activation='sigmoid'),
      layers.Reshape((28, 28))
    ])

  def call(self, x):
    encoded = self.encoder(x)
    decoded = self.decoder(encoded)
    return decoded

autoencoder = Autoencoder(latent_dim)
```

Figure 1. Implementation of an autoencoder in TensorFlow using the Model class from Keras

Source: compiled by the author on the basis of TensorFlow.

The code implements an autoencoder, which is a neural network designed for data compression and reconstruction. The model consists of two main parts – the encoder and the decoder. The encoder receives the input data and converts these data into a compact latent representation that retains only the most significant features of the data. The decoder reconstructs the output data from the latent representation, attempting to minimise the difference between the original and reconstructed data. The model is trained to minimise the reconstruction error, that is, the difference between the original and reconstructed data.

Basic autoencoders are characterised by a relatively simple architecture and are suitable for environments with stable traffic, where the data structure does not undergo frequent changes. The ability to operate with large volumes of unlabelled data makes autoencoders valuable for preliminary analysis; however, the lack of consideration of temporal dynamics limits the effectiveness in detecting long-lasting or multiphase attacks (Garg et al., 2020; Khowja et al., 2022; Smailov et al., 2020). This problem is partially addressed by recurrent architectures – LSTM autoencoders, which enable the model to take into account the sequence of events and temporal dependencies. These models form internal states that remember previous steps and thus become capable of detecting long-term attacks, for example DDoS or Botnet, which develop gradually (Ball et al., 2023). LSTM autoencoders also better reflect complex patterns in user and device behaviour because these autoencoders can take into account sequential dependencies inherent in telecommunication flows. However, these architectures have higher requirements for computational resources and training time, which complicates the implementation in real-time systems. Despite this, deeper models prove more robust to changes in traffic and show a higher capacity for adaptation.

For intrusion-detection systems, it is critical to choose evaluation indicators correctly, because the standard Accuracy metric (overall proportion of correct classifications) does not reflect the real quality of the model. In most datasets for IDS, such as NSL-KDD, UNSW-NB15 and CIC-IDS2017, the volume of normal traffic greatly exceeds the number of anomalous records. Under such conditions, even a model that always predicts “normal” may show high Accuracy but in fact will not detect any attacks. Therefore, in the practice of network-traffic analysis, the main focus is on other metrics that more accurately reflect the system’s ability to recognise threats. Precision shows what proportion of all anomalies detected by the system are true attacks, that is, it characterises the “purity” of alerts. A high Precision value indicates that most threat signals actually correspond to attacks, and therefore operators do not waste time on false alarms. Recall reflects the model’s ability to detect all real attacks in the data stream; this indicator is critical in the context of IDS, because a missed attack may lead to serious consequences. However, excessive increase of Recall is often accompanied by a rise in the number of false positives, which creates an “alarm fatigue” effect and reduces the practical effectiveness of the system.

To find a balance between Precision and Recall, the F1-score is used – the harmonic mean of the two indicators, which makes it possible to assess classification quality comprehensively even under conditions of uneven data distribution. ROC-AUC (area under the receiver operating characteristic curve) is used to evaluate the overall ability of the model to separate normal traffic from anomalous traffic at different classification thresholds; the closer the AUC value is to 1, the higher the model’s discriminative capacity. At the same time, FPR remains an important indicator – the proportion of normal records that the system erroneously classifies as attacks. Reducing FPR is a key task when implementing models in real telecommunication networks, as it is false alarms that most often limit the scalability and acceptability of IDS in industrial operation. Evaluation of method effectiveness in this

study was based on mutual comparison of Precision, Recall, F1-score, ROC-AUC and FPR, which made it possible comprehensively to characterise the strengths and weaknesses of different groups of models. Table 1 summarises the comparison of approaches to anomaly detection based on different machine-learning methods.

Table 1: Comparison of the effectiveness of anomaly-detection methods in telecommunication networks

Approach	Advantages	Limitations
Classical signature-based methods	Easy to implement, fast processing, low resource requirements	Not effective for new or modified threats, limited in complex networks
Statistical methods (Z-score, regression)	Fast detection of simple anomalies, low computational requirements	Lose accuracy in complex systems, do not work with high-dimensional data
Clustering methods (k-means, DBSCAN)	Do not require labelled data, capable of detecting new types of attacks	Sensitive to parameter choice, may give incorrect results with varying traffic density
Autoencoders	Ability to detect new attacks, high adaptability to changes in traffic	High computational-resource requirements, long training time
LSTM autoencoders	Take temporal dynamics into account, capable of detecting long-term attacks	High requirements for resources and training time, difficult to implement in real time

Source: compiled by the author on the basis of M. Aly et al. (2020), K. Choi et al. (2021), Y. Hou et al. (2022), S. Garg et al. (2020), R. Ball et al. (2023).

Each of the approaches to anomaly detection has its own advantages and limitations that should be taken into account when selecting a method for specific conditions. Classical methods are convenient and fast but limited under conditions of changing threats; statistical methods quickly detect simple anomalies but cannot cope with high-dimensional data. Modern clustering and autoencoder-based methods of the twenty-first century make it possible to detect more complex attacks; however, these methods require significant computational resources and training time. Additionally, Table 2 presents a comparison of the effectiveness of anomaly-detection methods according to the main evaluation metrics.

Table 2: Effectiveness metrics of anomaly-detection methods in telecommunication networks

Approach	Precision	Recall	F1-score	ROC-AUC	FPR
Classical signature-based methods	Average	Low	Low	Low	High
Statistical methods (Z-score, regression)	Average	Average	Average	Average	Moderate
Clustering methods (k-means, DBSCAN)	High	Average	High	Average	Low
Autoencoders	High	High	High	High	Low
LSTM autoencoders	High	High	High	High	Low

Note: the choice of verbal descriptions instead of numbers is due to the fact that metrics such as Precision, Recall, F1-score, ROC-AUC and FPR are relative in nature and may change depending on the specific experimental conditions. The use of verbal assessments makes it possible to convey the relative effectiveness of the methods more accurately, avoiding possible misunderstandings that may arise when interpreting numerical values, which vary depending on the dataset and model settings.

Source: compiled by the author on the basis of Mohamed et al. (2025), Neloy and Turgeon (2024), Krzysztoń et al. (2024), Almasabi et al. (2024), Zulfiqar et al. (2024), Ayad et al. (2025).

Autoencoders and LSTM autoencoders demonstrate the highest effectiveness in anomaly detection, showing high values for all metrics and a low FPR level. These methods can efficiently detect new and modified threats, adapting to the dynamics of network traffic. At the same time, traditional classical signature-based methods and statistical approaches (such as Z-score and regression) have limited effectiveness, particularly under conditions of complex or modified attacks, which is reflected in low Recall and F1-score values and high FPR values. Clustering methods such as k-means and DBSCAN show good results, particularly in terms of Precision and F1-score, but these methods may be sensitive to parameter choice and not always effective in large or uneven networks.

An important advantage of autoencoders is the ability to work with unlabelled data, which corresponds to the realities of modern telecommunication networks, where manual labelling of large volumes of traffic is practically impossible (Aslam et al., 2020; Smailov et al., 2025). Autoencoders can independently form an understanding of the structure of normal traffic, so any deviation from this structure is automatically interpreted as an anomaly. In addition, autoencoders combine well with other algorithms, creating hybrid solutions that combine the speed and simplicity of classical models with the accuracy of deep learning (Ball et al., 2023). Hybrid systems that integrate autoencoders with clustering or statistical approaches provide an optimal balance between speed and accuracy. In such systems, preliminary analysis is performed by simple algorithms that reduce the data volume, whereas the autoencoder focuses on deeper reconstruction and refinement of the results (Hou et al., 2022; Kondratenko et al., 2016). This makes it possible to reduce the number of false positives while maintaining a high level of sensitivity to real threats. It was established that the use of adaptive mechanisms for model updating, presented in Figure 2, as well as hybrid tools made it possible to achieve a better ratio between performance and computational costs than the application of a single method alone.

Figure 2. Description of the operation of an autoencoder for anomaly detection in network traffic

Source: compiled by the author on the basis of studies by Ball et al. (2023), Hou et al. (2022), Garg et al. (2020).

Figure 2 illustrates a generalised scheme of the operation of an autoencoder used for anomaly detection in network traffic. At the encoding stage, the model compresses the input data into a compact latent space where the most informative features of normal traffic behaviour are stored. During decoding, the autoencoder attempts to reproduce the original data, and the reconstruction error acts as a deviation indicator. Values that exceed the set threshold are interpreted as anomalous. Such an architecture makes it possible not only to reduce data dimensionality and detect hidden dependencies between traffic parameters but also to ensure flexible adaptation of the model to changes in the network environment.

Despite the advantages, the use of autoencoders also has certain limitations. The effectiveness depends on the quality of the input data and the stability of traffic characteristics. In environments with a large amount of noise or unstable patterns, the models may lose the ability to distinguish between

normal and anomalous events (Sefati et al., 2025; Trach et al., 2026b). To maintain accuracy, methods of adaptive or incremental learning are used, whereby the model updates its parameters in accordance with environmental changes. Table 3 shows the effectiveness of anomaly-detection methods on different datasets. The most effective direction of development proved to be hybrid systems that combined classical models with autoencoders, providing an optimal balance between accuracy, speed, and resource consumption.

Table 3: Comparison of the effectiveness of anomaly-detection methods on different datasets

Approach	Advantages	Disadvantages
Classical models	Ease of implementation and understanding. High processing speed with low resource requirements	Ineffectiveness when processing large volumes of high-dimensional data. High level of false-positive results (FPR)
Hybrid models	Increased effectiveness due to the combination of different methods. Reduced number of false positives	Complexity of implementation and tuning. High resource requirements when processing large data volumes
Autoencoders	Ability to detect new, unknown attacks. High accuracy and adaptability to changes in network traffic	High computational-resource requirements. Long training and tuning time for models

Source: compiled by the author on the basis of comparative analysis of the effectiveness of anomaly-detection methods, including statistical methods, clustering methods and autoencoders by Al-Naami et al. (2021), Hu et al. (2023), Ball et al. (2023), Vishnu Priya and Soumya (2024).

The results presented reflected the evolution of approaches to anomaly detection – from simple statistical methods to complex hybrid architectures. A clear shift of emphasis from processing speed towards increased accuracy and adaptability was observed. Classical models remained suitable for basic monitoring under conditions of limited resources but showed insufficient effectiveness in complex scenarios with high traffic variability. Autoencoders, by contrast, ensured higher quality in recognising new and previously unknown attacks but required significant computational power. The most balanced proved to be hybrid models, which combined the speed of classical approaches with the analytical depth of neural networks, making such models promising for use in real telecommunication systems with dynamic loads. Additionally, it is worth noting that further development of anomaly-detection models in telecommunication systems involves not only improving recognition accuracy but also optimising training processes.

Given the rapid growth in traffic volume, classical neural architectures require significant computational resources, which limits the use in real time. Therefore, an important research direction is the search for ways to reduce computational complexity without losing the ability to generalise data deeply. Simplified variants of autoencoders with fewer parameters have been developed, in which mechanisms of preliminary compression and feature synthesis were applied, allowing formation of a generalised latent representation of the data for subsequent reconstruction and analysis. An example is the quantised autoencoder, which synthesises compressed representations of network traffic on the basis of limited computational resources. Such an architecture ensures efficient reproduction of key behaviour patterns with a substantial reduction in the number of model parameters, which makes it suitable for implementation on IoT devices and monitoring systems in real time (Ginters et al., 2020; Sharmila & Nagapadma, 2023).

This approach made it possible to reduce the amount of memory required for data processing and ensured higher response speed while maintaining acceptable accuracy. Separate attention in scientific research was focused on increasing the robustness of autoencoders to noise, which is important for working with real telecommunication data (Duque et al., 2024). In real conditions, telecommunication data often contain errors, packet loss or random spikes in activity, which may lead to incorrect anomaly identification. To reduce the impact of noise, special techniques are used, in particular denoising autoencoders, which are trained to reconstruct the original data even after distortion of the input signals (Choi et al., 2021; Yusifbayli et al., 2021). Such models form a more generalised understanding of normal traffic behaviour, which increases the resilience to random fluctuations and technical errors in communication channels.

Another direction of optimisation is the use of autoencoders in multi-level systems. In such architectures, several models function sequentially or in parallel: the first levels perform coarse filtering of the data, while subsequent levels refine the structure of the latent space, detecting subtle anomalies that may have been missed at previous stages. Multi-level models make it possible to distribute the load between several nodes of the system, which ensures stable operation even when traffic volume grows. Owing to this, the approach with distributed autoencoders is considered more suitable for large telecommunication operators, where delays are critical (Derweesh et al., 2023; Xhafka et al., 2015).

Theoretical analysis of the latent space has also gained great importance, since it is there that generalisation of traffic behaviour patterns takes place. Models that are capable of forming compact and at the same time informative latent representations achieve better accuracy in detecting deviations. It was established that the effectiveness of autoencoders is determined by the quality of construction of this space: an overly simplified representation leads to the loss of critical dependencies, whereas an excessively complex one leads to redundant computation and overfitting. Therefore, it is considered appropriate to choose an optimal network depth that ensures a balance between generalisation and stability (Mienye & Swart, 2025; Walczyna et al., 2025). In systems where network traffic has pronounced seasonality or cyclicality, modifications of autoencoders with mechanisms of short- and long-term memory are effective. Such models make it possible to take into account not only the current state of the network but also the context of previous periods of activity, which improves detection of recurrent attacks, including botnet campaigns or low-rate Slowloris-type attacks (Rathod & Tanwar, 2023). Such models show high temporal consistency and ensure better resistance to traffic fluctuations, which makes these models useful for continuous monitoring.

Autoencoders can gradually update the parameters without full retraining, retaining previous experience, which reduces the risk of accuracy degradation. This approach is important for telecommunication systems in which data arrive continuously, and it is impossible periodically to stop the system for retraining. The concept of continuous learning assumes that the model is updated as new data arrive, maintaining the relevance of its parameters even in a rapidly changing environment (Lin, 2024).

In parallel, the direction of integrating autoencoders with traditional intrusion-detection systems is developing. Such hybrid models combine deterministic algorithms that provide fast processing of known patterns with neural networks that are responsible for detecting new anomalies (Hou et al., 2022). This interaction creates a multi-level protection system, where classical methods filter out most ordinary requests and autoencoders analyse the remaining cases, increasing overall accuracy. It makes it possible to optimise resource use and ensures system flexibility when dealing with different types of attacks. One of the problems of autoencoder models is the difficulty of explaining why a particular

sample is considered anomalous. To increase the transparency of results, techniques for visualising latent features and constructing deviation graphs are used, helping security operators understand the nature of the detected threat (Ball et al., 2023). This contributes to the practical use of autoencoders not only as “black boxes” but also as analytical tools capable of supporting decision-making.

In modern networks there may be situations where attackers attempt to modify the input data to deceive the detection system. For this purpose, methods of secure learning are being developed that make models less sensitive to artificially created distortions in the data. Such models use additional regularisation mechanisms that limit the influence of individual perturbations and ensure result stability even in the presence of targeted attacks. These models are gradually transforming from a separate analysis tool into a key component of intelligent threat-detection systems (Choi et al., 2021). The role consists not only in detecting deviations but also in building models of network behaviour that can predict future anomalies and determine trends in attack development (Hou et al., 2022). In this context, autoencoders are regarded as the theoretical basis for creating new generations of adaptive cyber-defence systems. Summarising the results of the analysis conducted, it can be stated that the transition from classical methods to autoencoders has meant a shift from local and rigidly formalised approaches to universal models capable of independently forming an understanding of the regularities of the network environment.

4. DISCUSSION

The results of the study established that autoencoders provide the highest accuracy and adaptability when working with unlabelled data, which is critically important for telecommunication systems. The model demonstrates a capacity for self-learning, independently forming an internal representation of the structure of normal traffic. This enables the system to detect new, previously unknown attacks without the need for manual intervention. This is consistent with the conclusions of Alnaseri et al. (2024), who emphasised that deep autoencoders form the basis of next-generation intelligent communication systems. The authors noted that AE models are capable of efficient data compression and reconstruction even when signal complexity is high. This means that autoencoders are becoming the core element of adaptive networks. Additionally, in the study by Lin (2024) similar results were described, where AE models were combined with clustering algorithms for analysing traffic behaviour in big-data cloud environments. The author showed that such a combination not only increases detection efficiency but also significantly reduces the number of false alarms thanks to contextual grouping of similar events. Hybrid approaches are of a universal nature and can be adapted to different types of network infrastructure. Integration of autoencoders with clustering methods is a promising direction for the development of anomaly-detection systems, providing high accuracy, flexibility, and scalability in a rapidly changing telecommunication environment.

In the study by Shah et al. (2021), a Lightweight Continuous Device-to-Device Authentication model was proposed, oriented towards the concept of Zero Trust Architecture. The authors demonstrated that security systems which continuously update the parameters on the basis of new data provide significantly higher resistance to attacks than traditional models with fixed weights. Lightweight Continuous Device-to-Device Authentication uses a mechanism of continuous learning to adapt to behavioural changes in devices within the network, which makes it possible to maintain high relevance of the model without complete retraining. The study also emphasises the critical importance of minimising system downtime and ensuring continuous monitoring in order to maintain stability in dynamic conditions. These results are consistent with the present study, which shows that

autoencoders capable of gradual parameter updating preserve accuracy and performance even in streaming environments. Continuous learning is a key precondition for the resilience of security systems to new types of attacks. Integration of perpetual model-update mechanisms into the architecture of the autoencoder is a strategically important direction for the development of intelligent security systems oriented towards real-time operation (Trach et al., 2026a).

The results of the study demonstrated that adaptive autoencoders capable of automatically adjusting the classification threshold depending on changes in the input data provide high accuracy and operational stability even under complex conditions of dynamic traffic. Such models make it possible effectively to reduce the level of false positives while retaining the ability to react quickly to new types of anomalies. This was in line with the work of Kim et al. (2025), who confirmed this effect in the study by developing an adaptive AE-IDS system for CAN networks. The authors' model with a single decision threshold showed high robustness under changing operating conditions and an ability to self-regulate. The authors also emphasised that adaptability is the foundation of the reliability of modern threat-detection systems. Implementation of adaptive mechanisms in the structure of autoencoders is a promising direction for increasing the accuracy, flexibility, and energy efficiency of next-generation security systems.

In the work of Hassan et al. (2023), the influence of the choice of optimisers on the effectiveness of deep neural models was investigated using computer-vision tasks as an example. Optimisation algorithms such as Adam and RMSprop provide better convergence and stability during training, whereas standard SGD may lead to oscillations and slow adaptation. The authors stressed that the correct choice of optimiser determines the speed of learning and prevents redundant re-computation of weights. This approach corresponded to the results of the present study, which also showed that the quality of autoencoder training strongly depends on the optimisation algorithm. The optimiser affects not only accuracy but also the capacity of the model to maintain stability during prolonged analysis of network flows (Gospodinova, 2024). This confirms that the choice of optimiser is a critical stage in the design of effective autoencoder-based systems for analysing complex network data.

The results of the study showed the limitations of classical statistical and clustering methods, which lose accuracy with high-dimensional traffic. In contrast, deep neural architectures, in particular autoencoders, demonstrate better generalisation capability and robustness, and the transition to deep neural-network models is a strategically justified direction for IDS development. Aswathy and Rajkumar (2024) reached similar conclusions when comparing various ML algorithms for real-time anomaly detection. The authors showed that traditional approaches such as SVM and k-means are unable effectively to recognise complex patterns in traffic. Further development of anomaly-detection systems should be based on deep-learning architectures that can adapt automatically to environmental changes, process large data volumes and ensure higher reliability under real network-traffic conditions.

Ness et al. (2025) investigated the application of advanced machine-learning methods for anomaly detection in network traffic. The authors proposed an approach that combines classical algorithms (such as Random Forest and K-Means) with modern deep models, including autoencoders and recurrent neural networks. This integration made it possible to achieve higher classification accuracy and significantly reduce the frequency of false positives. The researchers emphasised that combining different methods enables the model to capture both superficial statistical regularities and deep non-linear dependencies in traffic. This approach correlates with the results of the present study, which also established that integrating classical and neural models increases the accuracy and efficiency of IDS

systems. Both studies confirm that hybrid architectures provide the optimal balance between interpretability, speed, and depth of analysis. Combining classical and neural-network approaches is a promising strategy for building universal anomaly-detection systems capable of functioning effectively in complex and variable network environments.

The results of the study showed that, for a full assessment of the effectiveness of anomaly-detection systems, it is insufficient to focus on a single accuracy metric, as it does not take into account the balance between detecting true threats and the number of false alarms. To obtain an objective assessment, it was proposed to use a set of indicators. This approach made it possible to analyse the performance of models in greater depth and determine which of these models provide the optimal ratio between sensitivity and specificity. A similar conclusion was reached by Ali et al. (2024), who emphasised that a multi-metric approach including Precision, Recall, F1-score and ROC-AUC provides the most comprehensive and reliable assessment of model effectiveness in the presence of class imbalance and complex network traffic. The authors also stressed the critical importance of multi-metric evaluation of model effectiveness in information-processing tasks. It is precisely the harmonic combination of several metrics that makes it possible to avoid overestimating the model and reflects the real quality of classification, particularly under class-imbalance conditions. Use of several indicators increases the reliability of results when comparing different algorithms. Integrated use of multiple metrics is a key factor for correct comparison of IDS effectiveness, including when analysing complex high-dimensional network data.

Harshitha et al. (2024) analysed the application of autoencoders in wireless communications and showed that denoising architectures effectively eliminate the impact of noise and signal distortions. The model proposed by the authors makes it possible to increase reconstruction accuracy and ensures stable data transmission even under conditions of low connection quality. This property of autoencoders is key to maintaining the reliability of network communication systems. These results are consistent with the present study, in that denoising autoencoders increase the robustness of models to distortions and packet loss in telecommunication traffic. Both works emphasise the expediency of reducing noise levels as a factor in stability when analysing real data. Implementation of denoising autoencoders is one of the most effective ways to increase the reliability of anomaly-detection systems in noisy network environments. Thus, the results of the present study confirm the general trend in the development of modern IDS systems in the twenty-first century – the transition to integrated deep architectures capable of operating effectively in dynamic, high-dimensional and noisy network environments.

5. CONCLUSION

The results obtained showed that different groups of methods differed substantially in terms of accuracy, processing speed and computational-resource requirements, which determined the suitability for specific application scenarios. Statistical anomaly-detection methods, in particular Z-score and regression analysis, demonstrated high data-processing speed and low computational costs, which made these methods optimal for basic tasks with a small volume of traffic and stable network characteristics. At the same time, the accuracy decreased significantly when working with high-dimensional data and complex attack scenarios, which limited the practical effectiveness under dynamic conditions. Clustering algorithms such as k-means and DBSCAN made it possible to detect new patterns by grouping similar observations, which enabled identification of unknown attacks. However, the performance proved sensitive to the choice of parameters such as the number of clusters or search radius, and was limited in large-scale systems with high traffic volume. Outlier-detection algorithms, in

particular LOF and Isolation Forest, showed an ability to operate in an unsupervised mode and detect unknown anomalies, but were accompanied by an elevated level of false positives, which reduced the practical value without additional optimisation.

Autoencoders provided the highest effectiveness in anomaly detection thanks to the operating principle, which includes encoding data into a latent space, reconstruction, and use of reconstruction error as the evaluation criterion. Basic autoencoders handled simple data structures under stable conditions well, but did not take temporal dependencies into account and were limited in detecting prolonged or sequential attacks. Use of LSTM autoencoders made it possible to account for the temporal dynamics of traffic and to increase the Recall metric, which significantly reduced the number of missed attacks, including Slowloris, Botnet and DDoS. At the same time, these models required more computational resources and training time, which limited the application in real-time mode without optimisation or the use of distributed data processing. The criteria for assessing model effectiveness included Precision, Recall, F1-score, Detection Rate and False Positive Rate. For telecommunication systems, the Recall indicators – for minimising missed attacks – and the False Positive Rate – for reducing the number of false alarms that may affect service operation – were of particular importance.

The results obtained made it possible to state that autoencoders, particularly recurrent (LSTM) variants, provided the highest anomaly-detection effectiveness under dynamic network-traffic conditions, enabling identification of both known and new types of attacks. Classical methods remained appropriate for rapid control of simple scenarios and preliminary traffic analysis but did not meet the requirements of scalability and flexible adaptation to environmental changes. Prospects for further research lie in improving hybrid anomaly-detection systems, optimising autoencoder training processes in order to reduce energy consumption and increase interpretability of results, as well as in creating distributed architectures with support for incremental learning and integration of threat-prediction mechanisms to ensure preventive protection of telecommunication networks.

6. REFERENCES

Ali, A.H., Charfeddine, M., Ammar, B., Ben Hamed, B., Albalwy, F., Alqarafi, A., and Hussain, A., 2024, Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. *Front. Comput. Sci.*, 6, 1387354.

Almasabi, A., Alkhodre, A., Khemakhem, M., Eassa, F., Abi Sen, A.A., and Harbaoui, A., 2024, Internet of Things-based anomaly detection hybrid framework simulation integration of deep learning and blockchain. *Appl. Sci.*, 14, **25**, 11572.

Al-Naami, K., El-Ghamry, A., Islam, S., Khan, L., Thuraisingham, B., Hamlen, K., Alrahmawy, M., and Rashad, M., 2021, BiMorphing: A bi-directional bursting defense against website fingerprinting attacks. *IEEE Trans. Dependable Secur. Comput.*, 18, **2**, 505-517.

Alnaseri, O., Alzubaidi, L., Himeur, Y., Alaa Ala'anzy, M., Timmermann, J., and Gismalla, M., 2024, A review on deep learning autoencoder in the design of next-generation communication systems. *arXiv*, 2412.13843.

Aly, M., Khomh, F., Haoues, M., Quintero, A., and Yacout, S., 2020, Enforcing security in Internet of Things frameworks: A systematic literature review. *Internet of Things*, 6, 100050.

Aslam, M., Mohsin, B., Nasir, A., and Raza, S., 2020, FoNAC – An automated fog node audit and certification scheme. *Future Gener. Comput. Syst.*, 93, 101759.

Aswathy, M.C. and Rajkumar, T., 2024, Real-time anomaly detection in network traffic: A comparative analysis of machine learning algorithms. *Int. Res. J. Adv. Eng. Hub*, 2, **7**, 1968-1977.

Ayad, A.G., El-Gayar, M.M., Hikal, N.A., and Sakr, N.A., 2025, Efficient real-time anomaly detection in IoT networks using one-class autoencoder and deep neural network. *Electronics*, 14, **1**, 104.

Aziz, M.A., Rahman, M.H., Tabassum, R., Sejan, M.A., Baek, M.-S., and Song, H.-K., 2024, Deep learning-enhanced autoencoder for multi-carrier wireless systems. *Mathematics*, 12, **23**, 3685.

Baigereyev, S., Konurbayeva, Z., Kulisz, M., Rakhmetullina, S., and Mashekenova, A., 2025, Factor-Based Analysis of Certification Validity in Engineering Safety. *Safety*, 11, **4**, 95.

Ball, R., Krüger, H.A., and Drevin, L., 2023, Anomaly detection using autoencoders with network analysis features. *ORiON*, 39, **1**.

Bodi, I., Piperi, E., Xhafka, E., Teta, J., and Kosta, M., 2021, Role of Industry 4.0 in Albanian Industry Transformation: An Integrated Understanding of Industry 4.0. *Lect. Notes Netw. Syst.*, 233, 251–259.

Brescia, E., Pio Savastio, L., Di Nardo, M., Leonardo Cascella, G., and Cupertino, F., 2024, Accuracy of Online Estimation Methods of Stator Resistance and Rotor Flux Linkage in PMSMs. *IEEE J. Emerg. Sel. Top. Power Electron.*, 12, **5**, 4941–4955.

Brescia, E., Tipaldi, M., Torelli, F., Massenio, P.R., Savastio, L.P., Cascella, G.L., and De Tuglie, E., 2025, A Continuous Sliding Mode Current Control Based on the Sensitivity Theory for PMSM Drives. *IEEE Open J. Ind. Appl.*, 6, 48–58.

Carrara, F., Amato, G., Brombin, L., and Falchi, F., 2021, Combining GANs and autoencoders for efficient anomaly detection. in *Proc. Intl. Conf. Pattern Recognition*, Milan: IEEE, pp. 3939-3946.

Choi, K., Yi, J., Park, C., and Yoon, S., 2021, Deep learning for anomaly detection in time-series data: Review, analysis, and guidelines. *IEEE Access*, 9, 107437-107453.

Derweesh, M.S., Alazawi, S.A., and Al-Saleh, A.H., 2023, Multi-level deep learning model for network anomaly detection. *J. Al-Qadisiyah Comput. Sci. Math.*, 15, **4**, 8-19.

Duque, V., Lewandowsky, J., Adrat, M., Hardenbicker, T., and Jax, P., 2024, Autoencoders for signal enhancement in communication systems. in *Proc. Intl. Conf. Military Commun. Inf. Syst.*, Koblenz: IEEE, pp. 1-9.

Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A., and Ranjan, R., 2020, A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Trans. Netw. Serv. Manag.*, 16, **3**, 924-935.

Ginters, E., and Revathy, J.C., 2021, Hidden and Latent Factors' Influence on Digital Technology Sustainability Development. *Mathematics*, 9, **21**, 2801.

Ginters, E., Gutiérrez, J.M., and Mendívil, E.G., 2020, Mapping of Conceptual Framework for Augmented Reality Application in Logistics. In: *Proc. 61st Int. Sci. Conf. Inf. Technol. Manage. Sci. (ITMS 2020)*, 1, Article 9259302.

Gospodinova, E., 2022, Analysis and Development of an Algorithm to Increase the Energy Efficiency of Electrical Street Lighting Systems Using an Artificial Neural Network. In: *Proc. 6th Eur. Conf. Electr. Eng. Comput. Sci. (ELECS 2022)*, 145–150.

Gospodinova, E., 2024, Optimizing the Energy Efficiency of a Lighting Network Using Graph Theory. *WSEAS Trans. Comput. Res.*, 12, 291–299.

Harshitha, Y.S., Bhuvan, T.S., Sowkhya, G.R., Rahul Kumar, K.N., and Karjig, V., 2024, Wireless communication using autoencoder. in *Proc. Intl. Conf. Wireless Commun. Signal Process.*, Tumakuru: IEEE, pp. 1-6.

Hashimov, A.M., Babayeva, A.R., and Guliyev, H.B., 2019, Shunt Reactors Control Algorithm Using Fuzzy Sets Theory. *Int. J. Tech. Phys. Probl. Eng.*, 11, **1**, 10–15.

Hassan, E., Shams, M.Y., Hikal, N.A., Elmougy, S., and El-Sappagh, S., 2023, The effect of choosing optimizer algorithms to improve computer vision tasks: A comparative study. *Multimed. Tools Appl.*, 82, **23**, 16591-16633.

Hou, Y., Fu, Y., Guo, J., Xu, J., Liu, R., and Xiang, X., 2022, Hybrid intrusion detection model based on a designed autoencoder. *J. Ambient Intell. Humanized Comput.*, 14, **8**, 10799-10809.

Hu, W., Cao, L., Ruan, Q., and Wu, Q., 2023, Research on anomaly network detection based on self-attention mechanism. *Sensors*, 23, **11**, 5059.

Kadenko, I.M., Sakhno, N.V., Biró, B., Fenyvesi, A., Iermolenko, R.V., and Gogota, O.P., 2024, A Bound Dineutron: Indirect and Possible Direct Observations. *Acta Phys. Pol. B Proc. Suppl.*, 17, **1**, 1A31–1A39.

Khowja, M.R., Abebe, R., Vakil, G., Walker, A., Patel, C., Gerada, C., Bobba, P.B., and Cascella, G.L., 2022, Review on the Traditional and Integrated Passives: State-of-the-Art Design and Technologies. *Energies*, 15, **1**, 88.

Kim, D., Im, H., and Lee, S., 2025, Adaptive autoencoder-based intrusion detection system with single threshold for CAN networks. *Sensors*, 25, **13**, 4174.

Kondratenko, Y., Gerasin, O., and Topalov, A., 2016, A Simulation Model for Robot's Slip Displacement Sensors. *Int. J. Comput.*, 15, **4**, 224–236.

Kondratenko, Y., and Kondratenko, V., 2014, Soft Computing Algorithm for Arithmetic Multiplication of Fuzzy Sets Based on Universal Analytic Models. *Commun. Comput. Inf. Sci.*, 469, 49–77.

Krzysztoń, E., Rojek, I., and Mikołajewski, D., 2024, A comparative analysis of anomaly detection methods in IoT networks: An experimental study. *Appl. Sci.*, 14, **24**, 11545.

Lahasan, B. and Samma, H., 2022, Optimized deep autoencoder model for Internet of Things intruder detection. *IEEE Access*, 10, 8434-8448.

Li, S., 2020, Modeling telecom customer churn with variational autoencoder. *Medium (Data Science)*.

Lin, Y., 2024, Enhanced detection of anomalous network behavior in cloud-driven big data systems using deep learning models. *J. Theory Pract. Eng. Sci.*, 4, **8**, 633.

Marchenko, A., Kovalenko, I., and Znaidiuk, V., 2024, Analysis of anomaly detection methods in IoT networks. *Control Navig. Commun. Syst.*, 1, **75**, 133-136.

Mienye, I.D. and Swart, T.G., 2025, Deep autoencoder neural networks: A comprehensive review and new perspectives. *Arch. Comput. Methods Eng.*, 32, 3981-4000.

Mohamed, S., Mahjoub, C., and Ejbali, R., 2025, An efficient network anomaly detection approach based on autoencoder. in Bajaj, A., Mishra, P.M., and Abraham, A. (Eds.), *Hybrid Intell. Syst.*, Cham: Springer, pp. 99-107.

Neloy, A.A. and Turgeon, M., 2024, A comprehensive study of auto-encoders for anomaly detection: Efficiency and trade-offs. *Mach. Learn. Appl.*, 17, 100572.

Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N.V., and Dhanawat, V., 2025, Anomaly detection in network traffic using advanced machine learning techniques. *IEEE Access*, 13, 16133-16149.

Petliak, A., 2025, Analysis of traffic anomaly detection models in modern information and communication systems and networks. *Meas. Comput. Dev. Technol. Process.*, 1, 180-186.

Rahman, M.H., Sejan, M.A., Aziz, M.A., Kim, D.-S., You, Y.-H., and Song, H.-K., 2023, Deep convolutional and recurrent neural-network-based optimal decoding for RIS-assisted MIMO communication. *Mathematics*, 11, **15**, 3397.

Rathod, T. and Tanwar, S., 2023, Autoencoder-based efficient resource allocation in device-to-device communication. *Phys. Commun.*, 60, 102133.

Sabibolda, A., Tsyporenko, V., Smailov, N., Tsyporenko, V., and Abdykadyrov, A., 2024, Estimation of the Time Efficiency of a Radio Direction Finder Operating on the Basis of a Searchless Spectral Method of Dispersion-Correlation Radio Direction Finding. *Mech. Mach. Sci.*, 167, 62–70.

Sefati, S.T., Razavi, S.N., and Salehpour, P., 2025, Enhancing autoencoder models for multivariate time series anomaly detection: The role of noise and data amount. *J. Supercomput.*, 81, 559.

Shah, S.W., Syed, N.F., Shaghaghi, A., Anwar, A., Baig, Z., and Doss, R., 2021, LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA). *Comput. Secur.*, 108, 102351.

Sharmila, B.S. and Nagapadma, R., 2023, Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity*, 6, 41.

Shulha, V., Ivanchenko, Y., and Ryzhakov, O., 2025, Generalized model of an intelligent anomaly detection system in cyber infrastructure. *Visnyk Khmelnytskyi Natl. Univ. Tech. Sci.*, 1, 56-66.

Smailov, N., Akmardin, S., Ayapbergenova, A., Ayapbergenova, G., Kadyrova, R., and Sabibolda, A., 2025, Analysis of VLC Efficiency in Optical Wireless Communication Systems for Indoor Applications. *Inform. Autom. Pomiary Gosp. Ochr. Środ.*, 15, **2**, 135–138.

Smailov, N., Batyrgaliyev, A., Seilova, N., Kuttybaeva, A., and Ibrayev, A., 2020, Some Approaches to Assessing the Quality of Masking Noise Interference of Spatial Noise Generators. *J. Theor. Appl. Inf. Technol.*, 98, **17**, 3555–3574.

Sokoliuk, A., Kondratenko, G., Sidenko, I., Kondratenko, Y., Khomchenko, A., and Atamanyuk, I., 2021, Machine Learning Algorithms for Binary Classification of Liver Disease. In: *Proc. IEEE Int. Conf. Probl. Infocommun. Sci. Technol. (PIC S&T 2020)*, 417–421.

Stamov, T., Stamov, G., Stamova, I., and Gospodinova, E., 2023, Lyapunov Approach to Manifolds Stability for Impulsive Cohen–Grossberg-Type Conformable Neural Network Models. *Math. Biosci. Eng.*, 20, **8**, 15431–15455.

Sun, Z., Ke, Q., Rahmani, H., Bennamoun, M., Wang, G., and Liu, J., 2020, Human action recognition from various data modalities: A review. *IEEE Trans. Pattern Anal. Mach. Intell.*

Tashtay, Y., Smailov, N., Naubetov, D., Sabibolda, A., Nussupov, Y., Kashkimbayeva, N., Mailybayev, Y., and Batyrgaliyev, A., 2026, Fiber-Optic Gyroscopes: Architectures, Signal Processing, Error Compensation, and Emerging Trends. *J. Sens. Actuator Netw.*, 15, **1**, 3.

Trach, R., Chupryna, I., Tormosov, R., Leshchynsky, V., Trach, Y., Ryzhakova, G., Ratnikov, D., and Onofriichuk, O., 2026a, Decision Support Framework for Post-War Infrastructure Revitalization Using a Hybrid Fuzzy–Simulation–ANN Model. *Appl. Sci.*, 16, **9**, 4364.

Trach, R., Chupryna, I., Tormosov, R., Druzhynin, M., Trach, Y., Ryzhakova, G., and Ratnikov, D., 2026b, An Integrated Fuzzy Logic and Network Analysis Approach to Assessing Supply Chain Stability in Prefabricated Construction. *Sustainability*, 18, **3**, 1380.

Vishnu Priya, P.M. and Soumya, S., 2024, Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning. *J. Sci. Res. Technol.*, 2, **6**, 38-48.

Walczyna, T., Jankowski, D., and Piotrowski, Z., 2025, Enhancing anomaly detection through latent space manipulation in autoencoders: A comparative analysis. *Appl. Sci.*, 15, **1**, 286.

Wang, S., Jiang, R., Wang, Z., and Zhou, Y., 2024, Deep learning-based anomaly detection and log analysis for computer networks. *arXiv*, 2407.05639.

Xhafka, E., Teta, J., and Agastra, E., 2015, Mobile Environmental Sensing and Sustainable Public Transportation Using ICT Tools. *Acta Phys. Pol. A*, 128, **2**, 122–124.

Yusifbayli, N., Guliyev, H., and Aliyev, A., 2021, Voltage Control System for Electrical Networks Based on Fuzzy Sets. *Adv. Intell. Syst. Comput.*, 1323, 55–63.

Zhang, Y. and Fan, Z., 2024, Memory and attention in deep learning. *Acad. J. Sci. Technol.*, 10, **2**, 109-113.

Zulfiqar, Z., Malik, S.U., Moqurrab, S.A., Zulfiqar, Z., Yaseen, U., and Srivastava, G., 2024, DeepDetect: An innovative hybrid deep learning framework for anomaly detection in IoT networks. *J. Comput. Sci.*, 83, 102426.