

Machine Learning and Deep Learning Approaches for Anomaly Detection: A Review

Shaifun Nahar Sonia¹, Atul Sharma²

¹University of Science and Technology Chittagong (USTC), Chittagong, Bangladesh, South Asia.

²Department of Computer Science and Engineering, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, Haryana, India.

OPEN ACCESS

Article Citation:

Shaifun Nahar Sonia¹, Atul Sharma², "Machine Learning and Deep Learning Approaches for Anomaly Detection: A Review", International Journal of Recent Trends in Multidisciplinary Research, September-October 2026, Vol 6(05), 349-354.



©2026 The Author(s). This is an open access article distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. Published by 5th Dimension Research Publication

Abstract: Anomaly detection is a crucial machine learning problem designed to uncover observations or patterns that are unusual, or outlier behaviors. It is commonly used in cyber security, Internet of Things (IoT), industrial monitoring, health care and other data-driven systems. But anomaly detection is still a challenge due to the rarity, labelability, heterogeneity, and fluctuation of data distributions. In response to these challenges, a range of machine learning and deep learning techniques have emerged in recent years, including distance-based methods, classification models, clustering, reconstruction-based learning, sequential modelling, and sophisticated hybrid architectures. This review focuses on the key methods in the fields of ML and DL for anomaly detection, highlighting their mathematical formulation, principles, anomaly scoring methods, and applicable limitations. The studies reviewed show that DL approaches are suitable for complex non-linear and temporal patterns while ML approaches are suitable for structured and resource limited applications. The review also points out that class imbalance, false positives, generalisation, interpretability and computational requirements are challenges.

Keywords: Anomaly Detection; Machine Learning; Deep Learning; Cybersecurity; IoT.

1. Introduction

Anomaly detection is one of the significant challenges in machine learning and data analysis, aiming at the detection of observations or patterns that significantly deviate from normal behaviour. These deviations can be due to equipment failures, fraud, network intrusion, abnormal system conditions, and/or unusual events in large-scale data. As digital systems, sensors, communication networks and data driven applications generate more and more data, it has become increasingly difficult to manually identify abnormal patterns. Hence, automated anomaly detection is gaining popularity in intelligent monitoring and security, fault diagnosis, and decision-support applications [1]. The very concept of anomaly detection is shown in Fig. 1, where observations that do not follow the "normal" data pattern are detected as anomalous.

The basic approaches to anomaly detection are based on statistical assumptions, distance measures, density estimation, clustering and/or prescriptive decision rules. Patterns and decision boundaries can be learned from the available data by using machine learning techniques like Support Vector Machines, Decision Trees, Random Forests, k-Nearest Neighbours, clustering and ensemble learning [3]. Anomaly detection can be done by supervised, semi-supervised or unsupervised learning methods depending on the availability of labelled observations. These methods offer alternative means of modelling normal behaviour and specifying observations that fall out of the learned behaviours.

The growing dimensionality and complexity of today's data have also fueled the adoption of deep learning. Deep neural networks can learn a nonlinear and hierarchical representation from the data itself, thus decreasing the need for manually-designed features. An autoencoder can be used to identify anomalies via reconstruction error and a Convolutional Neural Network can identify spatial patterns, while Recurrent Neural Networks or Long Short-Term Memory networks can model temporal dependencies [4]. Other approaches that have been investigated, such as transformer-based models, have also been considered for learning contextual relations in complex data.

With all of this improvement, anomaly detection is still challenging because of the difficulty in labelling rare, diverse and hard-to-understand anomalous observations. Detection performance can be significantly influenced by the class imbalance, changing data distributions, feature quality, model selection, and detection-threshold selection. Moreover, even for highly

Machine Learning and Deep Learning Approaches for Anomaly Detection: A Review

imbalanced data sets, precision, recall, F1-score, ROC-AUC, PR-AUC are relevant evaluation measures besides accuracy [8].

This review examines machine learning and deep learning techniques used for anomaly detection with an emphasis on the underlying principles, mathematical formulations, important algorithms, training methods, measures for evaluation, and advantages and disadvantages. The discussion covers conventional ML methods, deep learning based approaches, reconstruction based techniques, representation learning, and emerging methods; followed by current challenges and future research directions of robust and reliable anomaly detection systems.

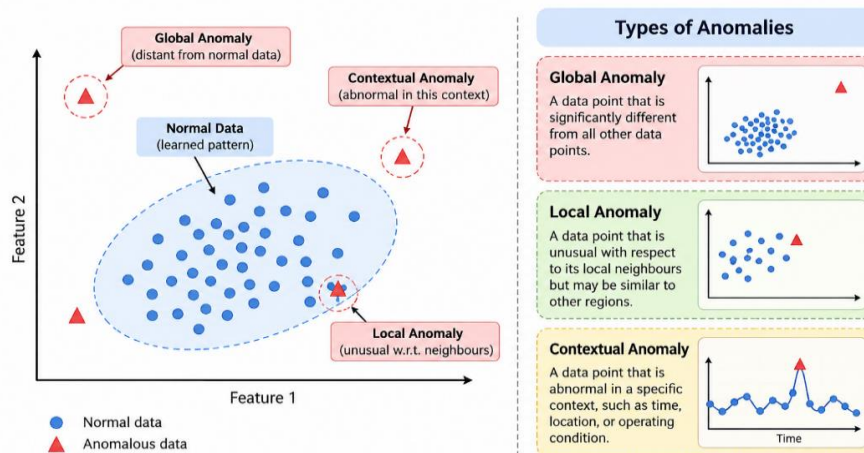


Fig. 1. Illustration of anomaly detection showing normal and anomalous data in a feature space.

2. Related Work

New research work has investigated machine learning and deep learning approaches for anomaly detection in IoT, industrial systems, networks, and cybersecurity. In recent years, conventional ML methods have evolved and been enhanced by hybrid architecture, feature learning, ensemble models, and domain-specific strategies to boost detection performance. Hence, Baimukanov et al. [1] introduced a multi-tier ML framework for IoT-Edge-Cloud anomaly detection with Isolation Forest, LOF, and XAI, but they focused their evaluation on an IoT-healthcare case study. Likewise, Aslam et al. [2] integrated ML, DL, statistical methods and feature augmentation for ICS anomaly detection, and the evaluation was primarily performed on the SWaT and Wind Turbine SCADA datasets. Narmadha and Balaji [3] optimized Autoencoder-LSTM model for network anomaly detection by using PSO, which focuses on false positive and class imbalance, but mainly highlights the detection accuracy. Although heterogeneous IoT traffic is a challenge, Hernandez-Jaimes et al. [4] proposed an attention-driven DNN for better One-Class SVM anomaly detection via network traffic representation. Additionally, Yadav et al. [5] presented LSTM-KNN-based framework with PSO/CFS feature selection technique, which obtained 95.76% accuracy, but using accuracy as the key reported indicator does not give much of an idea about this in highly imbalanced scenario. Mizanur et al. [6] studied Decision Tree, Random Forest and SVM based cyber threat prevention but their study was based on questionnaire based evidence and was not experimented on anomaly datasets.

More recently, the focus has shifted to advanced representation learning, uncertainty modelling, ensemble learning, and emerging computational paradigms. Goumidi and Pierre [7] built a stacking ensemble for the real-time detection of anomalies for the UNSW-NB15 and a medical specific dataset which needs further validation in medical environments and additional attacks. Yuan et al. [8] proposed using conformal prediction with ML/DL detectors to manage false alarms in the presence of temporal distribution shifts, but more testing on different industrial environments is needed. Although the framework proposed by Ahmad et al. [9] is based on QGAN for anomaly detection in IoT, substantial experimental validation and practical deployment in quantum are yet difficult. Gawusu et al. [10] proposed a compositional data-aware Autoencoder based on the CLR/ILR transformation and loss based on Aitchison-distance to identify geochemical anomalies, however, validation was limited to a small collection of data specific to a region, preventing broader generalisation. Zhang et al. [11] fused the sequence reconstruction with contrastive learning for protocol anomaly detection, but there is not enough information in the evaluation to generalise the results to other protocols. Likewise, Li et al. [12] introduced CKDGAT with GAT and reconstruction for the task of industrial time-series anomaly detection, and their two industrial testbeds do not have enough evidence to show cross-domain robustness. While FLOGA-AD is introduced by Wang et al. [13] which integrates CvT-LSTM, genetic client selection, federated learning and privacy mechanism for satellite networks, an extensive validation under heterogeneous federated setting is needed. In order to reduce energy usage, while maintaining lightweight Zero Trust authentication, Abdelhady et al. [14] fused LightGBM and Autoencoder-based detection with LoRaWAN. Last, Lachure and Doriya [15] combined hierarchical clustering with deep learning for ICS anomaly detection with BATADAL and WADI, with WADI having a poorer performance, suggesting its dependence on the dataset and operating conditions.

Table 1 summarizes the above discussed representative studies to emphasize the key aspects of the anomaly detection methods, application domains, contributions, and reported limitations.

Study	Application / Domain	Main Method	Key Contribution	Main Limitation
Baimukhanov et al. [1]	IoT-Edge-Cloud	Isolation Forest, LOF, XAI	Multi-tier anomaly detection with explainability	Healthcare-focused validation
Aslam et al. [2]	Industrial Control Systems	Hybrid ML, DL, statistical methods	Multi-feature anomaly detection	Limited dataset diversity
Narmadha and Balaji [3]	Network Security	Autoencoder-LSTM + PSO	Sequential anomaly detection with class-imbalance handling	Limited evaluation metrics
Hernandez-Jaimes et al. [4]	IoT Networks	Attention-DNN + One-Class SVM	Improved network traffic representation	Heterogeneous traffic remains challenging
Yadav et al. [5]	Network Security	LSTM-KNN + PSO/CFS	Temporal modelling with feature selection	Limited assessment under imbalance
Mizanur et al. [6]	Cybersecurity	Decision Tree, RF, SVM	ML-based cyber threat detection analysis	Questionnaire-based evaluation
Goumidi and Pierre [7]	IoMT	RF-ANN-XGBoost stacking	Real-time healthcare anomaly detection	Limited cross-environment validation
Yuan et al. [8]	Industrial CPS	Conformal ML + ML/DL	False-alarm control under distribution shifts	Broader industrial validation required
Ahmad et al. [9]	IoT	QGAN / QML	Quantum-based anomaly detection framework	Limited practical quantum validation
Gawusu et al. [10]	Geochemical Data	CLR/ILR + Autoencoder	Compositional-aware anomaly detection	Small, region-specific dataset
Zhang et al. [11]	Protocol Security	GRU + Reconstruction + Contrastive Learning	Temporal protocol behaviour modelling	Limited cross-protocol validation
Li et al. [12]	Industrial Time Series	CKDGAT + Reconstruction	Variable interaction and temporal modelling	Only two industrial testbeds
Wang et al. [13]	Satellite Networks	CvT-LSTM + FL + GA	Spatial-temporal and privacy-aware detection	Limited heterogeneous-environment validation
Abdelhady et al. [14]	LoRaWAN	LightGBM + Autoencoder	Hybrid detection with lightweight security	Energy overhead and limited validation
Lachure and Doriya [15]	Industrial Control Systems	Hierarchical Clustering + DL	Hybrid industrial sensor analysis	Dataset-dependent performance

Table 1. Comparison of representative ML and DL approaches for anomaly detection

3. ML and DL Approaches for Anomaly Detection

The research works presented in the previous section showed that machine learning and deep learning are utilized in a wide variety of application fields for the detection of abnormal patterns. These methods, however, vary greatly in the way they represent normal behavior, how they measure deviations and what they consider an anomalous observation.

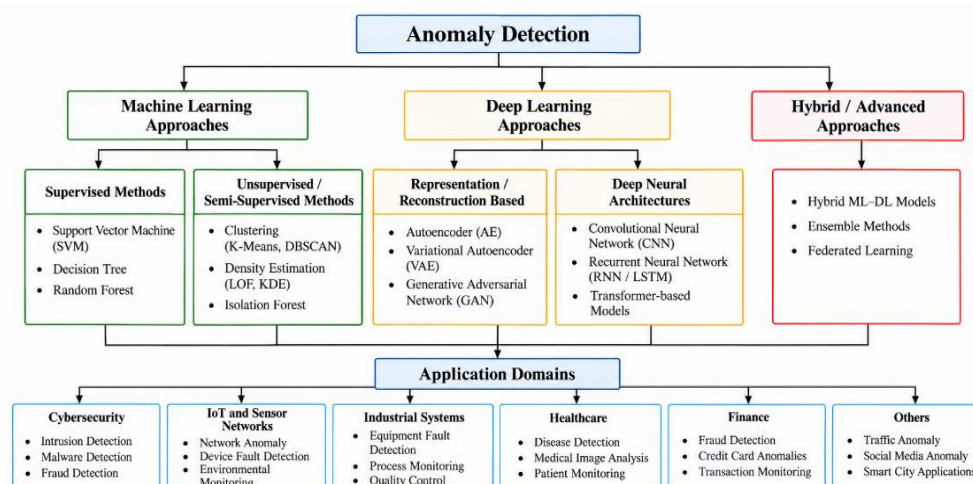


Fig. 2. Taxonomy of ML and DL approaches for anomaly detection.

Machine Learning and Deep Learning Approaches for Anomaly Detection: A Review

The simple taxonomy of machine learning and deep learning approaches for anomaly detection is shown in Figure 2. It classifies major methods into traditional ML, deep learning, and hybrid/advanced ML methods that were reviewed in the literature. This section therefore gives a brief overview of the main ML and DL approaches along with their mathematical formulations focusing on anomaly scoring, reconstruction, classification and threshold-based detection.

3.1 Machine Learning-Based Approaches

Traditional machine learning algorithms identify anomalies by looking for distances, statistical relationships, densities, or decision boundaries in the data. K-Nearest Neighbour (KNN) measures abnormality based on the distance between an observation and its K closest neighbours in a dataset $X = \{x_1, x_2, \dots, x_n\}$, where $x_i \in \mathbb{R}^d$. The distance-based score that is widely used is:

$$S_{KNN}(x_i) = \frac{1}{k} \sum_{j=1}^k d(x_i, x_j). \quad (1)$$

A higher number means that the observation is further from its local neighbourhood and so the observation may be an anomaly. Support Vector Machine (SVM), in the particular case of One-Class SVM, learns a boundary around the normal observations. Its decision function is:

$$f(x) = \text{sign}(w^T \phi(x) - \rho), \quad (2)$$

where $\phi(x)$ encodes the input into a feature space, w determines the separation boundary, and ρ determines the position of the separation boundary. Tree-based techniques like Decision Trees and Random Forests detect abnormal patterns by using hierarchical decision rules. Clustering-based detection can also assign higher anomaly score to observations which are not near the cluster centres. The distance corresponding to a cluster centre c is given by

$$S_c(x_i) = \|x_i - c\|_2. \quad (3)$$

Although these methods are relatively simple and interpretable, high-dimensional features, complex nonlinear relationships, and varying data distributions can impact their performance.

3.2 Deep Learning-Based Approaches

Deep learning techniques learn the nonlinear representations directly from the input data and hence are appropriate for complex high-dimensional and sequential anomaly detection tasks. One of the most popular unsupervised methods is the autoencoder. The encoder maps an input x to a latent representation,

$$z = f_\theta(x), \quad (4)$$

while the decoder reconstructs the original input from the learned representation. The reconstruction is given by

$$\hat{x} = g_\phi(z) = g_\phi(f_\theta(x)). \quad (5)$$

The difference between x and $\hat{x}$ is a measure of abnormality. CNNs learn local spatial patterns, LSTMs and RNNs are suitable for sequential and temporal dependencies. In an LSTM-based model, the hidden representation is usually denoted as

$$h_t = \text{LSTM}(x_t, h_{t-1}), \quad (6)$$

where x_t denotes the input at time t and h_{t-1} denotes the previous hidden state. Further, transformer-based models also enable the modeling of relationships between elements in a sequence using attention mechanisms. The DL approaches can sometimes learn more complex patterns which might be hard to represent by conventional distance-based and/or rule-based approaches, but they typically demand more computation power and meticulous training.

3.3 Mathematical Formulation and Detection Strategy

The mathematical expression of anomaly detection is related to the representation of the normal behavior and the measure of the deviation from the normal behavior. Typically, an anomaly detection model is a model that learns a function from an input observation to a numerical score that quantifies how abnormal the observation is. For reconstruction-based approaches, the anomaly score can be expressed as

$$S(x) = L(x, \hat{x}) = L(x, f_\theta(x)). \quad (7)$$

where x represents an observation from input, $\hat{x}$ is the reconstructed observation, and L is the chosen loss function. The mean squared reconstruction error can be expressed for a d -dimensional input as

$$S_{\text{MSE}}(x) = \frac{1}{d} \sum_{j=1}^d (x_j - \hat{x}_j)^2. \quad (8)$$

The more the observation is farther away from the learned patterns, the larger the reconstruction error will be, thus making it more probable that the observation is anomalous. In the case of distance-based methods the anomaly score may alternatively be expressed as distance from an observation to its reference or neighbourhood:

$$S_{\text{dist}}(x) = d(x, c), \quad (9)$$

where c denotes a reference point, as an instance a cluster centre or learned normal representation. The final anomaly status is obtained by comparing the score obtained to a threshold τ :

$$A(x) = \begin{cases} 1, & S(x) > \tau, \\ 0, & S(x) \leq \tau, \end{cases} \quad (10)$$

where $A(x) = 1$ represents an anomalous observation and $A(x) = 0$ represents normal behaviour. Alternatively, the decision in supervised anomaly detection can be made based on the predicted probability of the anomalous class:

$$\hat{y} = \begin{cases} 1, & P(y = 1 | x) > \tau, \\ 0, & P(y = 1 | x) \leq \tau. \end{cases} \quad (11)$$

While there are differences between ML and DL methods in terms of representation and learning mechanisms, the detection process can often be summarized as estimating the scores and setting a decision threshold. The threshold is especially critical in unbalanced anomaly detection as a wrong value can cause false alarms or missed alarms.

4. Comparative Analysis and Challenges

Based on the mathematical formulations introduced in Section 3, anomaly detection can be realised by employing various learning mechanisms such as distance-based, decision-boundary or reconstruction and representation learning. However, their practical usability hinges on the characteristics of the data, computational needs, interpretability, and adaptability to varying circumstances. The major differences between conventional ML and DL approaches are summarised in Table 2.

Aspect	Machine Learning	Deep Learning
Feature extraction	Often requires engineered features	Learns features automatically
Data requirement	Low to moderate	Generally higher
Nonlinear modelling	Moderate	Strong
Temporal modelling	Limited	Strong with LSTM/Transformer
Computational cost	Relatively low	Generally high
Interpretability	Usually higher	Often more difficult
Training complexity	Lower	Higher
Typical methods	KNN, SVM, RF, Clustering	AE, CNN, LSTM, Transformer

Table 2. Comparative characteristics of ML and DL approaches for anomaly detection

Despite their relative simplicity of decision-making processes and lower computation demands, ML methods are still useful for structured datasets. On the contrary, the DL methods are more suited for high dimensional and sequential data where nonlinear representations can be learned without a lot of manual feature engineering. However, challenges in the training of DL models, interpretability, computational cost, reliable deployment also arise with the increased complexity.

4.1 Challenges in Anomaly Detection

While significant advances have been made, there remain a number of issues related to the reliability of anomaly detection systems. The problem of class imbalance is still prevalent since the number of anomalous observations is usually much smaller than the number of normal observations and therefore can affect the learning process and make the accuracy a poor indicator of the results. Supervised learning is also limited by the small number of anomalies available with labels. When the behaviour of the system changes over time, then distribution shifts and concept drift can further decrease the detection performance. These high-dimensional and heterogeneous datasets can lead to redundant features and to a higher computational requirement. Another issue is false positives and in the security and industrial applications, a high number of false alarms can diminish the usefulness of the operation. Also, determination of an adequate threshold is challenging due to the direct correlation between threshold and false alarm and missed anomaly rates. Cross-domain validation is also a key challenge that needs to be overcome for real-world deployment, and other challenges such as model interpretability, privacy and resource constraints also exist to a certain extent.

5. Conclusion

Anomaly Detection is a crucial component in the detection of abnormal behaviour in cybersecurity, IoT, industrial systems, healthcare, and many other data driven applications. The primary machine learning and deep learning techniques such as KNN, SVM, clustering, tree-based models, Autoencoders, CNNs, LSTM networks, and Transformer-based models were explored. The reviewed studies demonstrate that the traditional ML methods are still applicable to structured data and with reduced computation cost, while the DL methods are able to learn more complex nonlinear and temporal patterns. Another set of mathematical formulations shows how anomaly scores can be achieved using distance measures, reconstruction errors, and classification probabilities coupled with thresholding. Nevertheless, practical deployment issues such as class imbalance, limited labelled data, distribution shifts, false positives, computational requirements and crossdomain generalisation are important challenges. Future work should be directed towards adaptive, explainable, and uncertainty-aware models that learn under varying and incomplete data scenarios. Scalable and reliable anomaly detection in real-world settings can also be achieved by lightweight edge learning, federated learning, and emerging hybrid architectures.

References

- [1] Baimukhanov, S., Ali, H., & Yazici, A. (2025). Enhancing ML-based anomaly detection in data management for security through integration of IoT, cloud, and edge computing. *Expert Systems with Applications*, 293, 128700.
- [2] Aslam, M. M., Tufail, A., De Silva, L. C., & Apong, R. A. A. H. M. (2025, August). Multi-Feature Hybrid Anomaly Detection in ICS: An Integration of ML, DL, and Statistical Techniques. In *Proceedings of the 3rd ACM Workshop on Secure and Trustworthy Deep Learning Systems* (pp. 43-51).
- [3] Narmadha, S., & Balaji, N. V. (2025). Improved network anomaly detection system using optimized autoencoder– LSTM. *Expert Systems with Applications*, 273, 126854.

Machine Learning and Deep Learning Approaches for Anomaly Detection: A Review

- [4] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Morales-Reyes, A. (2025). Network traffic inspection to enhance anomaly detection in the Internet of Things using attention-driven Deep Learning. *Integration*, 103, 102398.
- [5] Yadav, K. S., Kumbham, A. R., Vallurupalli, P., Mallreddy, S. R., & Mahendrakumar, G. (2025, August). A Deep Learning Framework for Network Anomaly Detection using KNN and LSTM Models. In *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 2110-2115). IEEE.
- [6] Mizanur, M., Kumer, S., & Reza, N. (2025). Machine learning-based anomaly detection for cyber threat prevention. *Journal of Primeasia*, 6(1), 1-8.
- [7] Goumidi, H., & Pierre, S. (2025). Real-time anomaly detection in IoMT networks using stacking model and a healthcare-specific dataset. *IEEE Access*, 13, 70352-70365.
- [8] Yuan, S., Li, J., Wang, C., & Zhang, X. (2026). Conformal machine learning for reliable anomaly detection in industrial cyber-physical systems. *Reliability Engineering & System Safety*, 112417.
- [9] Ahmad, I., Yang, L., Alkhrijah, Y., Almadhor, A., Alawad, M. A., Peng, L., & Ho, P. H. (2026). Quantum machine learning for anomaly detection: The future of smarter and safer IoT networks. *IEEE Network*.
- [10] Gawusu, S., Abu, M., & Mvile, B. N. (2026). Compositional data-aware deep learning for geochemical anomaly detection: A novel framework for mineral prospectivity mapping. *Physics and Chemistry of the Earth, Parts A/B/C*, 104352.
- [11] Zhang, C., Zhu, H., Zhu, A., Liao, J., Xiao, Y., & Zhang, Z. (2026, February). Deep learning approach for protocol anomaly detection using status code sequences. In *Proceedings of the 2026 International Conference on Generative Artificial Intelligence and Education* (pp. 10-15).
- [12] Li, Q., Ji, Y., Sun, L., Zhang, N., & Yang, T. (2026). Anomaly detection for industrial time series in process industry using informed machine learning with graph attention networks. *Computers in Industry*, 176, 104445.
- [13] Wang, Z., Cao, J., & Di, X. (2026). Anomaly detection method for satellite networks based on genetic optimization federated learning. *Expert Systems with Applications*, 295, 128627.
- [14] Abdelhady, G., Ghandoura, A., Motwakel, A., & Alajmi, A. (2026). Hybrid Machine Learning Anomaly Detection and Lightweight Zero Trust Authentication for LoRaWAN Networks. *IEEE Access*.
- [15] Lachure, J., & Doriya, R. (2026). Intelligent sensor data analysis through hybrid deep hierarchical clustering for anomaly detection. *Transactions of the Institute of Measurement and Control*, 48(6), 1205-1220.