10.16920/jeet/2026/v39is4/26121

Adaptive Threshold-Based Autoencoder Model for Enhancing Security through Anomaly Detection in E-Learning Environments

[1]Ramalakshmi K, [2]Santhrupth B C, [3]Supriya H S, [4]Padmini K, [5]Praveen Kumar R, [6*]Rakesh V S

[1,6]Department of Computer Science and Engineering, Cambridge Institute of Technology, Karnataka, India

[2]Department of AIML & DS, Christ University, Bengaluru, India

[3,5]Department of Computer Science and Engineering, Global Academy of Technology, Karnataka, India

[4]Department of Information Science and Engineering, Don Bosco Institute of Technology, Karnataka

[1]rama.cse@cambridge.edu.in, [2]santhrupth23@gmail.com, [3]supriyahonur.s@gmail.com, [4]padmini.roopesh@gmail.com, [5]praveenkumar.r@gat.ac.in, [6*]rakesh.tech102@gmail.com

***Abstract*—Securing the e-learning platforms has become increasingly difficult as user activities grow more complex and cyber threats become more advanced. Conventional detection techniques often fail to capture subtle irregularities in behavior, which can result in a higher number of false alarms and reduced accuracy. To overcome these limitations, this study adopts an autoencoder model enhanced with an adaptive threshold mechanism. The model first learns the pattern of normal user activity and then identifies unusual behavior by measuring reconstruction errors—where typical patterns are reconstructed accurately, while anomalies produce larger deviations. Unlike fixed thresholds, the adaptive approach adjusts dynamically based on the distribution of these errors, allowing for more precise detection. The experimental findings show strong performance, achieving 99.35% accuracy, 98.84% precision, 100% recall, and an F1-score of 99.41%, clearly surpassing traditional methods. Overall, the results suggest that this approach is highly effective for detecting anomalies and can significantly strengthen security in modern, data-driven e-learning environments.**

***Keywords* — Adaptive Thresholding; Anomaly Detection; Autoencoder; Digital Education Security; E-Learning Systems.**

***JEET Category* — Research**

I. INTRODUCTION

THE rapid expansion of digital learning platforms has transformed modern education by enabling flexible and remote access to knowledge. However, this expansion has also introduced significant security concerns due to increased user interaction, distributed access, and cloud-based integration. E-learning environments are vulnerable to unauthorized access, account misuse, and abnormal user behavior, which can threaten data integrity and system reliability. Traditional security mechanisms based on static rules or signature matching are often ineffective against evolving threats, underscoring the need for intelligent, adaptive anomaly detection in dynamic, user-driven systems (Zhang, 2025).

Intrusion detection is essential for maintaining security of large-scale digital environments. The increasing complexity and high-dimensional nature of user activity and network data require advanced techniques capable of capturing intricate patterns. Conventional Machine learning methods often face difficulties with nonlinear relationships and temporal dependencies. In comparison, deep learning models have demonstrated strong capability for learning meaningful representations from complex data, thereby improving the detection of anomalous behavior in real-time systems (Sajid, 2024). Among deep learning methods, autoencoders and sequence-based models are effective in detecting deviations from normal behavior without relying on predefined attack signatures. These models are capable of learning underlying patterns and complex relationships within the data and adapt to varying behavioral characteristics, leading to improved detection accuracy and reduced false alarms. Such adaptability is particularly relevant for e-learning platforms, where user behavior is diverse and continuously evolving (Ataa, 2024).

Despite these advancements, several challenges still persist in achieving consistent detection performance. Many existing approaches rely on static thresholding, which fails to adapt to changing data distributions and leads to inconsistent results. Adaptive thresholding techniques address this limitation by dynamically adjusting detection boundaries based on data characteristics, improving sensitivity and robustness. Integrating such mechanisms with Deep learning models provide an effective approach for anomaly detection in dynamic environments like e-learning systems (Chinnasamy, 2025).

The key contributions of this study can be summarized as follows:

1. An autoencoder-based model is used to learn normal behavior patterns and detect anomalies in user activity.
2. An adaptive thresholding method dynamically adjusts

detection limits, overcoming the limitations of fixed thresholds.

3. The approach improves detection performance and robustness, supporting enhanced security in e-learning environments.

The rest of the paper is structured as follows. Section II reviews the related work. Section III outlines the proposed methodology. Section IV presents the experimental setup along with the performance evaluation metrics. Section V provides a detailed discussion of the results and comparative analysis. Finally, Section VI concludes the study and highlights possible directions for future research.

II. Related Works

Recent progress in anomaly detection has focused on both machine learning and deep learning methods to recognize unusual patterns in complex and dynamic data settings, such as networked and user-centric systems. Within e-learning environments, these techniques play a crucial role in monitoring user behavior and strengthening security against continuously evolving threats.

A reconstruction-based learning approach has been applied to anomaly detection in cloud network environments by capturing normal traffic patterns and identifying anomalies via reconstruction errors. This error serves as an important measure for differentiating between normal and anomalous behavior, where feature-level analysis further enhances detection accuracy compared to baseline machine learning and deep learning methods (Torabi, 2023). In visual inspection domains, reconstruction-driven techniques have been extensively studied and applied to detect anomalies by learning standard patterns and identifying deviations. To overcome limitations of pixel-level comparisons, advanced methods integrate convolutional architectures with deep feature extraction and one-class classification, leading to improved detection performance across complex datasets, although challenges related to accuracy and adaptability remain (Saeedi, 2023). For sensor signal data, deep learning-based approaches using semi-supervised training on normal samples have shown effectiveness in anomaly detection. Techniques combining reconstruction error with statistical methods such as kernel density estimation enable adaptive thresholding, where integrated and simpler models typically deliver improved performance when sufficient normal data is available (Esmaeil, 2023).

Autoencoder-based unsupervised anomaly detection methods have been extensively studied for their ability to learn underlying data distributions and spot anomalous patterns. Variational and generative autoencoders enhance representation learning and reconstruction, thereby improving anomaly classification. Experimental analyses reveal trade-offs between model efficiency, reconstruction quality, and latent space representation, which affect overall detection performance (Neloy, 2024). An intrusion detection approach integrating deep autoencoder models incorporating various optimization techniques has been introduced to improve performance in complex network environments. By combining effective feature extraction with advanced optimization strategies, the method improves learning efficiency and mitigates the problem of local minima during training. Experimental evaluations on benchmark datasets indicate achieving higher detection accuracy and reduced false alarm rates compared to traditional neural network-based approaches (Hacılar, 2024). An anomaly detection approach has been implemented to network traffic data by learning normal behavior patterns and identifying deviations through reconstruction errors. The method utilizes the UNSW-NB15 dataset and highlights the importance of proper data preprocessing, feature selection, and model configuration for effective detection. Experimental findings demonstrate that the approach is robust and practical, capable of detecting malicious activities and adapting to varying traffic patterns (Bashurov, 2024).

A convolutional neural network-based approach has been utilized for anomaly detection using the UNSW-NB15 dataset, with feature selection techniques employed to reduce data complexity. By using methods such as random forests to select significant features, the model improves efficiency and focuses on relevant patterns. Experimental results demonstrate high detection performance, indicating the effectiveness of deep learning models for real-time network anomaly detection (Vibhute, 2024).

A hybrid feature selection method that combines filter and wrapper methods has been proposed to improve anomaly detection performance on the UNSW-NB15 dataset. By integrating techniques such as information gain, random forest, and recursive feature elimination, the method efficiently reduces the number of features while preserving the most important and relevant information. The experimental results indicate that optimized feature selection enhances classification accuracy and overall detection performance compared to conventional methods (Yin, 2023). A hybrid deep learning approach combining generative and discriminative models has been proposed to address class imbalance in intrusion detection systems. By integrating Conditional GANs with CNN classifiers, synthetic attack samples are generated to improve the detection of rare anomalies and enhance model performance. Experimental results on the UNSW-NB15 dataset demonstrate high accuracy and reduced false alarm rates, outperforming several baseline models (Fathima, 2023).

TABLE I
SUMMARY OF RELATED WORKS

Ref	Method Used	Dataset	Key Idea	Limitation
Torab, 2023	Reconstruction-based model	Cloud dataset	Detects anomalies using reconstruction error	Uses fixed/global threshold
Saeed, 2023	CNN + Feature extraction + One-class classification	Image datasets	Improves detection via deep feature learning	Limited adaptability to different domains

Esmaeil, 2023	Autoencoder + KDE	Sensor data	Adaptive threshold using statistical methods	Depends on sufficient normal data
Neloy, 2024	Variational / Generative Autoencoders	MNIST / FMNIST	Learns latent representations for anomaly detection	Trade-off between efficiency and accuracy
Hacılar, 2024	Deep Autoencoder + Optimization	UNSW-NB15	Improves detection using optimization techniques	High computational complexity
Bashurov, 2024	Reconstruction-based anomaly detection	UNSW-NB15	Uses reconstruction error for detecting anomalies	Manual threshold selection
Vibhute, 2024	CNN + Random Forest	UNSW-NB15	Feature selection + deep learning for detection	No adaptive threshold mechanism
Yin, 2023	Hybrid Feature Selection (IG + RF + RFE)	UNSW-NB15	Reduces feature space and improves classification	Moderate improvement in accuracy
Fathima, 2023	CGAN + CNN	UNSW-NB15	Handles class imbalance using synthetic data	Increased model complexity

However, many existing approaches lack adaptability because they rely on fixed thresholds, which can lead to inconsistent detection performance. To fix this issue, the proposed work introduces an adaptive threshold-based autoencoder for more dependable and adaptable anomaly detection.

III. Methodology

The proposed method learns normal behavior patterns and identifies deviations using reconstruction errors. In contrast to traditional approaches that depend on fixed thresholds, the system dynamically adjusts detection limits based on the underlying data distribution, improving accuracy and robustness. The overall workflow, shown in Fig. 1, begins with preprocessing input data obtained from a benchmark dataset that provides representative network traffic patterns for anomaly identification. Although the dataset is not specific to e-learning environments, it effectively captures network-level behaviors relevant to digital learning systems.

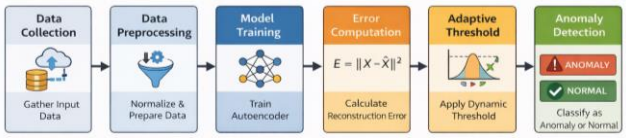

Fig. 1. Workflow of Proposed Technique

After preprocessing, the data is fed into an autoencoder that learns to replicate normal patterns. The reconstruction error, representing the difference between the input and the reconstructed output, is used to detect anomalies. An adaptive threshold is derived from the distribution of these errors, and data instances are classified as normal or anomalous based on whether their error values exceed the threshold.

A. Data Preprocessing

The dataset used in this study is first cleaned and prepared to ensure consistency and quality. Unnecessary features are removed, and missing values are properly addressed. Categorical features are transformed into numerical representations, and all features are normalized to a common scale to avoid bias during training. The model was primarily trained on normal data instances.

B. Autoencoder Model Design

An autoencoder is utilized to learn the typical patterns within the dataset. It works by first encoding the input data into a compressed, lower-dimensional form and then decoding it to reconstruct the original input. During training, the model focuses on minimizing the difference between the input and its reconstructed version. Through this process, it effectively captures the inherent structure and characteristics of normal data, making it easier to identify deviations later.

C. Reconstruction Error Computation

The reconstruction error reflects how accurately the model is able to reproduce the input data. It is calculated as shown in (1).

$$E = \left\| X - \hat{X} \right\|^2 \tag{1}$$

where X represents the original input, and $\hat{X}$ denotes the reconstructed output. Lower error values indicate normal behavior, while higher values suggest anomalies.

D. Adaptive Threshold Mechanism

To identify anomalies, an adaptive threshold is calculated based on the distribution of reconstruction errors. Eq. (2) determines the adaptive threshold.

$$T = \mu + k\sigma \tag{2}$$

where μ and σ represent the average value and the standard deviation of the errors, respectively, and k is a scaling parameter. This allows dynamic adjustment of the decision boundary for improved detection.

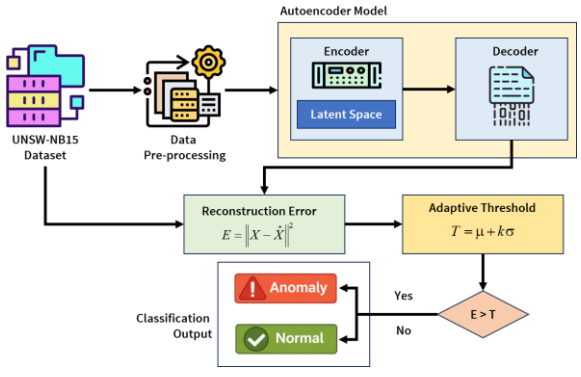

Fig. 2. Architecture of Proposed System

The structure of the proposed system is shown in Fig. 2, highlighting interactions among its components. The autoencoder forms the core of the model, with the encoder and decoder working together to learn compact representations and

reconstruct input data. The reconstruction error module serves as a bridge between the learning component and the decision mechanism, providing a quantitative measure of deviation. This error is then used by the adaptive threshold unit, which dynamically determines the decision boundary. The complete system architecture integrates learning and decision-making modules, enabling effective identification of anomalous patterns. In addition to the proposed approach, classical machine learning models such as Support Vector Machine (SVM), Random Forest (RF), k-Nearest Neighbors (kNN), and Logistic Regression (LR) are considered for comparative evaluation.

IV. Experimental Setup

This section outlines the experimental setup employed to assess the performance of the proposed anomaly detection model.

A. Dataset Description

The experiments conducted in this study utilize the UNSW-NB15 dataset, a well-known benchmark in intrusion detection research. This dataset includes network traffic data that represents both normal behavior and various types of anomalous activities, including various types of cyber-attacks. The dataset includes a diverse set of features, such as flow-based, statistical, and protocol-related attributes, that effectively represent network behavior. It is chosen due to its relevance and suitability for evaluating anomaly detection models. Although the dataset is not specific to e-learning environments, it provides realistic network-level patterns applicable to modeling security scenarios in digital learning systems.

Fig. 3 shows the distribution of normal and major attack categories in the UNSW-NB15 dataset. Normal traffic accounts for the largest share, followed by prominent attack types such as Generic and Exploits. Less frequent attack categories are grouped under 'others' to improve visualization clarity, highlighting the inherent class imbalance in the dataset.

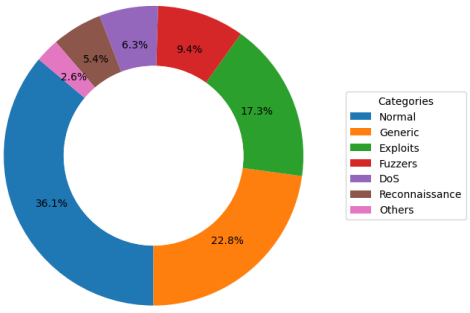

Fig. 3. Distribution of Normal and Attack Categories in UNSW-NB15 Dataset

B. Data Preparation

The UNSW-NB15 dataset is preprocessed to ensure consistency and suitability for anomaly detection. To allow the autoencoder to effectively learn patterns of normal behavior, it is trained mainly using normal data samples. During evaluation, the test set includes both normal and anomalous instances to assess the model's detection capability. Categorical attributes are converted into numerical form, and all features are normalized using min-max scaling to a range of 0 to 1 to ensure consistent feature representation and improve training stability.

C. Model Configuration

The proposed model is built using an autoencoder architecture designed to learn patterns of normal data. The encoder reduces the input into a compact, lower-dimensional representation, while the decoder reconstructs it back to its original form. The model is trained using the Adam optimizer with mean squared error as the loss function. Key training parameters are presented in Table I. Furthermore, for comparative analysis, previously discussed traditional machine learning models are also applied to the same preprocessed dataset.

TABLE II
Model Configuration Parameters

Parameter	Value
Input Dimension	42
Latent Dimension	16
Activation Function	ReLU
Optimizer	Adam
Loss Function	Mean Squared Error
Batch Size	32
Epochs	50
Parameter	Value
Input Dimension	42

D. Data Preprocessing

To classify instances based on reconstruction error, both fixed- and adaptive-thresholding approaches are considered. For the fixed threshold method, a constant value is selected based on the reconstruction error distribution observed during training. In this study, the threshold is set to 0.01, as it effectively distinguishes between normal and anomalous instances. To improve detection performance, an adaptive threshold is computed from the statistical properties of reconstruction errors in the training data, as defined in Eq. (2).

The scaling parameter $k$is set to 3, allowing the threshold to adjust dynamically based on the mean and standard deviation of the error distribution. During testing, each instance is evaluated by comparing its reconstruction error with the corresponding threshold. If the error exceeds the threshold, it is classified as an anomaly; otherwise, it is considered normal. The adaptive threshold approach provides more robust and reliable detection compared to the fixed threshold method

E. Evaluation Metrics

The performance of the proposed model is evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. Accuracy measures overall correctness, while precision indicates the proportion of detected anomalies that are actually anomalous. Recall reflects the model's ability to identify actual anomalous instances, and the F1-score provides a balanced measure by combining precision and recall. In addition, the false-positive rate is used to assess the model's ability to minimize incorrect anomaly detections. These metrics collectively provide a comprehensive evaluation of the model's effectiveness and enable comparison with both fixed threshold methods and classical machine learning models.

V. Result and Discussion

This section evaluates the proposed approach and compares it with fixed-threshold methods and traditional machine learning models. The results demonstrate the effectiveness of the adaptive threshold mechanism in improving anomaly detection accuracy and robustness. Table II presents the comparative performance of the proposed model under the same experimental setup.

TABLE III
Performance Comparison of Anomaly Detection Methods for E-Learning Systems

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FPR (%)
Logistic Regression	92.4	90.5	91.8	91.1	7.6
kNN	94.6	92.9	93.5	93.2	5.9
SVM	95.3	94.1	94.6	94.35	5.2
Random Forest	97.6	96.5	97.1	96.8	3.1
Autoencoder (Fixed Threshold)	98.2	97.4	97.9	97.65	2.5
Proposed (Adaptive Threshold)	99.3	98.8	100	99.4	1.2

The proposed approach achieves the highest performance across all evaluation metrics. In particular, the model achieves perfect recall, indicating that it detects all anomalous instances. Compared with the fixed-threshold approach, the adaptive method shows improved precision and a significantly lower false-positive rate, demonstrating greater robustness and reliability. Furthermore, the proposed model outperforms classical machine learning models such as SVM, kNN, Random Forest, and Logistic Regression, highlighting the effectiveness of combining reconstruction-based learning with adaptive thresholding.

The Receiver Operating Characteristic (ROC) curve is used to evaluate how well different models distinguish between normal and anomalous instances. The area under the curve (AUC) quantifies classification effectiveness. Fig. 4 shows the ROC curves for all models considered in this study.

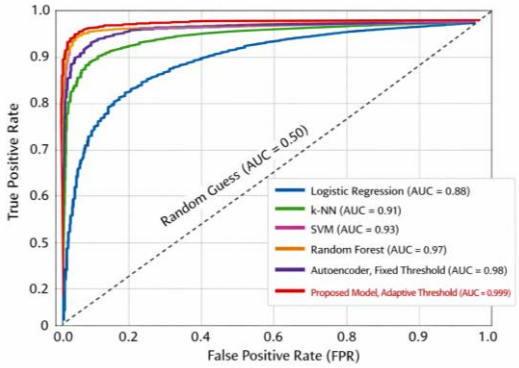

Fig. 4. ROC Curve Comparison of Anomaly Detection Methods

Fig. 5 shows the confusion matrices of all models, providing a detailed view of classification performance. Consistent with the ROC results, the proposed adaptive threshold model achieves the highest accuracy with minimal false positives and no false negatives, indicating reliable anomaly detection. Other models exhibit higher misclassification rates, confirming the effectiveness of the proposed approach.

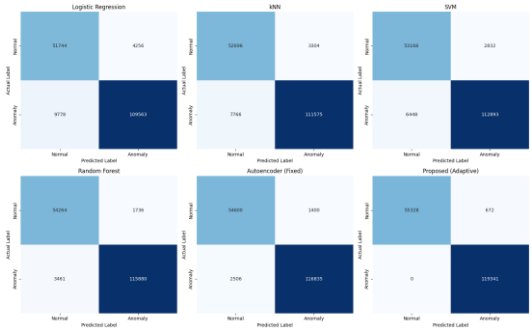

Fig. 5. Confusion Matrix Comparison of Anomaly Detection Models

To better understand the behavior of the proposed model, the distribution of reconstruction errors is analyzed for normal and anomalous instances. This helps visualize the separation between the two classes and justifies the use of threshold-based detection. Fig. 6 shows the distribution of reconstruction errors for normal and anomalous instances. It is evident that normal data produces lower error values, while anomalies result in significantly higher errors, creating a clear separation between the two. The adaptive threshold lies between these distributions, enabling accurate identification of anomalous behavior.

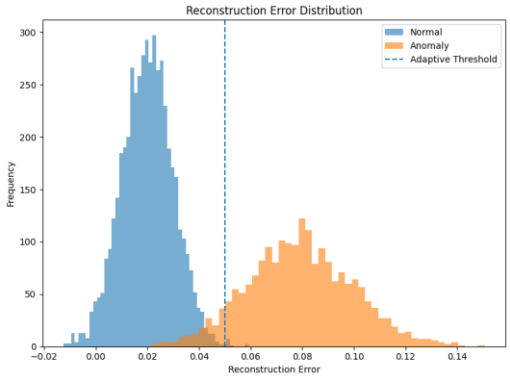

Fig. 6. Reconstruction Error Distribution for Normal and Anomalous Data

In addition to the distribution analysis, a threshold-based visualization is presented to further illustrate how anomalies are identified. Fig. 7 shows the sorted reconstruction error across all instances along with the adaptive threshold. It can be observed that most normal instances lie below the threshold, while anomalous instances exceed it, resulting in a clear separation. This demonstrates the effectiveness of the proposed adaptive threshold in accurately distinguishing abnormal behavior.

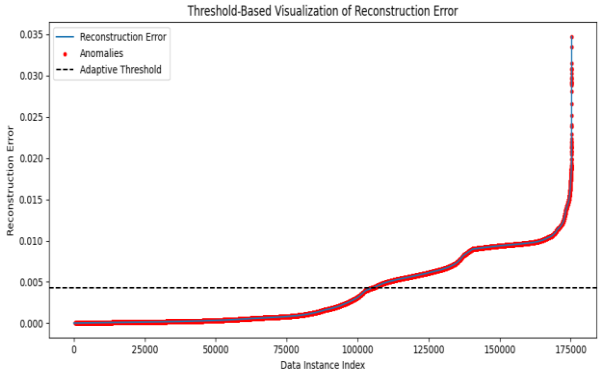

Fig. 7. Sorted Reconstruction Error with Adaptive Threshold

To provide a clear comparative analysis, the performance of all models is evaluated across key metrics as shown in Fig. 8. This visualization highlights the effectiveness of the proposed approach relative to existing methods.

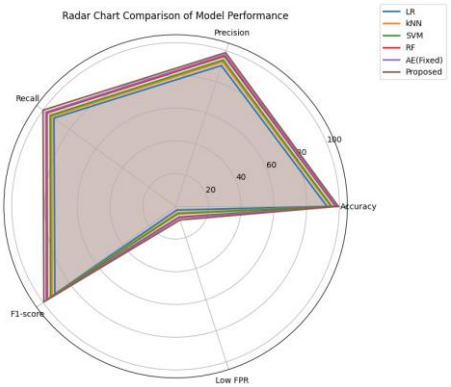

Fig. 8. Performance Comparison of Different Models

The proposed approach consistently achieves superior results, maintaining higher accuracy, precision, recall, and F1-score while simultaneously reducing the false-positive rate. This balanced improvement across all metrics highlights its ability to detect anomalies with greater reliability than existing methods.

Conclusion and Future Scope

This study presents an adaptive, threshold-based autoencoder approach for anomaly detection, with a focus on enhancing security in e-learning environments. By learning normal behavior patterns and dynamically adjusting the detection threshold based on reconstruction error, the method effectively distinguishes between legitimate user activity and potential threats. Experimental results on the UNSW-NB15 dataset demonstrate improved performance over classical machine learning models and fixed-threshold techniques, indicating its capability to handle complex and imbalanced data. In the context of e-learning systems, this approach can help identify abnormal access patterns, safeguard user data, and ensure a secure learning experience. Future work can explore real-time implementation in live e-learning platforms, integration with more advanced deep learning architectures, and evaluation on domain-specific datasets to further enhance its practical applicability and scalability.

References

Ataa, M. S., Sanad, E. E., & El-Khoribi, R. A. (2024). Intrusion detection in software defined network using deep learning approaches. *Scientific Reports*, *14*(1), 29159. https://doi.org/10.1038/s41598-024-79001-1

Bashurov, V., & Safonov, P. (2024). Machine Learning Using Autoencoder Method: An Application to Detecting Anomalies in Internet Traffic. (2024). *Issues in Information Systems*, *25(4)*,277. https://doi.org/10.48009/4_iis_2024_122

Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). Deep learning-driven methods for network-based intrusion detection systems: A systematic review. *ICT Express*, *11*(1), 181–215. https://doi.org/10.1016/j.icte.2025.01.005

Esmaeili, F., Cassie, E., Nguyen, H. P. T., Plank, N. O. V., Unsworth, C. P., & Wang, A. (2023). Anomaly detection for sensor signals utilizing deep learning Autoencoder-Based neural networks. *Bioengineering*, *10*(4), 405. https://doi.org/10.3390/bioengineering10040405.

Hacılar, H., Dedeturk, B. K., Bakir-Gungor, B., & Gungor, V. C. (2024). Network anomaly detection using Deep Autoencoder and parallel Artificial Bee Colony algorithm-trained neural network. *PeerJ Computer Science*, *10*, e2333. https://doi.org/10.7717/peerj-cs.2333

Fathima, A., Khan, A., Uddin, M. F., Waris, M. M., Ahmad, S., Sanin, C., & Szczerbicki, E. (2023). Performance evaluation and comparative analysis of machine learning models on the UNSW-NB15 Dataset: A Contemporary Approach to Cyber Threat Detection. *Cybernetics & Systems*, *56*(8), 1160–1176. https://doi.org/10.1080/01969722.2023.2296246

Neloy, A. A., & Turgeon, M. (2024). A comprehensive study of auto-encoders for anomaly detection: Efficiency and trade-offs. *Machine Learning With Applications*, *17*, 100572. https://doi.org/10.1016/j.mlwa.2024.100572

Saeedi, J., & Giusti, A. (2023). Semi-supervised visual anomaly detection based on convolutional autoencoder and transfer learning. *Machine Learning With Applications*, *11*, 100451. https://doi.org/10.1016/j.mlwa.2023.100451

Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing Advances Systems and Applications*, *13*(1). https://doi.org/10.1186/s13677-024-00685-x

Torabi, H., Mirtaheri, S. L., & Greco, S. (2023). Practical autoencoder based anomaly detection by using vector reconstruction error. *Cybersecurity*, *6*(1). https://doi.org/10.1186/s42400-022-00134-9

Vibhute, A. D., Khan, M., Patil, C. H., Gaikwad, S. V., Mane, A. V., & Patel, K. K. (2024). Network anomaly detection and performance evaluation of Convolutional Neural Networks on UNSW-NB15

dataset. *Procedia Computer Science*, *235*, 2227–2236. https://doi.org/10.1016/j.procs.2024.04.211.

Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F., & Kwak, J. (2023). IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. *Journal of Big Data*, *10*(1). https://doi.org/10.1186/s40537-023-00694-8.

Zhang, Y., Muniyandi, R. C., & Qamar, F. (2025). A review of Deep Learning Applications in Intrusion Detection Systems: Overcoming challenges in spatiotemporal feature extraction and data Imbalance. *Applied Sciences*, *15*(3), 1552. https://doi.org/10.3390/app15031552