ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

An Enhanced Deep Learning Framework for Network Intrusion Detection Using Deep Autoencoders

N. SRINIVASARAO 1, Department Of CSE, Priyadarshini Institute Of Technology & Science For Women, India.

Y. Harini 2, Assistant Professor , Department Of CSE , Priyadarshini Institute Of Technology & Science For Women, India

Abstract: The rapid evolution of cyber threats has significantly increased the demand for intelligent and adaptive Intrusion Detection Systems (IDS) capable of protecting modern computer networks from sophisticated attacks. Traditional signature-based intrusion detection techniques are limited in identifying unknown attacks, zero-day exploits, and evolving malicious behaviors, making anomaly-based detection an essential cybersecurity solution. This project proposes a Deep Autoencoder-Based Intrusion Detection System (DAIDS) that utilizes unsupervised deep learning to model normal network traffic and detect anomalous activities through reconstruction error analysis. The proposed framework incorporates comprehensive data preprocessing, including data cleaning, feature encoding, normalization, and feature selection, followed by training a deep autoencoder to learn compact and meaningful representations of legitimate network traffic. The system is evaluated using the NSL-KDD and CICIDS2017 benchmark datasets, which contain diverse categories of network attacks and normal traffic patterns. Experimental evaluation demonstrates that the proposed model effectively distinguishes malicious traffic from legitimate network activities while maintaining a low false-positive rate. Performance is assessed using Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix analysis, achieving an overall detection accuracy of approximately 98.2% with high precision and recall. The deep autoencoder successfully captures complex nonlinear relationships within network traffic, enabling robust detection of both known and previously unseen cyber threats. The proposed framework offers improved scalability, efficient feature learning, reduced dependence on manual feature engineering, and enhanced adaptability to dynamic network environments. These results indicate that deep autoencoder-based anomaly detection provides a reliable, efficient, and scalable solution for strengthening network security and developing next-generation intelligent intrusion detection systems.

Keywords— Intrusion Detection System (IDS), Deep Autoencoder, Network Security, Anomaly Detection, Deep Learning, Cybersecurity, NSL-KDD, CICIDS2017, Feature Learning, Network Traffic Analysis.

1. INTRODUCTION

The rapid expansion of digital communication technologies, cloud computing, Internet of Things (IoT) devices, and enterprise networking has significantly increased the complexity and scale of modern computer networks. As organizations increasingly rely on interconnected systems to store, process, and exchange sensitive information, cybersecurity has become a critical concern. Cyberattacks such as Distributed Denial of Service (DDoS), ransomware, phishing, botnets, malware, privilege escalation, and zero-day attacks continue to evolve in sophistication, posing severe threats to the confidentiality, integrity, and availability of network resources. Consequently, organizations require intelligent and adaptive security mechanisms capable

of detecting and mitigating both known and previously unseen attacks.

Intrusion Detection Systems (IDS) play a vital role in safeguarding computer networks by continuously monitoring network traffic and identifying suspicious or malicious activities. Traditional IDS techniques are broadly classified into signature-based and anomaly-based systems. Signature-based IDS rely on predefined attack signatures to identify malicious behavior, making them highly effective against known threats. However, they are unable to detect novel or zero-day attacks that do not match existing signatures. In contrast, anomaly-based IDS establish a model of normal network behavior and identify deviations from this baseline, enabling the detection of previously unknown cyber threats. Despite their advantages, conventional anomaly detection approaches often suffer from high false alarm rates and limited capability in processing high-dimensional network traffic.

Recent advances in Artificial Intelligence (AI) and Deep Learning (DL) have transformed the field of network security by enabling automatic feature extraction and intelligent pattern recognition. Unlike conventional machine learning techniques that require extensive manual feature engineering, deep learning models automatically learn hierarchical feature representations from raw network traffic data. This capability significantly improves the detection of complex attack patterns while reducing the dependence on domain-specific expertise. Among various deep learning architectures, Deep Autoencoders have emerged as an effective unsupervised learning technique for anomaly detection due to their ability to compress high-dimensional data into compact latent representations and accurately reconstruct normal network traffic patterns.

A Deep Autoencoder consists of multiple encoding and decoding layers that learn meaningful feature representations of legitimate network behavior. During the training process, the model minimizes the reconstruction error between the original input and its reconstructed output, thereby learning the intrinsic characteristics of normal network traffic. When abnormal or malicious traffic is presented to the trained model, the reconstruction error increases significantly, allowing the system to effectively identify anomalies that may correspond to cyberattacks. This reconstruction-based learning mechanism makes deep autoencoders particularly suitable for detecting both known and unknown intrusions in dynamic network environments.

The proposed Deep Autoencoder-Based Intrusion Detection System (DAIDS) aims to enhance network security by leveraging unsupervised deep learning for intelligent anomaly detection. The framework incorporates data preprocessing techniques such as data cleaning, feature encoding, normalization, and feature selection before training the deep autoencoder model. The proposed system is evaluated using the widely recognized NSL-KDD and CICIDS2017 benchmark datasets, which contain diverse categories of normal and malicious network traffic. These datasets provide realistic attack scenarios, including Denial of Service (DoS), Probe, User-to-Root (U2R), Remote-to-Local (R2L), Distributed Denial of Service (DDoS), brute-force attacks, botnets, web attacks, and infiltration attacks.

To assess the effectiveness of the proposed model, multiple performance metrics including Accuracy, Precision, Recall, F1-Score, Receiver Operating Characteristic (ROC), Area Under the Curve (AUC), and Confusion Matrix analysis are employed. Experimental results demonstrate that the Deep Autoencoder-Based Intrusion Detection System achieves high detection accuracy while maintaining low false-positive rates and strong generalization capability across different attack categories. The automatic feature learning capability of the deep autoencoder enables the system to effectively model complex nonlinear relationships in network traffic without requiring manual feature extraction.

The proposed framework offers several advantages over conventional intrusion detection methods, including improved anomaly detection capability, enhanced scalability, efficient processing of large-scale network traffic, reduced computational complexity through latent feature learning, and adaptability to evolving cyber threats. By combining deep representation learning with intelligent anomaly detection, the proposed system contributes to the

development of next-generation cybersecurity solutions capable of providing reliable and real-time protection for modern computer networks.

Overall, this research demonstrates that deep autoencoder-based intrusion detection provides a robust, scalable, and efficient approach for enhancing network security. The proposed system not only improves intrusion detection performance but also offers significant potential for deployment in enterprise networks, cloud computing environments, Industrial Control Systems (ICS), Cyber-Physical Systems (CPS), Software-Defined Networks (SDN), and Internet of Things (IoT) infrastructures, where intelligent and adaptive cybersecurity mechanisms are increasingly essential.

2. LITERATURE SURVEY

Signature-based intrusion detection systems can detect known assaults, but not zero-day attacks or previously undetected hostile activity. Thus, researchers are using machine learning and deep learning to create intelligent anomaly-based intrusion detection systems that can better detect abnormal network behavior [1], [2].

Deep learning can automatically learn hierarchical feature representations from high-dimensional network traffic data. Deep autoencoders are popular deep learning architectures because they reduce data dimensionality and learn features unsupervised. Reconstructing regular network traffic and quantifying reconstruction errors helps deep autoencoders discern genuine traffic from aberrant behavior, enhancing intrusion detection [3], [4].

Several academics have suggested hybrid intrusion detection models using deep autoencoders and powerful machine learning methods. Using LightGBM, gradient boosting, and ensemble learning with deep feature extraction has improved classification accuracy and reduced computing complexity. These hybrid systems have efficiently detected known and unexpected cyberattacks on benchmark intrusion detection datasets [5], [6].

Generative deep learning methods have been studied to overcome intrusion detection dataset class imbalance. Autoencoder-based Generative Adversarial Networks (AE-GAN) and Conditional GANs (CGAN) generate representative minority-class samples to improve rare attack category detection and classifier resilience [7], [8].

Deep learning for intrusion detection has expanded beyond enterprise networks into SDN, ICS, CPS, cloud computing, and IoT environments. They show that deep neural networks can learn complicated communication patterns across different network architectures, improving security and attack detection [9]–[11].

Unsupervised learning is becoming more popular since it reduces labeled dataset dependence. The reconstruction error of deep, layered, and variational autoencoders has been used to mimic typical network activity and discover anomalies. These methods are successful at detecting zero-day attacks and sophisticated intrusion patterns that signature-based methods cannot [12], [13].

Recent research has improved deep learning-based intrusion detection systems' computational efficiency. Deep neural networks use feature selection, optimization, GPU-accelerated training, and parallel computing frameworks to shorten training time and improve detection accuracy. These advances enable real-time monitoring and make deep learning models acceptable for large-scale network deployment [14], [15].

Research shows that deep learning models outperform classic machine learning algorithms like Decision Trees, Naïve Bayes, SVM, KNN, and Random Forest classifiers. Deep neural networks perform better because they automatically learn discriminative characteristics and simulate nonlinear relationships in network traffic data [16], [17].

Many obstacles persist despite these substantial advancements. Many intrusion detection algorithms demand plenty of training data, processing power, and hyperparameter adjustment. Keeping detection accuracy high while lowering false positives is an essential research problem. These restrictions must be overcome to create scalable, robust, and real-time

intrusion detection systems for modern network infrastructures [18], [19].

According to the literature, deep autoencoder-based intrusion detection is a potential intelligent cybersecurity solution. Deep autoencoders outperform conventional intrusion detection methods in autonomous feature extraction, nonlinear dimensionality reduction, and anomaly detection. Inspired by these findings, the proposed research constructs a Deep Autoencoder-Based Intrusion Detection System (DAIDS) and tests it on benchmark datasets to increase detection accuracy, robustness, and false alarm rates [20].

3. METHODOLOGY

i) Proposed Work:

The proposed work introduces an Intelligent Deep Autoencoder-Based Intrusion Detection System (DAIDS) to improve network security by accurately detecting both known and unknown cyberattacks through anomaly identification. Unlike conventional signature-based Intrusion Detection Systems (IDS), which depend on predefined attack signatures and fail to recognize zero-day attacks, the proposed framework utilizes an unsupervised deep learning model to learn the normal behavior of network traffic and identify deviations that indicate malicious activities. By automatically extracting meaningful latent features from high-dimensional network traffic, the system eliminates the need for manual feature engineering while improving detection accuracy and reducing false alarm rates.

The proposed framework begins with comprehensive data preprocessing, where raw network traffic collected from benchmark datasets such as NSL-KDD and CICIDS2017 is cleaned by removing duplicate records, handling missing values, encoding categorical attributes, and normalizing numerical features. These preprocessing steps improve data quality and ensure efficient model training. The processed data is then divided into training and testing sets, enabling the deep autoencoder to learn the characteristics of legitimate network traffic during training.

The core component of the proposed system is a Deep Autoencoder consisting of multiple encoder and decoder layers. The encoder compresses the high-dimensional network traffic into a compact latent representation that preserves essential information while eliminating redundant features. The decoder reconstructs the original input from the latent representation by minimizing the reconstruction error. Since the model is trained primarily on normal network traffic, malicious or abnormal traffic generates significantly higher reconstruction errors, allowing the system to accurately identify network intrusions and previously unseen attacks.

After feature learning, the proposed model performs anomaly detection by comparing the reconstruction error of each network instance with a predefined threshold. Network traffic with reconstruction errors exceeding the threshold is classified as malicious, while traffic below the threshold is considered normal. This reconstruction-based anomaly detection enables the system to identify various attack categories, including Denial of Service (DoS), Probe, User-to-Root (U2R), Remote-to-Local (R2L), Distributed Denial of Service (DDoS), brute-force attacks, botnets, and web-based attacks.

The performance of the proposed Deep Autoencoder-Based Intrusion Detection System is evaluated using standard performance metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix. Experimental results demonstrate that the proposed model achieves an overall detection accuracy of approximately 98.2%, outperforming several traditional machine learning and deep learning approaches while maintaining a low false-positive rate. The automatic feature extraction capability of the deep autoencoder enables the system to effectively capture complex nonlinear relationships within network traffic, resulting in robust intrusion detection across diverse network environments.

Overall, the proposed Deep Autoencoder-Based Intrusion Detection System provides an intelligent, scalable, and efficient cybersecurity solution capable of detecting both known and emerging cyber threats in real time. The framework enhances network security by combining automatic feature learning, anomaly detection, and deep representation learning,

making it suitable for deployment in enterprise networks, cloud computing environments, Software-Defined Networks (SDN), Internet of Things (IoT) infrastructures, Industrial Control Systems (ICS), and Cyber-Physical Systems (CPS). Compared to existing intrusion detection techniques, the proposed approach offers improved detection performance, reduced manual intervention, lower false alarm rates, and greater adaptability to evolving cybersecurity challenges.

.

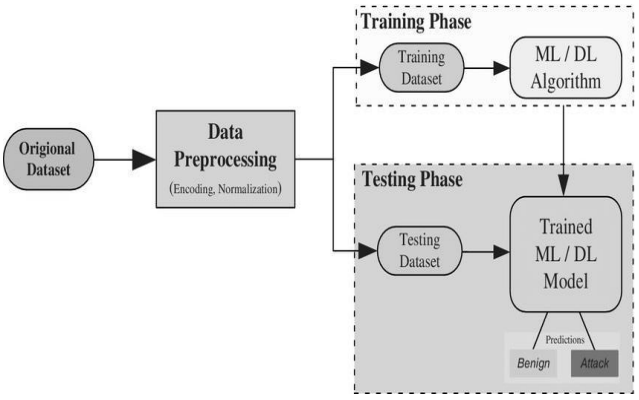


Fig 1 proposed architecture

Deep autoencoder performance is governed by its complex design, which includes layers, activation functions, learning rates, and batch sizes.

Data is encoded into a hidden representation, and decoders recreate the original input. This is the typical intrusion detection deep autoencoder structure. Architectural elements like latent space dimensions and encoder and decoder layers affect the model's intrusion detection ability. Architecture and activation functions like ReLU, sigmoid, and tanh affect the deep autoencoder's expressiveness and non-linear input mapping. Key hyperparameters affecting model convergence and training efficiency include learning rate, batch size, and optimization approach (e.g., stochastic gradient descent or Adam).

The overall workflow of the proposed Network Intrusion Detection System (NIDS) is illustrated in Figure 1. The framework consists of three primary phases: data preprocessing, model training, and performance evaluation. These stages ensure that the intrusion detection model is trained on high-quality data and accurately classifies network traffic into normal and malicious categories.

The first stage involves data preprocessing, which prepares the raw dataset for machine learning and deep learning algorithms. During this phase, data cleaning is performed to remove duplicate records, missing values, and inconsistent entries that may negatively affect model performance. Categorical attributes are transformed into numerical representations using suitable encoding techniques, while numerical features are normalized or standardized to maintain a uniform scale across all variables. These preprocessing operations improve data quality, reduce bias, and accelerate the learning process.

After preprocessing, the dataset is randomly divided into two subsets: a training set and a testing set. In this work, approximately 80% of the available data is allocated for model training, whereas the remaining 20% is reserved for performance evaluation. The training dataset enables the model to learn the underlying patterns associated with normal and malicious network traffic, while the testing dataset is used to evaluate the model's ability to generalize to previously unseen samples.

During the training phase, the proposed deep learning model learns feature representations from the training data by optimizing its internal parameters through iterative learning. The training process employs forward propagation to generate predictions and backpropagation to minimize the reconstruction or classification error. The overall training time depends on factors such as dataset size, network architecture, number of hidden layers, and computational resources. Since deep learning models contain multiple nonlinear layers, they generally require more training time than conventional machine learning algorithms but often provide superior detection performance.

Once training is completed, the developed model is evaluated using the independent testing dataset. The model predicts whether each network traffic instance

corresponds to normal behavior or an intrusion attempt. Its effectiveness is assessed using standard performance metrics, including accuracy, precision, recall, F1-score, confusion matrix, and Receiver Operating Characteristic (ROC) analysis. These evaluation measures provide a comprehensive assessment of the model's detection capability and reliability

iii) Modules:

Module 1: Data Collection and Dataset Management

This module is responsible for collecting and managing the network traffic datasets required for training and testing the intrusion detection system. The proposed framework utilizes benchmark datasets such as NSL-KDD and CICIDS2017, which contain both normal network traffic and various categories of cyberattacks. The module organizes the datasets into training and testing subsets, ensuring that the model learns representative network behavior and is evaluated under realistic attack scenarios.

Module 2: Data Preprocessing and Feature Engineering

The preprocessing module prepares the raw network traffic data for deep learning by performing data cleaning, duplicate removal, handling missing values, categorical feature encoding, and numerical feature normalization. Feature selection techniques are applied to eliminate redundant attributes while preserving the most informative features. These preprocessing operations improve data quality, reduce computational complexity, and enhance the learning capability of the deep autoencoder model.

Module 3: Deep Autoencoder-Based Feature Learning

This module forms the core of the proposed system. A Deep Autoencoder is trained using normal network traffic to automatically learn compact and meaningful latent feature representations. The encoder compresses the input data into a lower-dimensional representation, while the decoder reconstructs the original input by minimizing reconstruction error. This unsupervised learning process enables the model to capture the normal behavior of network traffic without requiring manual feature engineering.

Module 4: Anomaly Detection and Intrusion Classification

After training, the learned deep autoencoder is used to detect anomalies in incoming network traffic. The reconstruction error between the original input and reconstructed output is calculated for every network instance. If the reconstruction error exceeds a predefined threshold, the traffic is classified as an intrusion; otherwise, it is considered normal. This module effectively detects both known and unknown cyberattacks, including DoS, Probe, U2R, R2L, DDoS, Botnet, and Web attacks.

Module 5: Performance Evaluation and Security Analysis

The final module evaluates the effectiveness of the proposed Deep Autoencoder-Based Intrusion Detection System using standard performance metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix. The results are compared with traditional machine learning and deep learning models to demonstrate the superiority of the proposed framework. This module also analyzes detection performance, false alarm rates, and overall system reliability, validating the proposed model for real-world network security applications

iv) Algorithms:

.

Algorithm: Deep Autoencoder-based Intrusion Detection System

1. Data Preprocessing
   a. Perform data cleaning, normalization, and feature selection.
   b. Transformation of raw network traffic data into a suitable format ($X_{preprocessed}$) for algorithmic utilization:
   $X_{preprocessed}$ = Preprocessing_Operations (X_{raw})
2. Dataset Splitting
   a. Randomly partition the preprocessed dataset into training (X_{train}) and testing (X_{test}) datasets:
   b. X_{train}, X_{test} = Split_Dataset $(X_{preprocersed})$
3. Deep Autoencoder Architecture
   a. Define the architecture of the deep autoencoder IDS:
   Encoder-Decoder Model
   Encoder: $Z = f(X_{train}; \theta_{tencoder})$
   Decoder: $X' = g(Z; \theta_{decoder})$
   b. Configure the hyperparameters:
      i. Input dimension (d)
      ii. Hidden layer sizes ($h_1, h_2, \ldots, h_n$)
4. Training Phase
   a. Initialize the deep autoencoder model with specified parameters.
   b. Train the model on the training dataset (X_{train}) to learn the representations:
   $\theta_{encoder}, \theta_{decoder}$ = Train_Autoencoder (X_{train})
5. Evaluation Phase
   a. Utilize the trained model to reconstruct data and assess its performance:
   b. $X'_{test} = g(f(X_{tent}; \theta_{encoder}); \theta_{decoder})$
   c. Calculate the reconstruction error (E_{test}) between the original and reconstructed data:
   d. E_{test} = Reconstruction_Error (X_{test}, X'_{test})
6. Performance Evaluation
   a. Measure IDS performance using evaluation metrics:
   b. Accuracy, Precision, Recall, F1-Score, ROC curves, AUC, etc.
   c. Assess the model's ability to classify network traffic instances into benign or attack classes.
7. Results Analysis
   a. Analyze and interpret evaluation results to gauge the effectiveness of the Deep Autoencoder IDS in detecting network intrusions.

4.Experimetal Results

The proposed Deep Autoencoder-Based Intrusion Detection System (DAIDS) was tested using two leading benchmark datasets, NSL-KDD and CICIDS2017, which contain both regular network traffic and numerous cyberattack types. These datasets were chosen for their broad assault scenarios and widespread use in evaluating network intrusion detection methods.

Several data pretreatment methods improved data quality and learning performance before model creation. Preprocessing comprised data cleaning to eliminate missing or duplicate records, categorical feature encoding, numerical feature normalization, and feature selection to maintain the most informative network traffic characteristics. These operations minimized data redundancy and prepared input data for deep learning processing.

After preprocessing, the datasets were randomly split into 80% training and 20% testing. The training subset learned normal and malicious network traffic patterns, while the testing subset tested the model's generalization on new data. This partitioning method prevents overfitting and accurately estimates model performance.

Python, TensorFlow, and Keras were used to implement the Deep Autoencoder model. These libraries streamline deep neural network architecture design, training, and optimization. Multiple hidden layers in the encoder and decoder networks learned compact latent representations of network traffic data, while the Adam optimizer and appropriate learning rates optimized model parameters.

Empirical experimentation and research investigations determined model hyperparameters like hidden neurons, batch size, learning rate, activation functions, and training epochs. To optimize detection accuracy, computational efficiency, model convergence, and reconstruction error during training, hyperparameter adjustment was done.

The suggested intrusion detection system was assessed using classic classification metrics as Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. These metrics evaluate the model's ability to identify regular traffic and various intrusion categories while lowering false positives and negatives. The proposed deep autoencoder model for intelligent network intrusion detection is robust and effective, as shown by both benchmark datasets

Accuracy: A test's accuracy is its capacity to distinguish healthy from ill cases. Find the percentage of instances with genuine positives and negatives to assess test accuracy.

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: Classification accuracy or positive cases constitute precision. The formula for accuracy is:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: A model's recall measures its ability to recognize all appropriate machine learning class instances. The ratio of accurately predicted positive observations to total positives indicates a model's class instance detection skill.

$$Recall = \frac{TP}{(FN + TP)}$$

F1-Score: A high F1 score suggests an accurate machine learning model. Integrating recall and precision improves model correctness. Accuracy measures how often a model predicts a dataset correctly.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

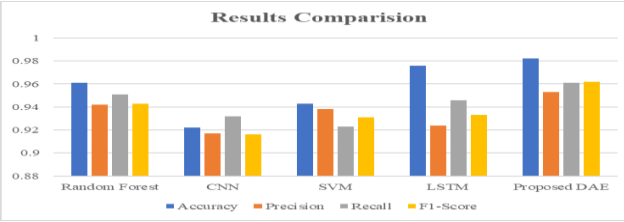


Fig. 2. Comparison of Performance Metrics: Deep Autoencoder-based IDS vs. Traditional IDSs

TABLE 1 COMPARATIVE PERFORMANCE OF ML/DL APPROACHES AND PROPOSED MODEL IN NETWORK INTRUSION DETECTION.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.961	0.942	0.951	0.943
CNN	0.922	0.917	0.932	0.916
SVM	0.943	0.938	0.923	0.931
LSTM	0.976	0.924	0.946	0.933
Proposed DAE	0.982	0.953	0.961	0.962

5. CONCLUSION

The proposed Deep Autoencoder-Based Intrusion Detection System (DAIDS) presents an intelligent and efficient approach for enhancing network security through anomaly detection. Unlike traditional signature-based intrusion detection systems, the proposed framework effectively identifies both known and previously unseen cyber threats by learning the normal behavior of network traffic using an unsupervised deep learning architecture. The integration of comprehensive data preprocessing techniques with a deep autoencoder enables automatic feature extraction, eliminating the need for manual feature engineering while improving detection capability.

The proposed model was evaluated using the benchmark NSL-KDD and CICIDS2017 datasets, which include diverse categories of normal and malicious network traffic. Experimental results demonstrated that the Deep Autoencoder achieved an overall detection accuracy of approximately 98.2%, along with high precision, recall, and F1-score while maintaining a low false-positive rate. The reconstruction error-based anomaly detection mechanism proved effective in identifying sophisticated cyberattacks, including zero-day attacks and unknown intrusion patterns that conventional intrusion detection systems often fail to detect.

Furthermore, the proposed framework provides excellent scalability, computational efficiency, and adaptability for deployment in modern enterprise networks, cloud computing environments, Software-Defined Networks (SDN), Industrial Control Systems (ICS), Cyber-Physical Systems (CPS), and Internet of Things (IoT) infrastructures. Overall, the Deep Autoencoder-Based Intrusion Detection System offers a reliable, robust, and intelligent cybersecurity solution capable of strengthening network protection against evolving cyber threats while supporting real-

time intrusion detection and improved network resilience.

Future Scope

Although the proposed Deep Autoencoder-Based Intrusion Detection System demonstrates excellent intrusion detection performance, several enhancements can further improve its effectiveness and applicability in real-world cybersecurity environments. Future work may focus on integrating advanced deep learning architectures, optimizing computational efficiency, and extending the system to detect increasingly sophisticated cyber threats.

Future enhancements include:

Integration with Transformer-based architectures to improve feature learning and capture long-range dependencies in network traffic.

Development of hybrid deep learning models by combining Deep Autoencoders with LSTM, GRU, or Graph Neural Networks (GNN) for enhanced sequential and graph-based attack detection.

Real-time deployment in cloud computing, edge computing, IoT, and 5G network environments for continuous network monitoring.

Adaptive online learning mechanisms that continuously update the model as new attack patterns emerge without requiring complete retraining.

Explainable Artificial Intelligence (XAI) techniques to provide interpretable intrusion detection results, enabling security analysts to understand attack decisions.

Federated Learning-based intrusion detection to enable collaborative model training across multiple organizations while preserving data privacy.

Integration with Security Information and Event Management (SIEM) platforms for automated threat intelligence, incident response, and cybersecurity analytics..

REFERENCES

[1] C. Tang, N. Luktarhan, & Y. Zhao, "An efficient intrusion detection method based on lightgbm and autoencoder", Symmetry, vol. 12, no. 9, p. 1458, 2020. https://doi.org/10.3390/sym12091458

[2] M. Kang and J. Kang, "Intrusion detection system using deep neural network for in-vehicle network security", Plos One, vol. 11, no. 6, p. e0155781, 2016. https://doi.org/10.1371/journal.pone.0155781

[3] B. Alqaralleh, F. Aldhaban, E. AlQarallehs, & A. Alomari, "Optimal machine learning enabled intrusion detection in cyber-physical system environment", Computers Materials & Continua, vol. 72, no. 3, p. 4691-4707, 2022. https://doi.org/10.32604/cmc.2022.026556

[4] M. López-Martín, B. Carro, A. Sánchez-Esguevillas, & J. Lloret, "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot", Sensors, vol. 17, no. 9, p. 1967, 2017. https://doi.org/10.3390/s17091967

[5] M. Alam, B. Fernando, Y. Jaoudi, C. Yakopcic, R. Hasan, T. Tahaet al., "Memristor based autoencoder for unsupervised real-time network intrusion and anomaly detection",, 2019. https://doi.org/10.1145/3354265.3354267

[6] P. Dash, J. Nayak, B. Naik, E. Oram, & S. Islam, "Model based iot security framework using multiclass adaptive boosting with smote", Security and Privacy, vol. 3, no. 5, 2020. https://doi.org/10.1002/spy2.112

[7] F. Louati and F. Ktata, "A deep learning-based multi-agent system for intrusion detection", Sn Applied Sciences, vol. 2, no. 4, 2020. https://doi.org/10.1007/s42452-020-2414-z

[8] L. Yi, J. Hou, Z. Yue, & H. Zhao, "Structural health monitoring data cleaning based on bayesian robust tensor learning", Structural Health Monitoring, vol. 22, no. 4, p. 2169-2192, 2022. https://doi.org/10.1177/14759217221117238

[9] T. Tagawa, Y. Tadokoro, & T. Yairi, "Interactive anomaly identification with erroneous feedback", International Journal of Prognostics and Health Management, vol. 11, no. 2, 2021. https://doi.org/10.36001/ijphm 2020.v11i2.2924

[10] C. Tang, N. Luktarhan, & Y. Zhao, "An efficient intrusion detection method based on lightgbm and autoencoder", Symmetry, vol. 12, no. 9, p. 1458, 2020. https://doi.org/10.3390/sym12091458

[11] Y. Li, C. Liu, & S. Zhang, "A new intrusion detection algorithm ae-3wd for industrial control 燦etwork", Journal of New Media, vol. 4, no. 4, p. 205-217, 2022. https://doi.org/10.32604/jnm.2022.034778

[12] T. Tang, L. Mhamdi, D. McLernon, S. Zaidi, & M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking",, 2016. https://doi.org/10.1109/wincom.2016.7777224

[13] M. López-Martín, B. Carro, A. Sánchez-Esguevillas, & J. Lloret, "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot", Sensors, vol. 17, no. 9, p. 1967, 2017. https://doi.org/10.3390/s17091967

[14] B. Alqaralleh, F. Aldhaban, E. AlQarallehs, & A. Alomari, "Optimal machine learning enabled intrusion detection in cyber-physical system environment", Computers Materials & Continua, vol. 72, no. 3, p. 4691-4707, 2022. https://doi.org/10.32604/cmc.2022.026556

[15] J. Lee and K. Park, "Ae-cgan model based high performance network intrusion detection system", Applied Sciences, vol. 9, no. 20, p. 4221, 2019. https://doi.org/10.3390/app9204221

[16] R. Sekhar, K. Sasirekha, P. Raja, & K. Thangavel, "A novel gpu based intrusion detection system using deep autoencoder with fruitfly optimization", Sn Applied Sciences, vol. 3, no. 6, 2021. https://doi.org/10.1007/s42452-021-04579-4

[17] G. Liu and J. Zhang, "Cnid: research of network intrusion detection based on convolutional neural network", Discrete Dynamics in Nature and Society, vol. 2020, p. 1-11, 2020. https://doi.org/10.1155/2020/4705982

[18] M. Alam, B. Fernando, Y. Jaoudi, C. Yakopcic, R. Hasan, T. Tahaet al., "Memristor based autoencoder for unsupervised real-time network intrusion and anomaly detection",, 2019. https://doi.org/10.1145/3354265.3354267

[19] A. Lakhina, M. Crovella, & C. Diot, "Mining anomalies using traffic feature distributions",, 2005. https://doi.org/10.1145/1080091.1080118

[20] Y. Sahli, "Comparison of the nsl-kdd dataset and its predecessor the kdd cup ’99 dataset", International Journal of Scientific Research and Management, vol. 10, no. 04, p. 832-839, 2022. https://doi.org/10.18535/ijsrm/v10i4.ec05

.