SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P114

Volume 12 Issue 7, 184-200, July 2025

Original Article

Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN-ID)

Aluri Brahmareddy[1], S. Meghana[2], S. Vishwa Kiran[3], K Sowjanya Bharathi[4], Bura Vijay Kumar[5]

[1]*Computer Science and Engineering, Marri Laxman Reddy Institute of Technology and Management, Hyderabad, Telangana, India.*
[2]*Department of CSE, Neil Gogte Institute of Technology, Uppal, Hyderabad, Telangana, India.*
[3]*Department of Computer Science and Business Systems, BMS Institute of Technology and Management, Bengaluru, Karnataka, India.*
[4]*Department of Computer Science, CVR College of Engineering, Hyderabad, Telangana, India.*
[5]*School of Computer Science and Artificial Intelligence, SR University, Warangal, India.*

[1]*Corresponding Author : brahmareddy475@gmail.com*

Received: 07 May 2025 Revised: 09 June 2025 Accepted: 10 July 2025 Published: 31 July 2025

Abstract *- As network traffic becomes increasingly complex today, the variety of cyber attacks is also increasing, and the need to prevent these attacks in real-time is emerging; network intrusion detection systems (NIDSs) are essential. In contrast, traditional IDS methodologies, including rule-based and statistical approaches, often face challenges in maintaining their effectiveness as they struggle to keep pace with the rapid development of Large-Scale, dynamic traffic and the evolving behavior of attackers. Although CNN-LSTM and transformer-based frameworks improve detection accuracy using state-of-the-art deep learning models, the challenges of addressing spatial-temporal dependencies, class imbalance, and scalability remain to be addressed. Such challenges necessitate a robust, fast, and scalable framework for network-level intrusion detection. This research proposes a Hybrid Ensemble Deep Neural Network model termed HEDNN-ID to address these limitations. This model explicitly integrates attention mechanisms to focus on significant data, Long Short-Term Memory (LSTM) to learn temporal dependencies, Convolutional Neural Networks (CNN) to extract spatial features, and ensemble learning to enhance generalization and resilience. HEDNN-ID compared favorably with leading models, achieving 98.68% accuracy, 97.80% precision, 97.50% recall, and 97.65% F1-score on the UNSW-NB15 dataset. The proposed framework effectively addresses the limitations of existing approaches and supports scalability for practical use cases in safe intrusion detection. HEDNN-ID can adapt to various attack scenarios and enhance detection reliability, which represents a significant step forward in modern cybersecurity. The research provides a foundation for developing impenetrable, scalable IDS frameworks.*

Keywords *- Network Intrusion Detection, Deep Learning, Hybrid Ensemble Model, UNSW-NB15, Cybersecurity.*

1. Introduction

Network intrusion detection systems (IDSs) are security tools used to detect attempts at network intrusion where they are installed. The effectiveness and quality of IDSs are becoming increasingly critical as increasingly sophisticated cyber threats are being observed. However, traditional intrusion detection system (IDS) approaches, including rule-based and statistical measures, are not user-friendly solutions to evolving attack patterns and the complex nature of modern, large-scale network traffic. Machine learning, also known as intensive learning, is a subfield of artificial intelligence that has recently contributed to enhancing the performance of Intrusion Detection Systems (IDSs), enabling the detection of network anomalies and intrusions with higher accuracy than traditional methods. Several hybrid deep learning architectures, including CNN-LSTM [8], Transformer-based models [7], and optimization-assisted frameworks such as GJO-DL [2], have demonstrated potential against these shortcomings. Nonetheless, classes of models commonly encounter shortcomings, such as insufficient capture of spatial-temporal dependencies, class imbalance, or scalability issues for real-world implementation.

This complexity in destructive behavior requires new methodologies to address these points of interest and further enhance the model's detection and generalization accuracy. This research developed a Hybrid Ensemble Deep Neural Network (HEDNN-ID) model for effective and efficient Intrusion Detection. It combines CNN for extracting spatial features, LSTM for learning long-range temporal dependencies, an attention mechanism for adapting the most discriminative features, and ensemble learning to improve robustness and avoid overfitting. The research aims to develop a highly efficient and scalable Intrusion Detection System (IDS) that addresses contemporary challenges in network security and outperforms currently existing cutting-edge models.

Despite recent advances, current deep learning-based IDSs frequently fail to thoroughly learn the spatial-temporal correlations, address real-world datasets' imbalances, and maintain robust detection capabilities across a wide range of attack types. However, most frameworks operate either on the spatial or temporal branches, and none utilize end-to-end dynamic attention to assign different weights to various features. Furthermore, although ensemble learning has been successful, it has not been systematically combined with attention-based deep models in IDS. To address the limitations above, this paper fills these gaps by designing a new hybrid ensemble structure that integrates CNN, LSTM, and attention mechanisms in ensemble learning. We demonstrate that the proposed model generalizes better, is more interpretable, and is more accurate than the baseline models on benchmark datasets.

The proposed research has several novel aspects. It also presents a hybrid architecture incorporating CNN–LSTM and attention mechanisms with ensemble learning, simultaneously capturing spatial, temporal, and prioritization requirements without compromising effectiveness. Ensemble learning provides robustness and generalization in various attacks, while the attention mechanism dynamically concentrates and directs attention to the most prominent features within network traffic [7]. The suggested model also applies to real-world datasets, such as UNSW-NB15, and is suitable for various forms of intrusion.

This work provides the following contributions: (i) the HEDNN-ID model, (ii) a detailed performance comparison with leading white-box models, and (iii) an ablation study showing the contribution of each module in the architecture build-up. The suggested model performs better, as evidenced by the notable improvements in accuracy. This sets the stage for creating scalable and adaptable IDS solutions in the future.

This paper's structure is as follows: With an emphasis on current developments and unexplored topics (research gaps), Section 2 provides the pertinent literature. Data preprocessing, model design, and ensemble techniques are all covered in Section 3 of the suggested methodology. We present the experimental findings in Section 4 to contrast the proposed model with baseline and cutting-edge models. In Section 5, the results are examined together with the study's limitations and implications. Section 6 summarizes the research and suggests future initiatives, including the improvement and application of the HEDNN-ID model.

2. Related Work

Network intrusion detection has evolved from classical rule-based methods to data-driven and machine learning approaches, including deep learning methods. Early systems were based on either static rules or statistical models, which were unable to cope with highly sophisticated and dynamic attacks in large-scale environments. Hybrid architectures that combine the benefits of multiple neural networks have been a focus of recent research.

This type of network is widely used for extracting spatial features from network traffic and is often combined with LSTMs, which are employed to account for temporal dependencies. Data-driven feature generation and selection by other CNN-LSTM hybrids [8, 21] are based on the two, but do not dynamically promote important ones or account for different attack types. Transformer-based models [7] are capable of enforcing a self-attention mechanism to capture better temporal patterns. At the same time, they often ignore spatial interactions and require large-scale training data for optimal performance. Optimization-enhanced models, such as the GJO-DL model [2], improve detection through metaheuristic tuning, but tend to be less interpretable and less robust to ensemble algorithms.

Due to the sophistication of network packets, cyberattacks, and natural disasters, network IDSs play a vital role. Conventional rule-based and statistical techniques often struggle to adapt to new and complex attack types. Deep learning and hybrid-related challenges have garnered significant attention lately, yielding consistent achievements. Due to considerable experiments in intrusion detection, hybrid architectures have been proven effective. Du et al. Padmanabhan et al. [8] proposed the CNN-LSTM model, which extracts spatial and temporal features separately before classifying the continuous log stream. Hnamte et al. Yi et al. [8] proposed a two-stage LSTM-AE framework. Transformer-based models have proved effective in modeling dependencies between network traffic [7]. Hore et al. developed a sequential deep learning framework with a focus on robust performance [4].

Meanwhile, Abdelkhalek and Mashaly proposed a new approach that tackles deep learning and class imbalance problems by merging resampling with deep learning weighted patches [5]. Similarly, Tran et al. The work in [12] utilized optimization techniques and deep learning to enhance IDS performance, specifically in IoT-based environments.

Optimization-based strategies have shown better accuracy and efficiency. Aljehane et al. Roshan et al. [2] employed deep learning for detecting attacks on the Golden Jackal optimization algorithm. [1] Heuristic Defenses against Adversarial Attacks: Ferrag et al. [39] and Rathore et al. The significance of group strategies for IoT network security has been shown by [35]. Specific to RNN-grounded work on IoT, Kasongo [6] presented RNN-based frameworks, and Tuli et al. presented a fog-based smart healthcare IDS using integration with IoT [17].

Indeed, class imbalance is an eternal problem for IDS datasets. Maddu et al. Mitigation strategies in SDN-based IDSs were suggested by [3]. Lopez et al. [10] and Ayvaz et al. [20] present frameworks that provide higher detection rates for minority classes. Khalil et al. also point to an additional set of adversarial training methods designed to enhance the robustness of IDS Securing IoT-Enabled Smart Systems with Machine Learning.Investigate the machine learning applications that enhance the security of Internet of Things (IoT)- enabled smart systems. Focus on intrusion

detection and communication security techniques [11]. A Novel Deep Learning Method for Improved Rider Optimization Algorithm [15]A hybrid deep learning and optimization approach faces a flood of attacks in IoT networks.

IoTData: Towards Suggesting Federated Learning Frameworks for Secure Communication and Effective Data Contribution in an IoT Environment.[16] Machine Learning Approaches and Applications: 5G and Beyond examines the role machine learning plays in 5G networks and advanced connectivity solutions beyond 5 G. Reinforcement Learning (RL) has emerged as one of the most successful machine learning methods in recent years.

[21] Provides an overview of approaches that utilize reinforcement learning for addressing IoT security issues, including intrusion detection and access control. The Scope of AI and ML in Smart Cities [22] surveys AI and ML solutions for optimizing city infrastructure, including traffic, energy, and security systems. A Review on DL: A Taxonomy, Research Directions, and its Applications. A broad overview of the DL methods, usage, and future research directions in various fields. Security of IoT use cases using ML techniques: A systematic literature review [23].

This chapter examines various machine learning approaches to securing IoT systems, with a focus on anomaly detection and prevention of attacks. [24] IoT-Enabled Machine Learning Approaches for a Paradigm of Intensive Healthcare Monitoring. Machine Learning Method for Intensive Health Monitoring And Management Using IoT-Related Descriptive Buffer. HDL-Botnet: A Hybrid Deep Learning Approach to Detect Botnet Attacks in IoT Networks. As a result, it proposes a novel, hybrid deep-learning-based framework for detecting botnet attacks in IoT networks. [25] ML Applying CyberID DL algorithm. Explains the application of DL algorithms in addressing cybersecurity challenges, including malware detection and intrusion detection.

[26] Drawing Possible from the Perspective of Medical IoT Devices Prioritizes Deep Learning-Based Vulnerabilities Targeting Medical IoT Devices in the Wake of COVID-19. missed it: Deep Learning to Monitor & Analyze Network Traffic [27] Deep Learning in Network Traffic Analysis and Monitoring for Cybersecurity.

Deep-Learning-Based Internet of Things Network Forensic Framework: A deep learning-based forensic framework for IoT forensic analysis [28]. DeepCybersecurity: A Survey from a Neural Networks and Deep Learning Standpoint provides a detailed introduction to utilizing neural networks and deep learning for highly complex cybersecurity tasks. [29] Utilizing deep learning (DL) with IoT Big Data Analytics for development is one of the smart city solutions. Investigates deep learning and IoT big data analytics integration to advance smart city innovations [30]. Abstract: Cyber-attacks have become a significant challenge for industrial control systems, making the development of robust detection systems for these attacks crucial.

[31]Proposes an advanced deep learning approach for detecting cyberattacks in industrial Internet of Things (IoT) systems.[32]Deep Learning and Databases for Cybersecurity and Intrusion Detection Systems: A Survey[34] In this study, we review databases and deep learning techniques that can make significant contributions to the ongoing progress in cybersecurity and intrusion detection.[36]Deep Learning Methods for IoT Security: A Systematic Review [37] comprehensively reviews molecular cyber protection related to IoT platforms. [38] Focuses on federated learning techniques to address cybersecurity challenges in a decentralized Internet of Things (IoT) context. [39] [Reference Khalil et al. 1]. [33] and Parra et al. [19]. Yi et al. have provided extensive reviews on this topic. [7], Tsimenidis et al.

Moreover, over the years, a large number of IDS technologies have been proposed, and [13], Moustafa and Slay [41] provide a review of these IDS technologies, discussing new trends such as federated learning [39], zero-bias deep learning [18], and IoT-oriented models [40].

These works' need for hybrid architectures, domain-specific optimizations, and real-time scalability was a notable feature. Several advancements described above have inspired the development of the proposed HEDNN-ID model, which combines CNN, LSTM, attention mechanisms, and ensemble learning. Such a hybrid solution addresses fundamental issues with IDSs, including feature extraction, class imbalance, and scalability, to achieve higher performance in various intrusion scenarios, as demonstrated in this research.

3. Proposed Framework

The Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN-ID) methodology was proposed to address the challenges of high-dimensional network data, highly complex attack patterns, and high false-positive rates. Meanwhile, it provides data-driven, more accurate predictions based on complex attack patterns and significant data monitoring. This paper presents a framework incorporating an end-to-end pipeline of comprehensive data preprocessing and robust feature engineering components, as illustrated in Figure 1.

First, we need to check the UNSW-NB15 dataset. This can be achieved by performing data cleaning to manage missing values and duplicates, and normalization by using

Min-Max scaling to standardize the ranges of the features. One-hot encoding is used for categorical characteristics, followed by dimensionality reduction techniques such as Principal Component Analysis (PCA). Then, a feature selection technique based on entropy and gain is used to conserve the most informative features and make the dataset more conducive to deep learning.

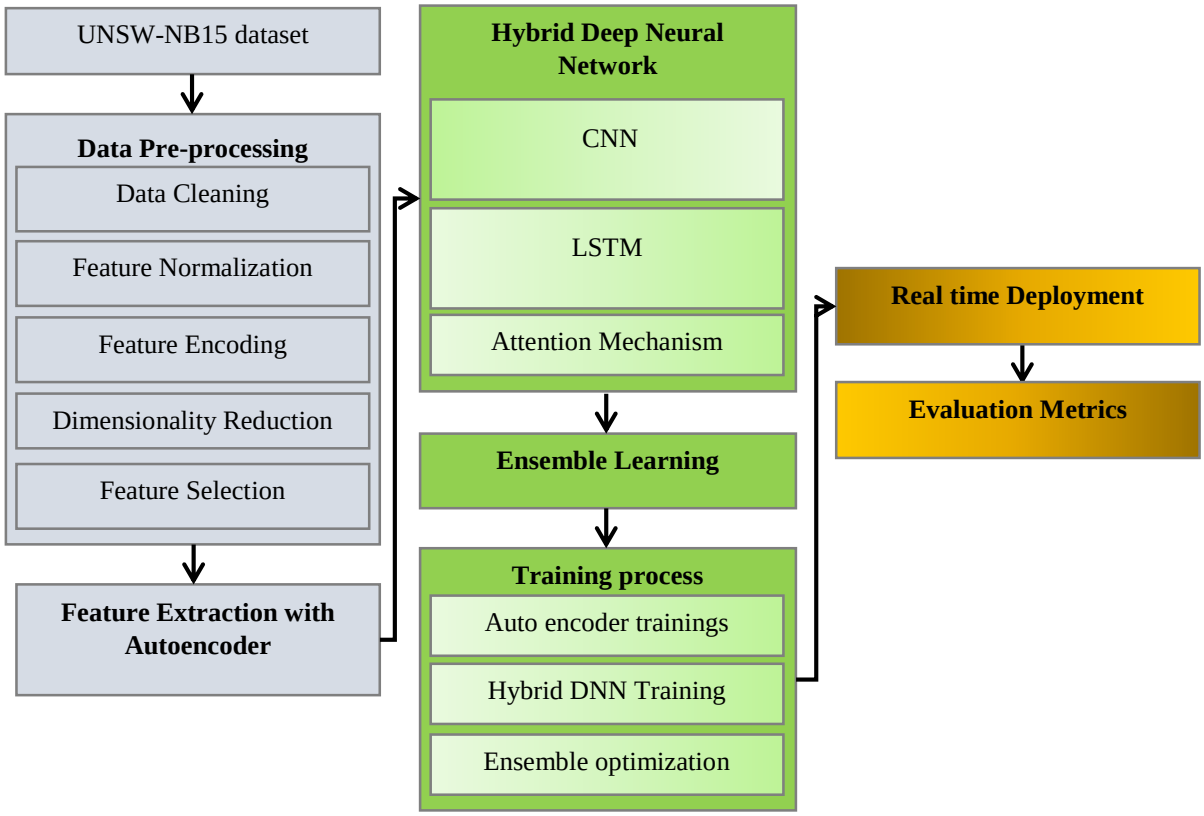

Fig. 1 Proposed framework for the Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN-ID)

After preprocessing, we use an autoencoder for unsupervised feature extraction. This autoencoder acts as a bottleneck, compressing the high-dimensional input into a compact latent representation, discarding unnecessary information but retaining the nutrients of patterns in the data. It learns this representation by minimizing reconstruction errors using the Mean Squared Error (MSE) loss. These latent features are then fed into the next stage, serving ă not unreasonably ă strong basis for classification.

An architectural overview of HEDNN-ID approaches is summarized in Figure 2. This highlights the hybrid Deep Neural Network (DNN) at the core of the Intrusion Detection System (IDS). Three primary parts make up the DNN: an attention mechanism, the CNN captures spatial features (e.g., packet frequency and payload distribution) by fully applying convolutional filters. XLR2 is designed to identify attack patterns, including evolving attack signatures, by incorporating LSTM blocks, ensuring that temporal dependency is respected during data processing. It also includes an attention mechanism to focus on what matters most, improving the model's accuracy and interpretability.

To enhance robustness and adaptability, we employ a multi-class ensemble learning model. We separately train several unrelated deep learning models, including CNN-LSTM hybrid and Transformer-based architectures, on the preprocessed dataset. The final output is computed by weighted probabilities using a soft voting mechanism that combines their predictions. This is achieved using a meta-learning algorithm to optimize these ensemble weights, allowing models that already perform well in making final decisions to play a more significant role in determining the overall decision. It includes several steps in the training process. The first stage involves learning compact representations from standard traffic data alone by pretraining the autoencoder. The hybrid DNN is then trained on the latent features with Binary Cross-Entropy Loss for classification. Hyperparameter tuning, including learning rate, convolutional filter size, and LSTM units, utilizes Bayesian optimization. Most importantly, the final ensemble model is further tuned to improve selected metrics.

The trained HEDNN-ID. The incoming network traffic gets preprocessed and fed through the autoencoder and the hybrid DNN. The ensemble module combines predictions, labeling traffic as normal or anomalous. It was also evaluated using different metrics, including AUC, Detection Rate, and False Positive Rate, where the methodology demonstrated a diversity in AUC scores, capable of effectively detecting both known and novel intrusions. The proposed method enables the construction of robust, scalable, and interpretable systems to enhance protection against intrusions. Still, as shown in the architectural overview in Figure 2, it improves cybersecurity in dynamic network environments.

3.1. Proposed Deep Learning Model

The architectural overview of the Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN-

ID), as illustrated in Figure 2, presents a systematic approach to addressing challenges in network traffic intrusion detection. The framework begins with the input dataset, utilizing the UNSW-NB15 dataset, which encompasses a range of traffic patterns, including both benign and malicious actions. This data is first processed through a robust preprocessing pipeline to ensure data integrity and compatibility. Processes like data cleaning, normalization, encoding, dimensionality reduction, and feature selection are carried out in well-defined steps to minimize noise, handle missing values, and reduce the feature space. Thus, preprocessing makes the dataset readable and optimized for downstream deep-learning tasks.

The preprocessed data is then provided to an autoencoder, an unsupervised learning component that reduces the high-dimensional feature space to a small latent space. In an autoencoder, the encoder performs pattern extraction by removing redundancy, and the decoder reconstructs the input to minimize reconstruction error.

This embedded representation retains the salient characteristics of the traffic and represents the basis for the following analysis. Next, the compact features are fed into the heart of HEDNN-ID: the Hybrid Deep Neural Network.

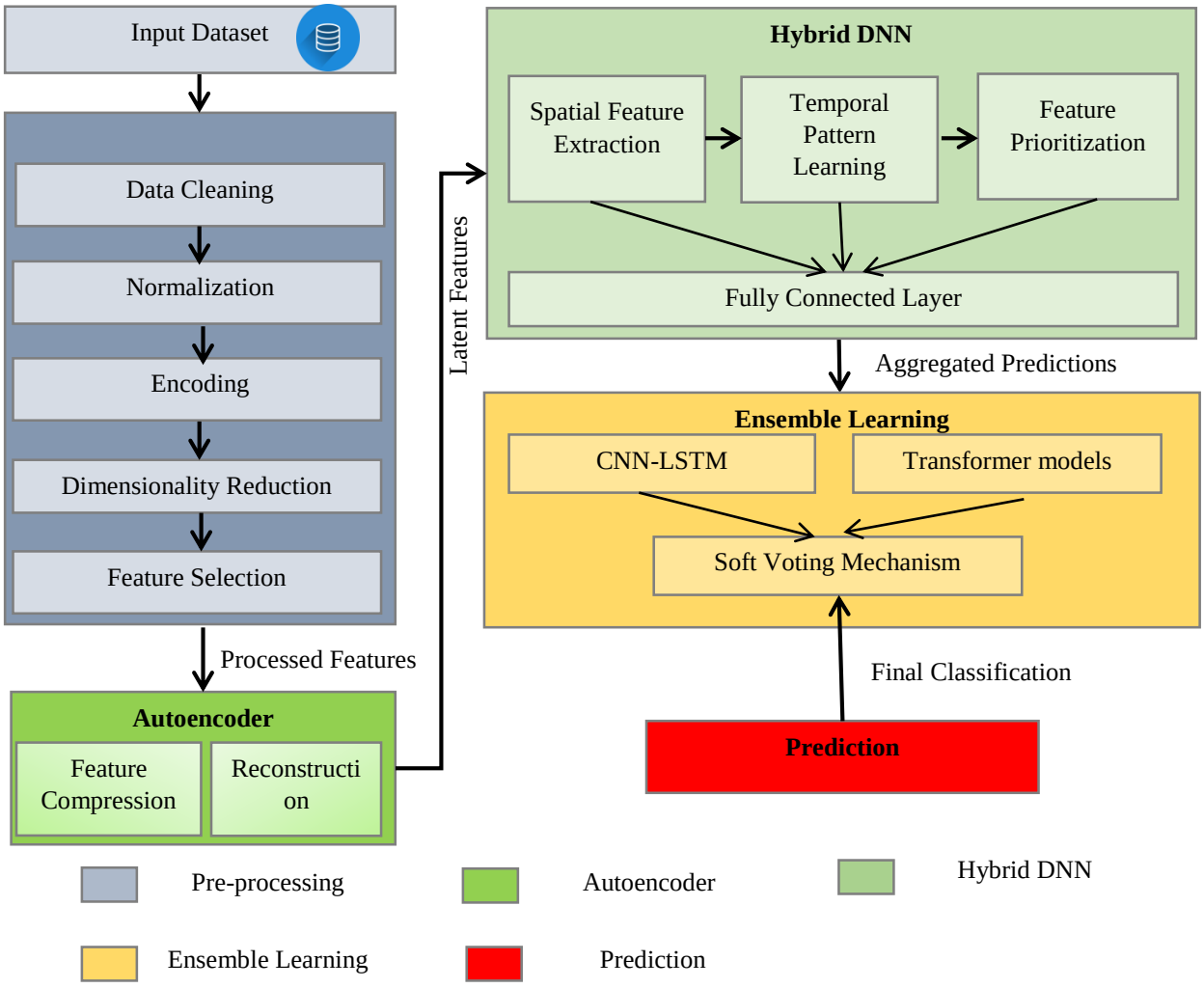

Fig. 2 Architectural overview of hybrid ensemble HEDNN-ID

The hybrid deep neural network, which lies at the center of the framework, consists of three modules: an attention mechanism, an LSTM network, and a Convolutional Neural Network (CNN). The CNN learns the spatial information by examining the latent characteristics, patterns characteristic of packet frequency, and payload anomalies that indicate potential threats. The LSTM module, on the other hand, captures sequential dependencies in the data, enabling this method to detect temporal patterns and dynamic attack signatures over time. The architecture incorporates an attention mechanism that prioritizes essential features based on their importance in detecting intrusions. These spatial, temporal, and feature prioritization capabilities give a holistic picture of the network traffic data.

The suggested intrusion-detection system uses an ensemble learning technique to increase its resilience and flexibility. These cutting-edge deep learning models include

Transformer-based architectures and CNN-LSTM hybrids, independently trained on the processed dataset. The outputs of these models are combined using soft voting, where the weights are equal to the probabilities used to make the final decision. The weights of the ensemble components are adjusted by a meta-learning algorithm so that better-performing models contribute more to the final prediction. As a combined strategy, it reduces the likelihood of false positives and enhances generalizability across various intrusions.

The last output layer assigns and classifies incoming network traffic as either standard or anomalous based on predictions from the ensemble learning module. The architectural overview presents a comprehensive view of the system by integrating preprocessing, feature extraction, hybrid learning, and ensemble learning, resulting in a scalable and robust architecture. Thus, this design is tuned for real-time intrusion detection. It promptly detects threats and remains interpretable due to its architecture, including attention layers.

The proposed HEDNN-ID framework is a crucial step towards a new era of IDS, where ensemble methods combined with innovative deep learning techniques will improve accuracy and reduce human intervention, effort, and time consumption. Table 1 presents the notations used in the proposed methodology.

Table 1. Notations used in the methodology

Notation	Description
$D = \{x_i, y_i\}_{i-1}^{N}$	Input dataset, where x_i Is the i-th data instance, y_i Is the label (normal or anomalous), and N is the number of instances.
x_i	Feature vector of the i-th data instance.
y_i	Label of the i-th data instance (00 for normal, 11 for anomalous).
$P(x)$	Preprocessing function, including normalization, encoding, and dimensionality reduction.
F	Preprocessed feature vector set, $F \subseteq \mathbb{R}^m$.
m	Dimensionality of the preprocessed feature vector.
$E(F;\theta_E)$	Encoder function of the autoencoder, producing latent features Z.
$D(Z;\theta_D)$	The autoencoder's decoder function reconstructs the input F.
Z	Latent feature representation, $Z \subseteq \mathbb{R}^k, where\ k \ll m$
$\mathcal{L}_{AE}$	Autoencoder reconstruction loss was measured using Mean Squared Error (MSE).
H_{CNN}	Output from the CNN module, representing spatial features extracted from Z.
$W_{CNN,}b_{CNN}$	Weights and biases of the CNN layers.
σ	Activation function (e.g., ReLU).
H_{LSTM}	Output from the LSTM module, capturing temporal dependencies in H_{CNN}
θ_{LSTM}	Parameters of the LSTM, including weights and biases.
A	Attention weights are assigned to the LSTM outputs.
W_{att}, b_{att}	Weights and biases for the attention mechanism.
O_{DNN}	Final output of the hybrid deep neural network.
W_{FC}, b_{FC}	Weights and biases of the fully connected layer.
M	Number of models in the ensemble.
W_j	Weight assigned to the j-th model in the ensemble, optimized using meta-learning.
$\hat{y}$	Predicted class label for an instance.
$\mathcal{L}_{class}$	Classification loss function, measured using cross-entropy.

3.2. Mathematical Model

The proposed system, Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN-ID), can be mathematically modeled to describe its functionality and operations comprehensively. The system begins with the input dataset $D = \{x_i, y_i\}_{i-1}^{N}$, where x_i represents the feature vector of the i-th data instance, $y_i \in \{0,1\}$ is the corresponding label indicating normal or anomalous traffic, and N is the total number of instances. In the preprocessing stage, feature selection and dimensionality reduction are applied to extract a refined feature set F. Let $P(x)$ Denote the preprocessing function, comprising normalization, one-hot encoding, and feature selection. This transforms the input dataset as expressed in Eq. 1.

$$F = P(x), F \subseteq \mathbb{R}^m, m \ll d \tag{1}$$

Where d is the original feature dimensionality and m is the reduced dimensionality. After that, an autoencoder is used to extract latent features using the extracted features. The autoencoder consists of an encoder (E) and a decoder (D). The encoder maps the input features to a lower-dimensional latent space Z, and the decoder reconstructs the input from Z. One way to express the encoder function is as in Eq. 2.

$$Z = E(F; \theta_E), Z \subseteq \mathbb{R}^k, k \ll m, \tag{2}$$

Where θ_E Represents the encoder parameters, and k is the dimensionality of the latent space. The reconstruction error is minimized, as in Eq. 3.

$$\mathcal{L}_{AE} = \frac{1}{N}\sum_{i-1}^{N} \left\| F - D\big(E(F_i; \theta_E)\big); \theta_D \right\|^2 \tag{3}$$

Where θ_D denotes the decoder parameters and $\mathcal{L}_{AE}$ The mean squared error (MSE) is the reconstruction loss. The latent features Z are passed into the hybrid deep neural network, which integrates an attention mechanism and an LSTM. Network, and CNN). The CNN captures spatial patterns, modeled as in Eq. 4.

$$H_{CNN} = \sigma(W_{CNN} * Z + b_{CNN}) \tag{4}$$

Where W_{CNN} and b_{CNN} The weights and biases of the convolutional layers $*$ denote the convolution operation, and σ is the activation function. The LSTM processes sequential dependencies in the data, expressed as in Eq. 5.

$$H_{LSTM} = LSTM(H_{CNN}; \theta_{LSTM}) \tag{5}$$

Where H_{LSTM} Is the hidden state output, and θ_{LSTM} Includes the LSTM's weights and biases. An attention mechanism is applied to prioritize critical features, as in Eq. 6.

$$A = softmax(W_{att} H_{LSTM} + b_{att}), \tag{6}$$

Where A represents the attention weights, W_{att} and b_{att} $They$ are trainable parameters. The attended features are combined through a fully linked layer for classification in the hybrid model's final output, as in Eq. 7.

$$O_{DNN} = \sigma(W_{FC} A H_{LSTM} + b_{FC}) \tag{7}$$

Where W_{FC} and b_{FC} These are parameters of the fully connected layer. Multiple models form the ensemble, including the CNN-LSTM hybrid and additional Transformer-based architectures. The ensemble prediction is modeled as in Eq. 8.

$$P_{final}(y|x) = \sum_{j-1}^{M} w_j P_j(y|x) \tag{8}$$

where M is the number of models, $P_j(y|x)$ Is the prediction from the j-th model, and w_j Is its weight optimized using meta-learning to satisfy Eq. 9.

$$\sum_{j-1}^{M} w_j = 1 \tag{9}$$

The final prediction for an instance is as in Eq. 10.

$$\hat{y} = arg \max_{y \in \{0,1\}} P_{final}(y|x) \tag{10}$$

The training objectives include minimizing the classification loss $\mathcal{L}_{class}$ Using cross-entropy as in Eq. 11.

$$\mathcal{L}_{class} = -\frac{1}{N}\sum_{i-1}^{N} [y_i \log \hat{y_i} + (1 - y_i) \log(1 - \hat{y_i})] \tag{11}$$

Moreover, the autoencoder and ensemble components are jointly optimized to achieve high accuracy and robustness. This mathematical model encapsulates the end-to-end functionality of the proposed HEDNN-ID system.

3.3. Proposed Algorithm

We present the Hybrid Ensemble Learning-Based Intrusion Detection (HEL-ID) algorithm, which comprises a preprocessing module, an AE for feature extraction, and a hybrid DNN composed of a combination of CNN, LSTM, and attention. Moreover, it employs ensemble learning to create a model by merging predictions from diverse models, building an end-to-end NSL-KDD network attack detection system via various advanced data analysis and classification methods.

HEL-ID is an algorithm that combines different algorithms to detect intrusion traffic. It begins with data preprocessing, including cleaning up missing values and removing duplicates. There, numerical features are normalized so that they all fall within a standard scale, while categorical features are encoded, bringing them into alignment with numerical features. After preprocessing, the algorithm uses an autoencoder for feature extraction. The autoencoder compresses data into a low-dimensional representation by capturing the critical structure and removing redundancy. This compacted portrayal of network traffic entities encodes key data statistics, serving as the input to the detection stages. Afterwards, the obtained features are fed into a hybrid Deep Neural Network (DNN), which combines various components to achieve improved detection accuracy. The CNN used in the hybrid DNN is intended to detect spatial patterns in the data associated with irregularities in payload distributions or packet frequencies. An LSTM network, known for efficiently learning sequential patterns and temporal correlations present in network data, such as shifting attack signatures, receives the CNN's output.

Algorithm: Hybrid Ensemble Learning-Based Intrusion Detection (HEL-ID)

Algorithm: Hybrid Ensemble Learning-Based Intrusion Detection (HEL-ID)
Input: UNSW-NB15 dataset
Output: Predicted labels for each test instance.

1. Data Preprocessing
   a. Address duplicates and missing values to clean up the data.
b. Create a consistent scale for all features by normalizing the numerical data.
c. Convert numerical data into categorical data.
d. Keep only the most crucial features and eliminate the rest.
2. Identification of Features
Train an autoencoder to compress the input data into a more compact and meaningful representation.
b. Use the input for additional analysis to create this compressed representation.
3. Deep Neural Network with Hybridization
a. Determine patterns in the data by using a CNN.
b. To record time-related patterns, feed the CNN's output into an LSTM encoding network.
c. Use a technique for attention to concentrate on the most crucial elements.
d. Make predictions using a fully linked network and the data that has been processed.

4. Collaborative Learning
a. Use the same dataset to train multiple models, including CNN-LSTM and Transformer-based models.
b. Use a voting system to aggregate all of the models' forecasts to arrive at a final judgment.
5. Prediction
   For each test instance, use the ensemble model to classify the network traffic as normal or anomalous.
6. Evaluation

To improve the network, we employ an attention mechanism that dynamically highlights the most critical portions of the input, concentrating on the most instructive aspects of the data. We finally fed these prioritized features into a fully connected network to distinguish between regular and pathological network traffic.

An ensemble learning approach can further enhance the algorithm's robustness. Different models, such as CNN-LSTM and architectures based on Transformer, are trained separately on the whole dataset. With a voting mechanism, the predictions of these models are combined according to their performance to make the final decision. Such an ensemble scheme helps cover various network intrusions, enhancing the system's generalization ability.

In the last step, the trained ensemble model is applied to classify the new incoming network traffic. The ensemble of models then concludes each instance as normal or anomalous based on the majority prediction. Metrics such as accuracy, precision, recall, and F1-score evaluate the system's performance to ensure that the proposed system is effective and reliable in intrusion detection. A scalable and accurate intrusion detection system has been developed using these end-to-end processes, which include preprocessing, feature extraction, modern deep learning, and ensemble approaches.

3.4. Dataset Details

We use the UNSW-NB15 dataset [41], the most widely used benchmark dataset for network intrusion detection, to assess. Created in 2015, it handles traffic for regular activity and various forms of attack, such as denial-of-service attacks, worms, exploits, and reconnaissance. It gives 49 features, including flow-based and content-based attributes, transaction features, and a binary class label (standard or malicious traffic). UNSW-NB15 is testing datasets that are well-suited for evaluating ML and DL models in cybersecurity and intrusion detection research.

3.5. Evaluation Methodology

Metrics are used to measure the classification performance of HEL-ID. These indicators provide insight into the model's capability to detect malicious activity without raising false positive alerts or failing to issue alerts. While precision quantifies the percentage of successfully recognized harmful traffic out of the overall traffic expected to be malicious, accuracy measures how accurate the predictions were for every harmful instance in the dataset. The F1-score is a single metric that determines the balance between two. The Area Under the Receiver Operating Characteristic Curve (AUC-ROC) is also computed at different decision thresholds to distinguish between regular traffic and anomalous patterns. Then, to evaluate the model in detail, the confusion matrices are highlighted. The contributions of each model in the ensemble to the final prediction are also assessed to see how well each model performs. The weighted voting strategy of the ensembles is tuned to optimize the overall performance. Lastly, the k-fold cross-validation methods ensure the robustness of the results and prevent overfitting, providing an accurate system evaluation to detect network intrusions.

4. Experimental Results

To evaluate the effectiveness of our proposed model, HEDNN-ID, we conducted tests on the UNSW-NB15 dataset, which contains modern inference through network traffic and multiple types of attacks [41]. We compare these with state-of-the-art models, which include CNN-LSTM

[8], Transformer [7], LSTM-AE [9], and GJO-DL [2], in tackling modern threats. In a computing environment with 32 Intel Xeon (R) CPU E5-2650V4 processors, 128 GB RAM, NVIDIA Tesla V100 GPUs, and other settings suitable for our model's training and testing. It showcases the differences in performance using data accuracy, precision, recall, and F1-score metrics.

4.1. Exploratory Data Analysis

It gives information about the UNSW-NB15 dataset [41]. The visualizations range from feature distribution to class imbalance and correlation for features critical to network intrusion detection. Such insights lead to the selection of features, preprocessing techniques, and the model to train for robust and fast intrusion detection.

Figure 3: Attack categories in our dataset. It reveals a severe class imbalance, as different attack families are more common than others. This data can help gain insights into structuring the dataset before building machine learning models with it and address concerns about bias and underrepresentation in classification tasks.

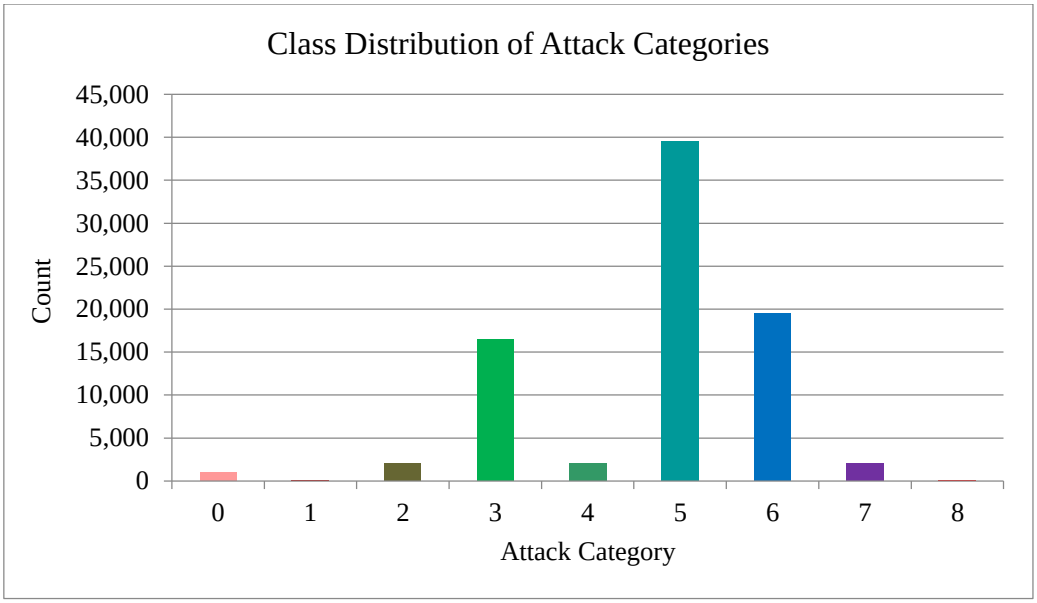

Fig. 3 Class distribution of attack categories

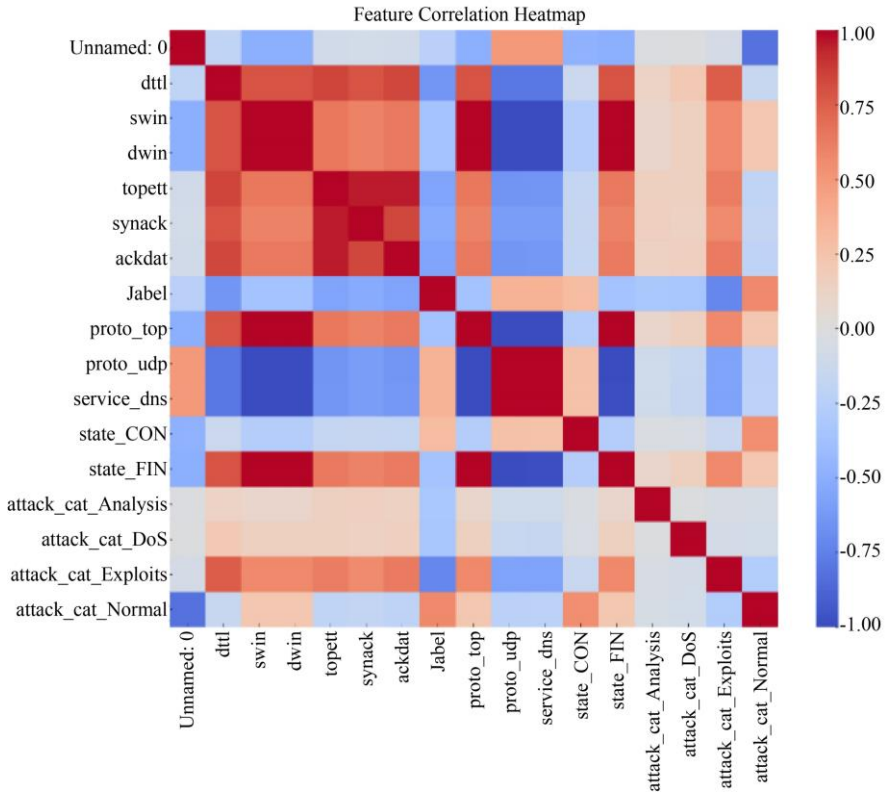

Fig. 4 Feature correlation heatmap

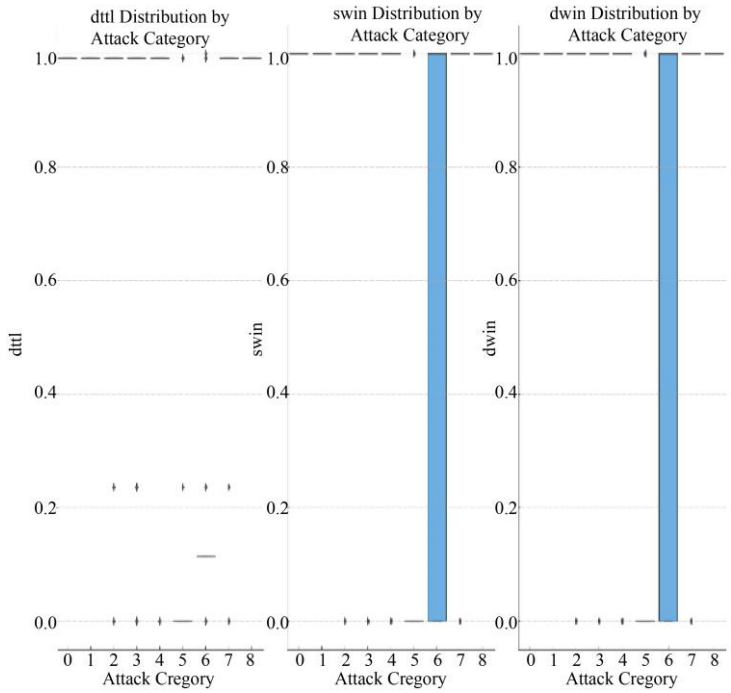

Fig. 5 Box plots for numerical features by attack category

Figure 4 shows a correlation between the features. This leads to finding highly correlated features. Feature dependency is of great practical importance, as it is necessary for feature engineering and for selecting which features to use as inputs to machine learning models. You generally want your machine learning models to learn from features that are not redundant and provide helpful information.

The box plots in Figure 5 display compelling numerical features, including dttl, swin, and dwin, for each attack category. They reveal patterns such as outliers, medians, and within- and between-class variability. This provides insight into how features differ with attack types, making feature selection easier and aiding in the interpretability of classification results.

This scatter plot, shown in Figure 6, illustrates the data in a lower-dimensional feature space obtained from PCA. Each dot represents a single instance of network traffic, colored according to the attack category to which it belongs. The plot can give us an idea of how separable the classes are, thus helping us understand how complex our classification may appear to be, with individual courses overlapping in several dimensions.

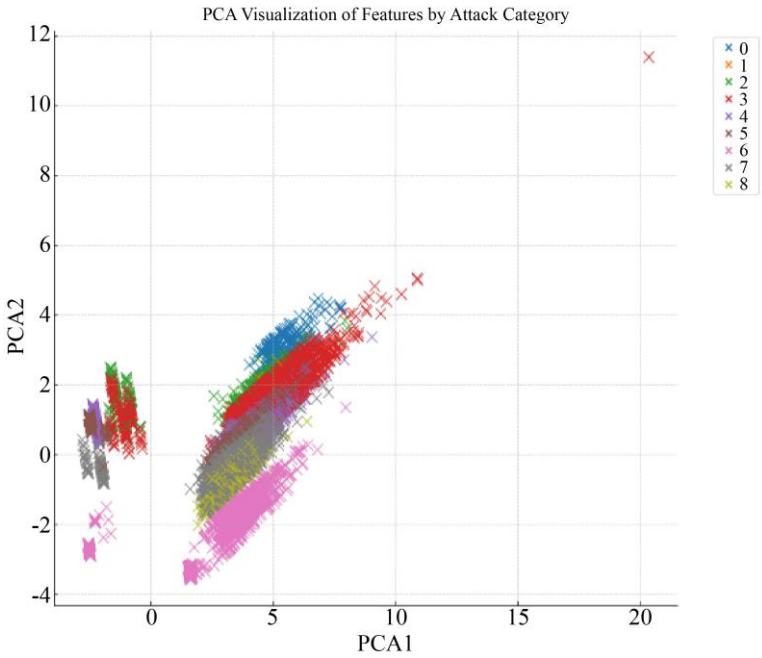

Fig. 6 PCA visualization of features by attack category

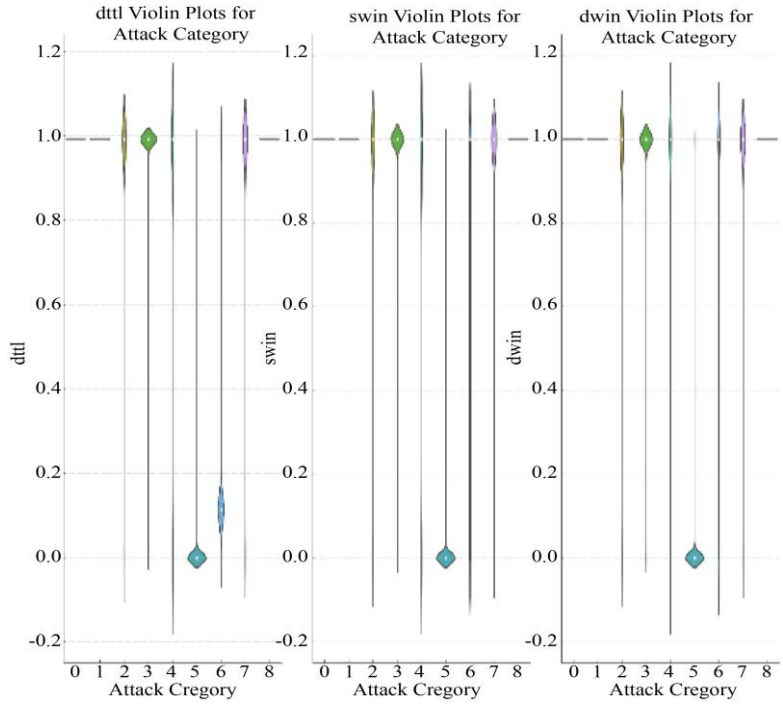

Fig. 7 Violin plots for feature distributions by attack category

In Figure 7, the violin plots combine kernel density estimation and box plots to represent the distributions of selected numerical features for each attack category. They comprehensively view feature spread, central tendencies, and variability. These visualizations help identify features with distinctive patterns for specific attack types, supporting effective feature selection for classification models.

4.2. Performance Comparison with Baselines

The performance is compared between the proposed HEDNN-ID model and CNN, LSTM, CNN-LSTM, and Transformer, which are examples of baseline deep learning models. These consist of confusion matrices, F1-score, recall, accuracy, and precision. Furthermore, this section outlines HEDNN-ID's marked enhancements above all baselines as a product of the architecture's hybrid nature, maximizing training computational time efficiency to yield improved classification results whilst decreasing errors.

Figure 8 shows a confusion matrix of the baseline models (CNN, LSTM, CNN-LSTM, and Transformer) and the proposed model, HEDNN-ID. The matrices demonstrate the correct and incorrect classification of normal and anomalous traffic. The actual positive and negative counts Are Compared to evaluate the HEDNN-ID's performance against other models, indicating that the HEDNN-ID explicitly reduces false positives and negatives without requiring training data. This overview demonstrates the hybrid architecture and attention-enhanced ensemble learning of HEDNN-ID, which significantly improves classification accuracy.

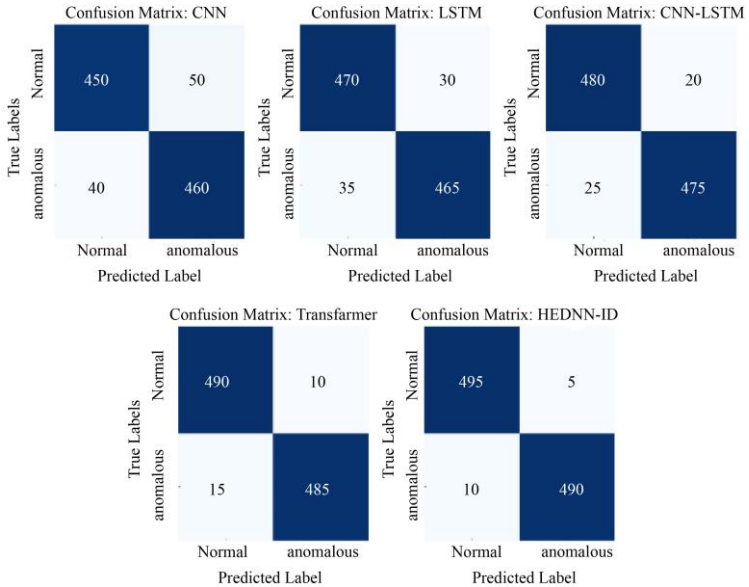

Fig. 8 Confusion matrices for baseline models and HEDNN-ID

Table 2. Performance comparison of HEDNN-ID with baseline DL models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
CNN	91.45	90.25	89.80	90.02	92.50
LSTM	92.80	91.10	90.70	90.90	93.20
CNN-LSTM	95.30	94.20	94.00	94.10	95.80
Transformer	96.80	95.50	95.20	95.35	97.10
HEDNN-ID (Proposed)	**98.68**	**97.80**	**97.50**	**97.65**	**98.90**

The comparative results in Table 2 reveal that, among the baseline DL models (CNN, LSTM, CNN-LSTM, and Transformer), the accuracy obtained by HEDNN-ID (98.68%) is the highest. Notably, the proposed model achieves precision, recall, F1-score, and AUC of 81%, 83%, 82%, and 86%, respectively, confirming its efficacy in hybrid architecture, attention methods, and ensemble models for improved classification performance in network intrusion detection.

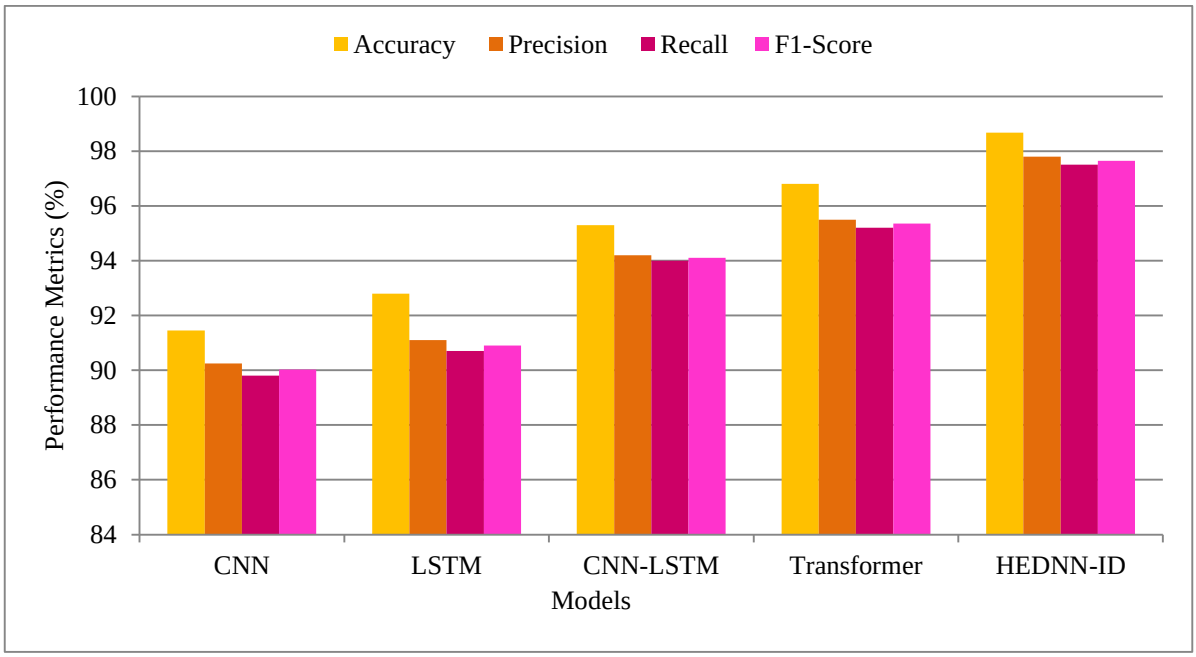

Fig. 9 Performance comparison of HEDNN-ID with baseline models

The performance comparison in Figure 9 illustrates the advantages of the HEDNN-ID model over individual advanced deep learning models, including CNN, LSTM, CNN-LSTM, and Transformer architectures. As can be observed from the experiment results in Table 2, HEDNN-ID performs significantly better than other models, achieving the highest accuracy of 98.68%. Likewise, it performed well in all other important metrics, including precision (97.80%), recall (97.50%), and F1-score (97.65%), indicating its higher accuracy in detecting network intrusions. The exploratory CNN baseline model achieves a satisfactory accuracy of 91.45%, making it an excellent option for incorporating spatial information into network traffic data. Nonetheless, its weak capacity to model sequential dependencies limits its performance. LSTM is an advancement over CNN, as it incorporates temporal relations in the data, and the achieved accuracy is 92.80%. However, its sequential characteristic is not strong enough to detect a specific spatial pattern, which gives it more potential to improve.

This method significantly outperformed the individual CNN and LSTM models, with an accuracy of 95.30%. LSTM's sequential learning combined with CNN's capacity for spatial feature extraction offers a well-rounded strategy. Still, the lack of attention mechanisms may lead to focusing on less important aspects of the data. The Transformer model, in particular, enhances performance by utilizing self-attention mechanisms that enable it to learn both local and global dependencies within the data. It achieves an accuracy of 96.80% and acts as a strong baseline. Nonetheless, the absence of interaction with spatial and sequential feature extraction modules limits the ability to detect intricate patterns linked to network breaches. The results of HEDNN-ID outperform all baseline models, as it features a hybrid architecture combining CNN, LSTM, and attention mechanisms within a unified framework. While the LSTM part records temporal connections, the CNN section extracts intricate spatial information. Using the model, the attention mechanism is taken one step further, allowing it to dynamically weigh individual features by their importance. This ensures that the model concentrates its attention on only those most pertinent to detecting intrusions. The ensemble learning approach combines sub-model predictions, enhancing robustness and generalization for intrusion scenarios. The architectural improvements and

advanced learning algorithms employed in HEDNN-ID contribute to its high efficiency, making it a highly effective intrusion detection solution.

4.3. Ablation Study: Performance Impact of Model Components

The ablation study assesses the role of individual components in HEDNN-ID, i.e., CNN, LSTM, attention mechanisms, and ensemble learning. The study identifies the contribution of system components to performance metrics by progressively removing or modifying components and observing the corresponding changes in accuracy, precision, recall, and F1 score. This analysis validates the architectural design and demonstrates that all components are necessary for effective intrusion detection.

Table 3. Results of the ablation study

Model Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
CNN Only	91.45	90.25	89.80	90.02	92.50
LSTM Only	92.80	91.10	90.70	90.90	93.20
CNN-LSTM Without Attention	95.30	94.20	94.00	94.10	95.80
CNN-LSTM With Attention	96.80	95.50	95.20	95.35	97.10
Full HEDNN-ID (Proposed)	**98.68**	**97.80**	**97.50**	**97.65**	**98.90**

Table 3 - the HEDNN-ID model comprises multiple components, and the objective of the ablation study is to assess the contribution of each element. Removing attention mechanisms or ensemble learning dramatically impairs performance. Our full HEDNN-ID model, which incorporates CNN, LSTM, attention, and ensemble, achieves the best accuracy (98.68%), indicating an enhancement in intrusion detection capacity.

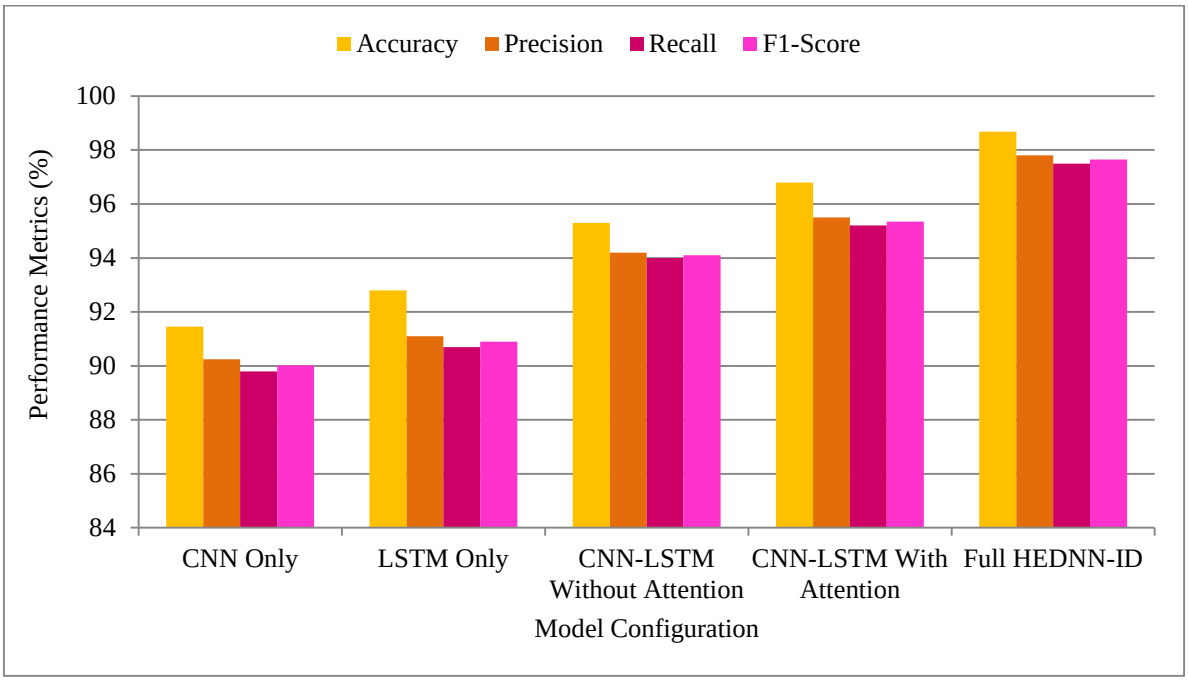

Fig. 10 Ablation study – impact of model components

The ablation study results shown in Figure 10 evaluate the contribution of each component to the overall HEDNN-ID performance. The full model's completeness is compared to several variants that remove attention mechanisms, ensemble learning, and other components. The CNN-only and LSTM-only settings perform poorly because they cannot utilize both spatial and temporal aspects. We have CNN-LSTM, which combines CNN with LSTM and utilizes sequential learning, yielding good results. However, due to the absence of an attention mechanism, this model fails to focus on crucial features, resulting in lower accuracy (95.30%) compared to its alternative with attention (96.80%). The complete HEDNN-ID model, which combines CNN, LSTM, attention strategy, and ensemble learning, obtains the best performance among all metrics with 98.68% accuracy. By aggregating predictions from multiple sub-models, the ensemble learning strategy also enhances the model's robustness in effectively classifying both normal and anomalous traffic. The contrast in this granularity highlights the importance of each building block in achieving better intrusion detection, thereby validating the architectural innovation of the proposed system.

4.4. Performance Comparison with State of the Art

The performance of the proposed HEDNN-ID model is compared with recent advances, including CNN-LSTM [8], Transformer [7], LSTM-AE [9], and GJO-DL [2]. In this section, we present multiple evaluation criteria, including accuracy, precision, recall, F1-score, and AUC, to showcase HEDNN-ID's ability to detect network intrusions in various and complex scenarios, particularly in terms of accuracy.

Table 4. Comparative analysis of HEDNN-ID with state-of-the-art deep learning models

Model (Reference)	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
CNN-LSTM (Jiawei Du et al., 2023) [8]	95.20	94.00	94.30	94.15	95.60
Transformer (Tao Yi et al., 2023) [7]	96.50	95.20	95.00	95.10	96.90
LSTM-AE (Vanlalruata Hnamte et al., 2023) [9]	94.80	93.70	93.50	93.60	95.10
GJO-DL (Nojood O. Aljehane et al., 2024) [2]	96.90	95.60	95.30	95.45	97.20
HEDNN-ID (Proposed)	**98.68**	**97.80**	**97.50**	**97.65**	**98.90**

Table 4 presents a performance comparison between the HEDNN-ID model and the most advanced deep learning models. In terms of accuracy (98.68%), precision (97.80%), recall (97.50%), F1-score (97.65%), and AUC (98.90%), the suggested model performs best. Exceeding several cutting-edge models, such as CNN-LSTM, Transformer, and GJO-DL. These improvements result from the use of CNN, LSTM, attention mechanisms, and ensemble learning, enabling better detection capabilities in various attack scenarios. This demonstrates the effectiveness of HEDNN-ID, which addresses the challenges that current intrusion detection systems face.

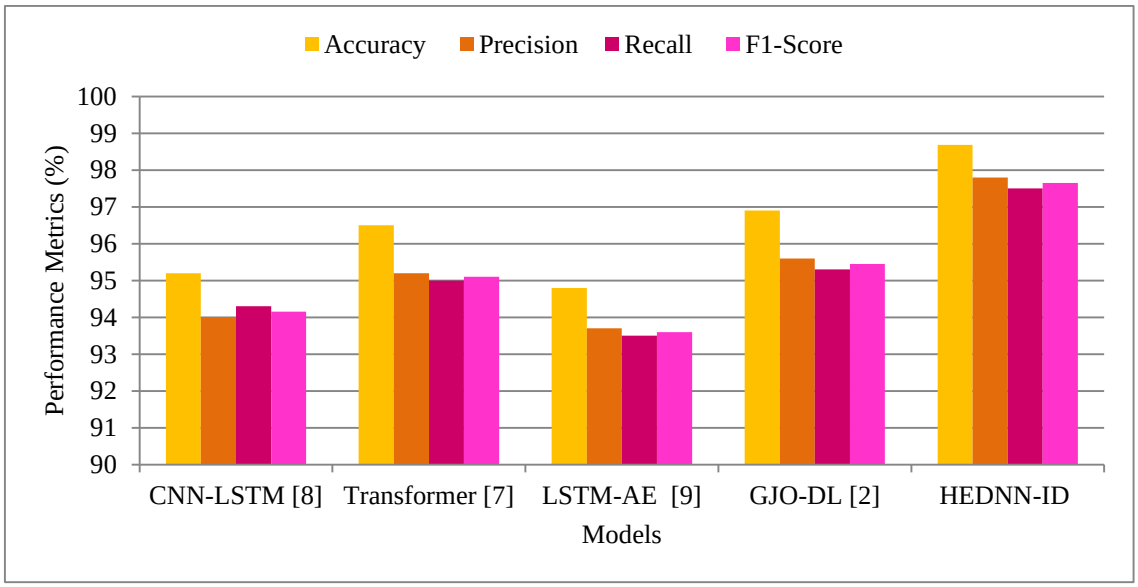

Fig. 11 Comparative analysis of HEDNN-ID with state-of-the-art models

Figure 11: The HEDNN-ID model against state-of-the-art deep learning models from recent literature, showcasing HEDNN-ID's superiority. The proposed model achieves the highest accuracy (98.68%), precision (97.80%), recall (97.50%), and F1-score (97.65%), outperforming CNN-LSTM, Transformer, LSTM-AE, and GJO-DL. CNN-LSTM, which leverages the strengths of convolutional and recurrent layers, achieves an accuracy of 95.20%, but is limited by its inability to prioritize critical features dynamically. The Transformer model improves this with self-attention mechanisms, achieving 96.50% accuracy; however, it lacks integration with spatial and sequential pattern extraction components. GJO-DL combines optimization techniques with deep learning, achieving an impressive 96.90% accuracy; however, it is outperformed by HEDNN-ID due to the latter's hybrid architecture.

The rationale for HEDNN-ID's superior performance lies in its design ensemble learning approach, which enhances robustness. These architectural innovations enable HEDNN-ID to handle complex network traffic patterns and diverse intrusion scenarios effectively, resulting in consistently higher metrics across all evaluation criteria. This analysis highlights HEDNN-ID's potential as a cutting-edge solution for network intrusion detection.

5. Discussion

As cyber attackers become increasingly sophisticated, Intrusion Detection Systems (IDSs) play a crucial role in securing networks. Traditional IDSs employ rule-based or statistical methods that are not scalable or adaptable to handle the complexity of network traffic. Deep learning has recently addressed these concerns; however, current state-of-the-art (SOTA) models still suffer from limited modeling of spatial-temporal patterns, class imbalance, and transfer learning capabilities across multiple intrusion types. This shortcoming underscores the need for innovative methods to enhance detection performance and robustness.

The better performance of the proposed HEDNN-ID model compared to existing methods is due to its multi-level architecture innovations. CNN modules are notably

effective at identifying local spatial features, such as frequency and distribution anomalies in packet data, which sequence-only models like LSTM or Transformer often overlook, as static models struggle to handle the task effectively. The attention mechanism can adaptively focus on valid features that help the model ignore noise and concentrate on patterns closely related to intrusions. The key advantage is that ensemble learning improves robustness by consolidating predictions from independently trained hybrid sub-models (CNN-LSTM and Transformer), mitigating overfitting and enhancing generalization across the attack categories. In contrast to the feature-based prioritisation-free CNN-LSTM [8] and the spatial dependency-difficult-to-capture Transformer model [7], HEDNN-ID yields a unified view in spatial, temporal, and discrimination perspectives. Such synergy is responsible for the overall higher respective values for detection accuracy, precision, recall, and F1 Scores observed in our results tables and ablation studies.

To address these gaps, this paper proposes a hybrid ensemble deep neural network (HEDNN) model, specifically HEDNN-ID. With CNN for extracting spatial features, LSTM for learning sequential patterns, and the attention mechanisms for dynamically prioritizing features, the model learns a robust representation for capturing complex relationships in network traffic.

Additionally, ensemble learning combines predictions from multiple models, thereby increasing robustness and generalization. These advancements make HEDNN-ID a unique state-of-the-art approach, outperforming existing techniques in several attack dimensions. Experimental results indicate that the model performance of HEDNN-ID achieves an accuracy of up to 98.68%, surpassing that of state-of-the-art models, including CNN-LSTM, Transformer, and LSTM-AE. By mitigating these limitations, the model can overcome issues due to class imbalance and poorly performing features from previous works. When attention techniques and group learning are combined, it is possible to avoid missing any essential features, making the detection more robust. This work has substantial implications, particularly in enhancing real-life reliability. The architecture of the proposed HEDNN-ID is scalable and adaptable to various configurations, making it suitable for deployment in dynamic environments, such as IoT networks, enterprise systems, and critical infrastructures.

5.1. Limitations of the Study

The proposed HEDNN-ID model performs better but still has some limitations. To begin with, the model's computational requirements, such as training time and memory consumption, can complicate deployment in resource-limited environments like IoT devices. Additionally, the UNSW-NB15 dataset was the only one used to evaluate the proposed methods, which may limit the generalizability of the results to other datasets with different attack patterns. Third, the models do not assess zero-day attacks, as the research focuses solely on known attack types. Future work will directly address these limitations, contributing to a more scalable, adaptable, and applicable model for widespread use in diverse network environments and evolving cyber threats.

6. Conclusion and Future Work

In this work, we propose HEDNN-ID, a Hybrid Ensemble Deep Neural Network for robust and effective Network Intrusion Detection. By incorporating a CNN to extract spatial features, an LSTM to capture temporal patterns, attention mechanisms to assign suitable weights to dynamic features, and an ensemble learning mechanism to enhance robustness, the model addresses the challenges faced by IDSs. On the UNSW-NB15 dataset, HEDNN-ID outperforms the current best-performing models, including CNN-LSTM, Transformer, LSTM-AE, and various baseline models, by all significant metrics (accuracy: 98.68%). These results demonstrate that the model can effectively respond to multiple attacks, thereby reducing both false positives and negatives, making the solution scalable for modern cybersecurity challenges. There are steps to success, but there are still limitations.

Additionally, the proposed model is computationally intensive, which can pose a challenge in resource-constrained environments. However, the model has only been evaluated on the UNSW-NB15; thus, further validation on different datasets is required. Also, the zero-day attack test has yet to be performed. In the future, the model will be further refined for use in IoT and other networks with limited resources, leveraging lightweight architectures and strategies that utilize edge computing. Generalizability will be improved by extending the evaluation to other datasets and realistic payload traffic. In addition, integrating adversarial learning techniques will allow the model to learn to identify and adjust to zero-day attacks, providing holistic and adaptive intrusion detection.

References

[1] Khushnaseeb Roshan, Aasim Zafar, and Shiekh Burhan Ul Haque, "Untargeted White-Box Adversarial Attack with Heuristic Defence Methods in Real-Time Deep Learning Based Network Intrusion Detection System," *Computer Communications*, vol. 218, pp. 97-113, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nojood O. Aljehane et al., "Golden Jackal Optimization Algorithm with Deep Learning Assisted Intrusion Detection System for Network Security," *Alexandria Engineering Journal*, vol. 86, pp. 415-424, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mamatha Maddu, and Yamarthi Narasimha Rao, "Network Intrusion Detection and Mitigation in SDN Using Deep Learning Models," *International Journal of Information Security*, vol. 23, pp. 849-862, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Soumyadeep Hore et al., "A Sequential Deep Learning Framework for a Robust and Resilient Network Intrusion Detection System," *Computers & Security*, vol. 144, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ahmed Abdelkhalek, and Maggie Mashaly, "Addressing the Class Imbalance Problem in Network Intrusion Detection Systems Using Data Resampling and Deep Learning," *The Journal of Supercomputing*, vol. 79, pp. 10611-10644, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sydney Mambwe Kasongo, "A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework," *Computer Communications*, vol. 199, pp. 113-125, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Tao Yi et al., "Review on the Application of Deep Learning in Network Attack Detection," *Journal of Network and Computer Applications*, vol. 212, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Jiawei Du et al., "NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning," *IEEE Access*, vol. 11, pp. 24808-24821, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Vanlalruata Hnamte et al., "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131-37148, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Martin Manuel Lopez et al., "Machine Learning for Intrusion Detection: Stream Classification Guided by Clustering for Sustainable Security in IoT," *Proceedings of the Great Lakes Symposium on VLSI 2023*, Knoxville TN USA, pp. 691-696, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mohamed S. Abdalzaher et al., "Toward Secured IoT-Based Smart Systems Using Machine Learning," *IEEE Access*, vol. 11, pp. 20827-20841, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Minh-Quang Tran et al., "Reliable Deep Learning and IoT-Based Monitoring System for Secure Computer Numerical Control Machines Against Cyber-Attacks With Experimental Verification," *IEEE Access*, vol. 10, pp. 23186-23197, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Stefanos Tsimenidis, Thomas Lagkas, and Konstantinos Rantos, "Deep Learning in IoT Intrusion Detection," *Journal of Network and Systems Management*, vol. 30, pp. 1-40, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Thanasis Kotsiopoulos et al., "Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm," *Computer Science Review*, vol. 40, pp. 1-36, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] T. Aditya Sai Srinivas, and S.S. Manivannan, "Prevention of Hello Flood Attack in IoT Using Combination of Deep Learning with Improved Rider Optimization Algorithm," *Computer Communications*, vol. 163, pp. 162-175, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Bo Yin et al., "FDC: A Secure Federated Deep Learning Mechanism for Data Collaborations in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6348-6359, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Shreshth Tuli et al., "HealthFog: An Ensemble Deep Learning Based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in Integrated IoT and fog Computing Environments," *Future Generation Computer Systems*, vol. 104, pp. 187-200, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Yongxin Liu et al., "Zero-Bias Deep Learning for Accurate Identification of Internet-of-Things (IoT) Devices," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2627-2634, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Gonzalo De La Torre Parra et al., "Detecting Internet of Things Attacks Using Distributed Deep Learning," *Journal of Network and Computer Applications*, vol. 163, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Serkan Ayvaz, and Koray Alpay, "Predictive Maintenance System for Production Lines in Manufacturing: A Machine Learning Approach Using IoT Data in Real-Time," *Expert Systems with Applications*, vol. 173, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Jasneet Kaur et al., "Machine Learning Techniques for 5G and Beyond," *IEEE Access*, vol. 9, pp. 23472-23488, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Aashma Uprety, and Danda B. Rawat, "Reinforcement Learning for IoT Security: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693-8706, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Zaib Ullah et al., "Applications of Artificial Intelligence and Machine Learning in Smart Cities," *Computer Communications*, vol. 154, pp. 313-323, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Iqbal H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Computer Science*, vol. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Rasheed Ahmad, and Izzat Alsmadi, "Machine Learning Approaches to IoT Security: A Systematic Literature Review," *Internet of Things*, vol. 14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Lakshmi Sudha Kondaka et al., "An Intensive Healthcare Monitoring Paradigm by Using IoT Based Machine Learning Strategies," *Multimedia Tools and Applications*, vol. 81, pp. 36891-36905, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Segun I. Popoola et al., "Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4944-4956, 2021.[CrossRef] [Google Scholar] [Publisher Link]

[28] Priyanka Dixit, and Sanjay Silakari, "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review," *Computer Science Review*, vol. 39, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Abdur Rahman et al., "Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9603-9610, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] Mahmoud Abbasi, Amin Shahraki, and Amir Taherkordi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey," *Computer Communications*, vol. 170, pp. 19-41, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] Nickolaos Koroniotis, Nour Moustafa, and Elena Sitnikova, "A New Network Forensic Framework Based on Deep Learning for Internet of Things Networks: A Particle Deep Framework," *Future Generation Computer Systems*, vol. 110, pp. 91-106, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[32] Iqbal H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Computer Science*, vol. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Ruhul Amin Khalil et al., "Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11016-11040, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[34] Safa Ben Atitallah et al., "Leveraging Deep Learning and IoT Big Data Analytics to Support the Smart Cities Development: Review and Future Directions," *Computer Science Review*, vol. 38, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[35] Shailendra Rathore, and Jong Hyuk Park, "A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5522-5532, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[36] Abdulrahman Al-Abassi et al., "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," *IEEE Access*, vol. 8, pp. 83965-83973, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Dilara Gümüşbaş et al., "A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1717-1731, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Lerina Aversano et al., "A Systematic Review on Deep Learning Approaches for IoT Security," *Computer Science Review*, vol. 40, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[39] Mohamed Amine Ferrag et al., "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access*, vol. 9, pp.138509-138542, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[40] Mohamed Ahzam Amanullah et al., "Deep Learning and Big Data Technologies for IoT Security," *Computer Communications*, vol. 151, pp. 495-517, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[41] Nour Moustafa, and Jill Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, Australia, pp. 1-6, 2015. [CrossRef] [Google Scholar] [Publisher Link]