Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 3, September 2025, pp. 645~667
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i3.6912

CyberShieldDL: A Hybrid Deep Learning Architecture for Robust Intrusion Detection and Cyber Threat Classification

S. Venkatramulu[1*], John Babu Guttikonda[2], Desidi Narsimha Reddy[3], Y. Madhavi Reddy[4], M. Sirisha[5]

[1]Associate Professor, Department of CSE(Networks), Kakatiya Institute of Technology and Science, Warangal, Telangana, India.
[2]Associate Professor, Department of Computer Science & Engineering (AI & ML), Anurag Engineering College, Kodad, Telangana, India.
[3]Data Consultant (Data Governance, Data Analytics: enterprise performance management, AI & amp; ML), Soniks consulting LLC, USA.
[4]Assistant professor, Department H&S (Mathematics), CVR College of Engineering, Ibrahimpatnam, Telangana , India.
[5]PhD scholar, Department Data science, kL University, Vijayawada, Andhra Pradesh India.
Emails: svr.cse@kitsw.ac.in johnbabug@gmail.com dn.narsimha@gmail.com
madhavireddy75@gmail.com msirisha87@gmail.com

Article Info

Article history:

Received Jul 5, 2025
Revised Aug 17, 2025
Accepted Sep 14, 2025

Keywords:

Intrusion Detection System, Deep Learning, CNN-BiLSTM, Attention Mechanism, Network Security

ABSTRACT

In modern network environments, securing systems from newly emerging attacks is essential, and a constructive approach is the use of an IDS (Intrusion Detection System). When faced with attacks that are not in the list of predefined patterns, traditional IDS methods such as signature-based detection or standalone machine learning models may not function properly to detect such attacks because they are not adaptable and not designed to deal with this type of attack. The current IDS systems that employ deep-learning architectures have enhanced detection capabilities; however, most prior art systems are limited by partial feature learning, which only learns features of either spatial or temporal traffic structures. Meanwhile, the lack of context-aware mechanisms, such as attention, limits their ability to attend more to the most informative network components, leading to suboptimal detection performance and generalization. To counter this issue, in this work, we introduce CyberShieldDL, which is the first deep learning-based IDS framework with a novel hybrid architecture: IntruNet-Hybrid, combining Convolutional Neural Networks (CNN) for spatial pattern extraction, Bidirectional Long Short-Term Memory (Bi-LSTM) networks for sequential feature extraction, and an attention mechanism to learn the salient features for intrusion detection dynamically. To create the framework, an optimized pre-processing and feature selection pipeline is presented to effectively and cost-effectively prepare the model input. Extensive experiments on the CIC-IDS2017 dataset demonstrate that CyberShieldDL consistently outperforms the state-of-the-art, achieving an overall accuracy of 98.35% and high precision, recall, and F1-score in various attack scenarios. Cross-dataset validations on NSL-KDD and UNSW-NB15 also verify the system's generalization. The design provides a scalable and flexible solution for real-world network security, offering the flexibility and adaptability necessary to enhance classification accuracy and robustness against evolving attack patterns. Its modular construction enables us to extend it for real-time deployment and future adversarial robustness easily.

Corresponding Author:

Dr. S. Venkatramulu,
Associate Professor,
Department of CSE(Networks), Kakatiya Institute of Technology and Science, Warangal, Telangana, India.
Email: svr.cse@kitsw.ac.in

1. INTRODUCTION

The world's society is gradually relying on personalized networks, and the remarkable increase in cybersecurity threats has encouraged the emergence of Intrusion Detection Systems (IDS) for protecting network infrastructures. Existing IDS techniques, originally dependent on signature matching, struggle to identify new and emerging threats, while those based on machine learning tend to exhibit poor adaptability and generality. In recent years, with the proliferation of new AI technologies, intelligent IDS (IDS) systems equipped with deep learning can be used to learn sophisticated patterns in network traffic data [1], [2]. However, most existing solutions utilize a separate deep learning architecture, such as Convolutional Neural Networks (CNN) or Long Short-Term Memory (LSTM), which are either weak at modelling temporal dependencies or ignore spatial feature interactions [3], [4]. Additionally, another issue is that some research works overlook the attention model, which may help focus on more attack patterns of interest [5]. Recent solutions to these problems have achieved reasonable effectiveness on benchmark datasets; however, robustness across datasets and reducing false alarms remain challenges.

The drawbacks in existing works necessitate a hybrid and adaptive IDS model that can effectively integrate the benefits of spatial and sequential features and adaptively focus on the most informative flow characteristics. In this paper, we present CyberShieldDL, a hybrid CNN–BiLSTM–Attention model for robust intrusion detection. The primary goal of this study is to propose an innovative, flexible, and transferable IDS framework that can effectively monitor various cyberattacks on different networks. The key contributions of this work stem from the hybrid deep learning architecture, feature relevance-driven learning (utilizing an attention mechanism), and a network traffic analysis-tailored feature selection pipeline. Unlike traditional models, the proposed method models both local and sequential dependencies, assigning different importance to the input for detection, which can significantly enhance detection performance. This integrated approach enables the system to adapt to ever-changing attack models and generalize across various datasets.

In contrast to the state-of-the-art CNN-BiLSTM-based models available in the literature for the same type of data, CyberShieldDL offers (i) a refined feature selection pipeline, (ii) comprehensive cross-dataset validation, (iii) attention-based interpretability analysis, and (iv) statistically robust reporting of results.

The main contributions of this work are the generation of the IntruNet-Hybrid model, its thorough experiments on the CIC-IDS2017 dataset, where cross-dataset validation (using the NSL-KDD and UNSW-NB15 datasets) has also been applied, its ablation study that justifies the effectiveness of each model component, and a comparative study that demonstrates superior performance over state-of-the-art methodologies. The proposed testing also introduced an optimized preprocessing and feature selection pipeline designed explicitly for network intrusion data, which was utilized to ensure model training with scalability and efficiency.

The remainder of the paper is structured as follows: Section 2 reviews related work on deep learning-based IDS. Section 3 presents the proposed methodology detailing the CyberShieldDL framework. Section 4 discusses the experimental results and performance evaluations. Section 5 presents a comprehensive discussion and highlights the study's limitations. Finally, Section 6 concludes the paper and outlines future research directions.

2. RELATED WORK

Recent advancements in deep learning have significantly enhanced intrusion detection systems, enabling adaptive, hybrid, and context-aware cybersecurity solutions across domains. Halbouni et al. [1] proposed a CNN-LSTM-based intrusion detection model that leverages the spatial and temporal feature extraction capabilities of deep learning to improve intrusion detection across diverse datasets. Hnamte and Hussain [2] developed the DCNNBiLSTM model, combining convolutional and recurrent layers to address evolving network vulnerabilities using real-time traffic datasets. Lansky et al. [3] provided a systematic review of deep learning-based IDS frameworks, categorizing them by architecture and highlighting their applications in modern cybersecurity contexts. Gueriani et al. [4] presented a CNN-LSTM hybrid IDS tailored for IoT environments, utilizing recent IoT-specific datasets to enhance the detection of malicious activities. Hnamte et al. [5] introduced a two-stage deep learning model that integrates LSTM and autoencoders for the robust detection of complex attack patterns in network traffic. Altunay and Albayrak [6] focused on industrial IoT security by applying CNN, LSTM, and a hybrid of the two to detect intrusions in industrial network environments. Olanrewaju-George and Pranggono [7] explored federated learning combined with supervised and unsupervised deep learning models to enhance privacy-preserving intrusion detection in IoT networks. Berguiga et al. [8] proposed HIDS-IoMT, a hybrid CNN-LSTM IDS designed for medical IoT environments using fog computing. Al-Shurbaji et al. [9] conducted a review of deep learning-based IDS approaches targeting IoT botnet attacks. Berguiga et al. [10] developed HIDS-RPL, a CNN-LSTM-based IDS for secure routing in IoMT networks.

Fares et al. [11] proposed a hybrid intrusion detection model that combines Swin Transformers and LSTM networks, utilizing transfer learning to address the data scarcity issue in IoT environments. Aboalela et al. [12] presented an approach for detecting DDoS attacks in IoT using optimized feature pruning and a hybrid deep learning model that integrates temporal convolutional networks and recurrent units. Al Mazroa et al. [13] introduced a cyberattack detection method for cyber-physical systems (CPS) that utilizes binary metaheuristics and deep learning, with a focus on optimizing feature selection and classification processes. Dayarathne et al. [14] investigated cyber risk mitigation in innovative cyber-physical power systems by integrating deep learning models with hybrid security frameworks to detect anomalies in renewable energy-based grids. Hariharan et al. [15] proposed a hybrid deep learning model that combines Seq2Seq architectures and ConvLSTM subnets, aiming to improve spatial and temporal dependency learning for network intrusion detection. Alhayan et al. [16] presented a deep learning-based IDS for cloud computing environments, integrating CNN-BiLSTM models with spotted hyena optimization for improved cloud security. Manivannan and Senthilkumar [17] developed the ARNN-FOX model, an adaptive recurrent neural network with a fox optimizer, enhancing intrusion detection through dynamic hyperparameter tuning. Khan et al. [18] designed an adaptive hybrid framework combining artificial neural networks and genetic algorithms for intrusion detection in Industrial IoT networks. Sun and Wang [19] proposed an image-based neural network classification approach, transforming network traffic into grid structures to leverage CNN-based intrusion detection. Duraibi and Alashjaee [20] introduced the IMFOHDL-ID approach, combining dimensionality reduction techniques with hybrid deep learning models for IoT cyberattack detection.

Huma et al. [21] proposed a hybrid deep random neural network model to enhance cyberattack detection in Industrial IoT environments, addressing diverse threat patterns. Ozkan-Okay et al. [22] introduced SABADT, a hybrid IDS combining anomaly and signature-based techniques for effective cyberattack detection in wireless local area networks. Ho et al. [23] developed a convolutional neural network-based intrusion detection model that can identify both known and novel cyberattacks using advanced feature representations. Elsaeidy et al. [24] presented a hybrid deep learning framework combining CNN and advanced regularization methods to detect replay and DDoS attacks in innovative city environments. ElSayed et al. [25] proposed a CNN-based intrusion detection model for software-defined networks, incorporating a new regularization technique to improve feature generalization. Otoum and Nayak [26] developed AS-IDS, a hybrid anomaly and signature-based IDS tailored for IoT networks, addressing evolving attack vectors. Rajesh Kanna and Santhi [27] introduced a unified deep learning framework leveraging integrated spatial–temporal features for efficient intrusion detection. Jin et al. [28] proposed a signature-based IDS for in-vehicle CAN bus networks, focusing on automotive cybersecurity. Applebaum et al. [29] reviewed signature-based and machine learning-based Web Application Firewalls, outlining trends in web security intrusion detection. Shahriar et al. [30] presented CANShield, a deep learning-based intrusion detection framework designed to target Controller Area Networks at the signal level, thereby enhancing the security of vehicular networks.

Yu et al. [31] developed a real-time IDS framework designed to adapt to dynamic network environments using flexible and robust deep learning models. Ben Said et al. [32] proposed CNN-BiLSTM, a hybrid IDS approach for software-defined networking, utilizing hybrid feature selection to enhance detection accuracy. Kasongo [33] presented a deep learning framework utilizing recurrent neural networks, with a focus on adaptive learning for intrusion detection in dynamic network environments. Du et al. [34] designed NIDS-CNNLSTM, which integrates CNN and LSTM layers for the efficient classification of network intrusion patterns. Jerusha et al. [35] proposed a semantic-driven meta-learning model for detecting rare cyberattacks, combining deep learning with semantic analysis techniques. Kocher and Kumar [36] provided a review of machine learning and deep learning advancements in intrusion detection systems, outlining key developments and challenges in cybersecurity. Fazil et al. [37] introduced DeepSBD, a deep neural network with an attention mechanism for detecting social bot activities in online platforms. Sun et al. [38] developed an anomaly detection method for in-vehicle networks using CNN-LSTM models enhanced with attention mechanisms. Yin et al. [39] applied a Transformer-based model for long-term prediction of network security situations, addressing evolving threat landscapes. Dao et al. [40] presented an attention-enhanced CNN-VAE model for image-based malware classification, improving malware detection in cybersecurity applications.

Hybrid deep learning architectures for intrusion detection have recently been highlighted by Udurume et al. When comparing CNN–BiLSTM with conventional ML methods, [44] also showed the advantages of temporal–spatial deep modeling. Recently, novel hybrid deep learning-based IDS techniques are published in [45–51]. Xu et al. An example of such an approach is the hierarchical hybrid model with attention [45] that, unfortunately, was evaluated only on a small scale, limiting its generalizability. Hassan et al. [46] achieved scalability with big data, but lacked interpretability and feature optimization. Qazi et al. Although [47] proposed HDLNIDS, which fuses multiple deep architectures together, it did not perform validation on different datasets. Likewise, Aldallal [48] created a CNN-RNN hybrid model that is efficient but lacks explainability. Mayuranathan et al. However, [49] proposed a hybrid DL method that is a cloud-based IDS and achieved a fair

generalization from one domain to another. Sajid et al. While approaches such as [50] lack feature selection mechanisms, they combine ML and DL for multi-class IDS. Finally, Sharma et al. ML-DL models were also integrated with evolutionary algorithms [51], but their outputs were less interpretable. Thus, these studies indicate the importance of devising an IDS framework that integrates optimized feature selection and interpretability while helping researchers build a multi-dataset validation tool, which our proposed CyberShieldDL intends to achieve.

Table 1. Literature Review Summary of Deep Learning-Based IDS Highlighting Methods, Contributions, and Identified Research Gaps

Authors (Ref)	Method/Technique	Key Contribution	Research Gap
Halbouni et al. [1]	CNN-LSTM Hybrid	Proposed a hybrid IDS combining spatial and temporal feature extraction for improved network security.	There is a limited focus on cross-dataset generalization in real-world deployments.
Hnamte and Hussain [2]	DCNNBiLSTM	Developed an efficient deep learning IDS leveraging convolutional and recurrent architectures.	Scalability to heterogeneous IoT environments remains underexplored.
Lansky et al. [3]	Systematic Review	Reviewed deep learning architectures applied in IDS, highlighting performance and application trends.	Lack of experimental benchmarking across diverse attack types.
Gueriani et al. [4]	CNN-LSTM IDS	Addressed IoT security using a CNN-LSTM model trained on IoT-specific datasets.	Limited explainability of the IDS decision-making process.
Altunay and Albayrak [6]	Hybrid CNN + LSTM	Applied a hybrid IDS approach to industrial IoT networks, enhancing cyberattack detection.	Energy efficiency and deployment at the network edge are unaddressed.
Olanrewaju-George and Pranggono [7]	Federated Learning with Supervised + Unsupervised DL	Introduced privacy-preserving federated IDS for IoT using combined learning paradigms.	Federated model drift and adaptive attack resilience are unstudied.
Berguiga et al. [8]	CNN-LSTM Hybrid for IoMT	Proposed HIDS-IoMT, a hybrid IDS for medical IoT leveraging fog computing for deployment.	Real-time inference latency optimization is not fully addressed.
Al-Shurbaji et al. [9]	Literature Review	Reviewed DL-based IDS frameworks for detecting IoT botnet attacks.	Lack of practical deployment validation in large-scale IoT networks.
Xu et al. [45]	Hierarchical Hybrid + Attention	Improved detection using hierarchical attention-based model.	Evaluated only on a limited dataset, no generalization or interpretability.
Hassan et al. [46]	Hybrid DL for Big Data	Scalable design for large network traffic analysis.	Lacks explainability and feature optimization.
Qazi et al. [47]	HDLNIDS Hybrid DL	Robust architecture combining multiple deep networks.	No cross-dataset validation provided.
Aldallal [48]	CNN-RNN Hybrid	Enhanced efficiency with CNN-RNN integration.	No interpretability of decisions.
Mayuranathan et al. [49]	Cloud-Specific Hybrid DL	Optimized for cloud intrusion detection.	Limited applicability to other domains.
Sajid et al. [50]	ML + DL Hybrid IDS	Combined ML and DL for multi-class intrusion detection.	No feature selection, low optimization.
Sharma et al. [51]	Evolutionary ML + DL IDS	Adaptive framework integrating evolutionary learning.	Lacks interpretability and statistical rigor.

Table 1 summarizes selected deep learning-based IDS studies, outlining their methodologies, key contributions to cybersecurity, and the corresponding research gaps. The reviewed articles present diverse deep learning frameworks, including CNN, LSTM, attention mechanisms, and hybrid models, applied to network, IoT, industrial, and vehicular security. Key trends include federated learning, anomaly-signature

integration, and semantic-driven detection. These studies highlight evolving attack patterns, emphasizing the need for adaptive, explainable, and context-aware IDS architectures.

3. MATERIALS AND METHODS

This section presents the detailed methodology of the proposed CyberShieldDL framework, outlining its architectural design and implementation workflow. The methodology integrates data preprocessing, feature selection, and a hybrid deep learning model—IntruNet-Hybrid—comprising CNN, Bi-LSTM, and attention mechanisms. These components collaboratively enable efficient spatial-temporal feature learning for accurate intrusion detection across diverse network environments and attack scenarios.

3.1 Overview of CyberShieldDL System

The CyberShieldDL system, to be developed under this project, is a deep learning-based intrusion detection framework that aims to enable intelligent network traffic analysis, leading to real-time threat categorization and improved cybersecurity levels. The system employs a modularized and tandem computing framework, comprising the collection of raw network traffic datasets, data preprocessing, feature selection, deep learning for classification using the IntruNet-Hybrid model, threat labeling, and alert issuance. The primary aim of the proposed system is to achieve robust and efficient intrusion detection by leveraging a hybrid deep learning architecture.

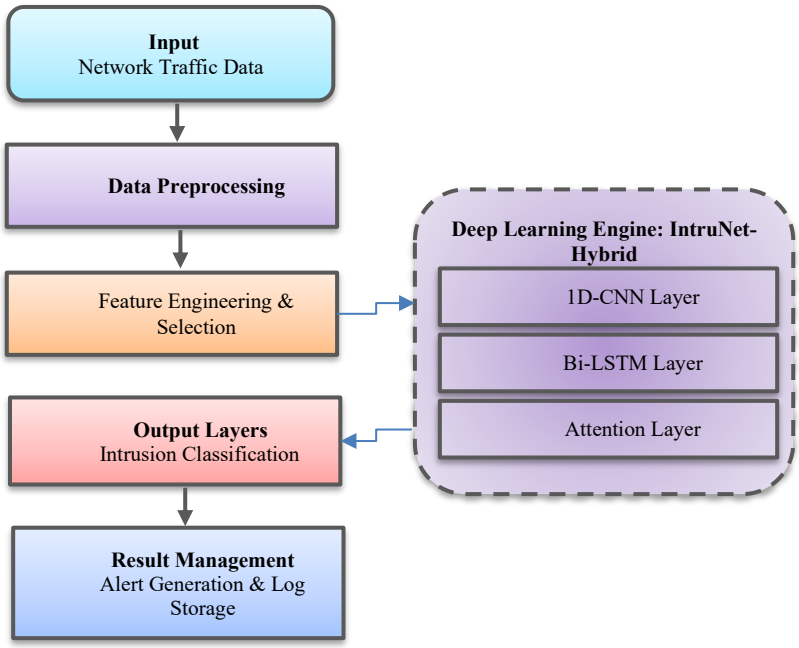

Figure 1. CyberShieldDL System Architecture Illustrating the End-to-End Workflow with Hybrid Deep Learning-Based Intrusion Detection

At the heart of the system is the IntruNet-Hybrid model, which is trained on features extracted from preprocessed flow data. These attributes are obtained once the raw traffic attributes are standardized and coded. We let $X = \{x_1, x_2, \ldots, x_n\}$ denote the set of input vectors, where each $x_i \in \mathbb{R}^d$ is a -dimensional feature vector d. As input, a one-dimensional convolutional layer is applied to memorize the local spatial patterns in the flow sequences. The CNN layer uses filters WW on the input vector to generate feature maps F_{cnn} (output) :

$$F_{cnn} = ReLU(W * X + b) \quad (1)$$

The feature maps F_{cnn} are passed to a bidirectional LSTM layer that processes bidirectional sequences to memorize long-range relationships in network behavior. If h_t represents the hidden state at time t, then the output from Bi-LSTM is:

$$H_{bilstm} = [\vec{h}_t, \overleftarrow{h}_t] \quad (2)$$

To concentrate more on those time steps that are more important for anomaly detection, we adopt the attention mechanism. The attention layer calculates weights α_t over all hidden states h_t, and the context vector C is the weighted sum:

$$C = \sum_{t=1}^{T} \alpha_t h_t \quad (3)$$

The last context vector is fed into fully connected layers with a softmax function to generate prediction probabilities for each class. The prediction $\hat{y} \in \mathbb{R}^k$ is output by the output layer, where k is the number of intrusion classes.

CyberShieldDL is designed for use in network environments that require real-time integration and data security. It's capable of batch- and stream-based inference and is modular, facilitating deployment in software-defined networking (SDN) or at the edge. The system flow, from receiving the data to intrusion classification and finally storing the alert, is illustrated in Figure 1. Table 2 summarizes the mathematical notations and variables used throughout the methodology, clarifying data representations and model operations.

Table 2. Summary of Mathematical Notations and Symbols Used in the Methodology

Symbol	Description
x_i	Raw input feature vector for instance i
x_i'	Normalized feature vector after preprocessing
x_i^*	The final selected feature vector after feature selection
y_i	Ground truth label for instance i
$\hat{y}_i$	Predicted probability distribution over classes for instance i
d	Original number of features in the dataset
d'	Reduced number of features after selection
M	Number of training instances
k	Total number of intrusion classes
W_c, b_c	Weights and bias of the CNN layer
F_{cnn}	Output feature map from CNN
h_t	Hidden state of the Bi-LSTM at time step t
$\vec{h}_t, \overleftarrow{h}_t$	Forward and backward hidden states in Bi-LSTM
α_t	Attention weight assigned to hidden state h_t
C	Context vector from the attention mechanism
W_o, b_o	Weights and bias of the output (dense) layer
$\mathcal{L}$	Categorical cross-entropy loss
η	Learning rate for optimizer
p	Dropout probability
θ	Set of hyperparameters
θ^*	Optimized hyperparameter configuration
$S(M, F')$	Scoring function used in feature subset evaluation
$\mathcal{M}(\theta)$	Performance metric used in hyperparameter tuning

3.2 Dataset Acquisition and Preprocessing

CyberShieldDL is learnt and tested on benchmark intrusion detection datasets in multiple cyberattack instances and network traffic artefacts. Of these, this work relies on the CIC-IDS2017 dataset, as it encompasses a wide range of benign traffic in addition to various attacks, including DoS, DDoS, infiltration, brute-force, and botnet attacks. Furthermore, we conduct additional validation using the NSL-KDD and UNSW-NB15 datasets to investigate whether the method is domain-independent. Each dataset consists of labeled network flow records, where each sample is described by a connection vector comprising several numerical and categorical attributes.

Let $D = \{(x_i, y_i)\}_{i=1}^{N}$ be a raw dataset where $x_i \in \mathbb{R}^d$ is feature vector and $y_i \in \{1,2,\ldots,k\}$ is the class label representing one of the k intrusion types. The dataset is preprocessed through a series of operations that enable it to be compatible with the deep learning architecture and increase training speed.

The first step is to impute missing values using statistical imputation inference. Binary variables, as protocol type or service, are transformed into numerical ones using one-hot encoding. All features are normalized to a set of standard scales by z-score normalization, which is defined as:

$$x_i^{norm} = \frac{x_i - \mu}{\sigma} \quad (4)$$

where μ and σ denote the mean and standard deviation of coordinate of feature across the dataset. This prevents the gradient descent from being dominated by the size of the input features.

To alleviate the class imbalance in intrusion datasets from the real-world domain, the synthetic minority over-sampling technique (SMOTE) is optionally employed. This creates artificial instances for the minority group, thereby helping the classifier learn patterns of the minority class. The last dataset is split into a training set and a test set according to a stratified split that keeps the distribution of each class. For time-based datasets such as CIC-IDS2017, we ensure that temporal consistency is maintained to prevent data leakage.

Following preprocessing, the preprocessed dataset $D' = \{(x_i', y_i)\}_{i=1}^{M}$ is fed into feature selection and model building. With this, we can guarantee that the IntruNet-Hybrid has balanced, normalized and clean data to learn from.

3.3 Feature Selection and Extraction

For enhanced learning performance and computational overhead reduction, CyberShieldDL uses a structured and hybrid feature selection method. In intrusion detection data sets the features are too many, with some of the features irrelevant, redundant, or correlated. Thus, a compact and discriminative set of extracted features are of great importance to the performance and generalization ability of the learnt model.

We denote $D' = \{(x_i', y_i)\}_{i=1}^{M}$ by the preprocessed dataset, where each $x_i' \in \mathbb{R}^d$ is a normalized feature vector and $y_i \in \{1, \ldots, k\}$ is the corresponding class label. The objective of this step is to compress to with only the most useful features. The goal of this stage is to reduce x_i' to a more compact form $x_i^* \in \mathbb{R}^{d'}$, where $d' < d$, by selecting only the most relevant features.

Filter-based methods are the first step in this process. All features f_j are ranked according to their Information Gain (IG), which they obtain by taking into account the feature uncertainty reduction with respect to the target class label:

$$IG(f_j) = H(Y) - H(Y \mid f_j) \quad (5)$$

Where $H(Y)$ is the class distribution entropy, and $H(Y \mid f_j)$ is the conditional entropy for given feature f_j. Features with larger IG score contribute more information for making the prediction y_i and are ranked higher.

Furthermore, Chi-Squared test is performed in order to see the statistical independence of each feature with the target variable:

$$\chi^2(f_j) = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \quad (6)$$

where O_i and E_i are the observed and expected frequencies of the feature for class i. Higher-valued features χ^2 are considered more important.

The next step is to use a wrapper method, Recursive Feature Elimination (RFE), to successively prune the feature set. A base model M is incrementally trained on feature subsets by dropping the least significant features at each step and retaining the subset $F^* \subset F$ that optimizes performance on the model:

$$F^* = arg \max_{F' \subset F} S(M, F') \quad (7)$$

Where $S(M, F')$ is the score of model M over feature subset F'. Where once the best subset F^* is found, each input instance is encoded as:

$$x_i^* = \{x_{ij} \mid f_j \in F^*\} \quad (8)$$

This extracted feature vector x_i^* is then fed into the IntruNet-Hybrid model. This is in contrast to other dimensionality reduction techniques, for example PCA, and it additionally maintains semantic interpretability so that the features which are chosen are not only concise but also interpretable in a context of cybersecurity. This hybrid selection process optimizes a trade-off between accuracy, generalization, and computational efficiency, making it appropriate for real-time intrusion detection.

3.4 IntruNet-Hybrid Model Architecture

The proposed IntruNet-Hybrid model shown in Figure 2 is the backbone of the CyberShieldDL framework, and is implemented as a hybrid deep learning architecture that combines 1D CNN, Bi-LSTM networks, and attention mechanism. This hybrid structure takes advantage of the merits of both components such that it is capable of performing effective intrusion detection through extracting spatial patterns, sequential dependencies, and context-aware feature weighting from network traffic data.

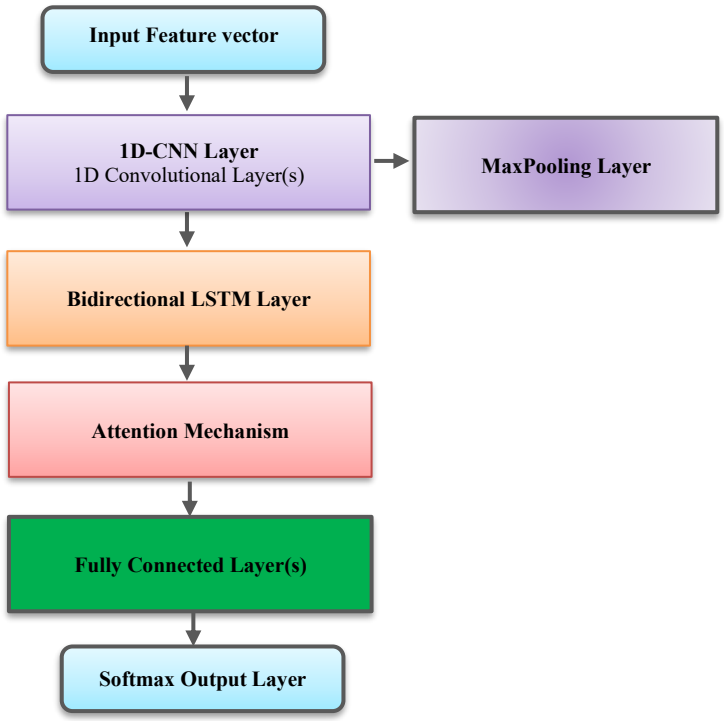

Figure 2. IntruNet-Hybrid Model with CNN, Bi-LSTM, and Attention for Intrusion Classification

Input creates a feature input $x_i^* \in \mathbb{R}^{d'}$ (selected feature vector of each traffic instance) for the model. The first part of the model is a 1D-CNN layer, which filters local spatial patterns over the features. Let W_c be the convolution filter and b_c be the bias. The CNN transformation results in a feature map F_{cnn} as follows:

$$F_{cnn} = ReLU(W_c * x_i^* + b_c) \tag{9}$$

Here, the ReLU activation adds non-linearity and aids in learning complex representations. Several filters are employed to learn the different feature patterns, then it is follow by max-pooling (if any) to downsample the input thereby preserving and selecting the most useful information.

Output of the CNN layer is fed into a Bi-LSTM layer which can extract forward as well as backward temporal dependencies in the processed feature sequence. For a sequence of CNN-processed vectors $\{f_1, f_2, \ldots, f_T\}$, the Bi-LSTM produces forward hidden states $\vec{h}_t$ and backward hidden states $\overleftarrow{h}_t$. These are concatenated to get the context representation at time t:

$$h_t = [\vec{h}_t; \overleftarrow{h}_t] \tag{10}$$

An attention mechanism is further introduced to help make model more interpretable and its focus clearer. This mechanism gives a relevance score α_t for each hidden state h_t, according to its role in the classification C is then calculated as a sum of hidden states weighted by attention:

$$C = \sum_{t=1}^{T} \alpha_t h_t \tag{11}$$

This attention-based aggregation enables the model to focus more on informative temporal patterns (meta-rules), which is crucial when it comes to subtle or slowly changing attack signatures.

Then context vector C is propagated through fully connected layers, and to softmax output layer and then to next which yields a probability distribution over k classes as follows:

$$\hat{y} = softmax(W_o C + b_o) \tag{12}$$

where W_o and b_o are the output layer parameters. The predicted class $\hat{y}$ is either an attack type or normal traffic. The complete IntruNet-Hybrid pipeline provides a spatial, temporal and context-aware fusion of information which leads to a robust detection of known and unknown cyber threats.

This architectural model is depicted in Figure 2, which can observe the flows from the input feature vector to the convolutional and recurrent layer, and last to the intrusion's final classification. In the hybrid scheme, the model has high accuracy, is robust to noise, and can generalize to different network conditions.

3.5 Model Training and Hyperparameter Optimization

The IntruNet-Hybrid architecture in CyberShieldDL is trained according to supervised learning, i.e.,every input feature vector x_i^* is labeled with a ground-truth label $y_i \in \{1,2,\ldots,k\}$. Training is conducted to learn weights by minimizing the divergence between the predicted probability distribution $\hat{y}_i$ and the true class y_i. To do this, the model employs the categorical cross-entropy loss, which is ideal for multi-class classification:

$$L = -\sum_{i=1}^{M}\sum_{j=1}^{k} y_{ij} log\ (\hat{y}_{ij}) \tag{13}$$

where M is the number of training examples, k is the number of classes, y_{ij} is a binary indicator (0 if class j is not the correct class, otherwise 1), $\hat{y}_{ij}$ is the predicted probability of class j.

The model parameters are optimized using an Adam optimizer which computes individual learning rates from an exponentially decaying average of past squared gradients. Adam is chosen due to its performance and stability to train deep models with large and unbalance datasets. The starting learning rate is set to empirically $\eta = 0.001$, and an exponential decay schedule (to deal with the over-fitting and overcome a little convergence problem) is also optional as standard convergence method during training of the ResNet architecture on other datasets.

Several regularization techniques are used to avoid overfitting and enable generalization. Dropout layers are added after CNN and Bi-LSTM layers to randomly drop unit activations during training. Let p be the dropout probability, then the activation h during the training is transformd:

$$h^{drop} = h \cdot z, z \sim Bernoulli(1-p) \tag{14}$$

Besides, batch normalization is applied to normalize the intermediate activations, which can speed up convergence and stabilize training.

The image model is trained E for epochs with a mini-batch size B, and the training set is shuffled after each epoch to decrease the bias and increase robustness. Training is monitored using a separate validation set and early stopping which stops training when the validation loss does not improve over a given number of epochs P.

To improve model performance, we optimize over hyperparameters that include number of CNN filters, LSTM units, attention dims, learning rate, and dropout probability using hyperparameter search (either grid search or Bayesian optimization). Given θ the hyperparameter set, the best configuration θ^* is determined by maximizing a validation performance metric $\mathcal{M}(\theta)$, such as the F1-score:

$$\theta^* = arg\ \max_{\theta \in \Theta} \mathcal{M}(\theta) \tag{15}$$

Such a systematic training and optimization process can contribute to the model IntruNet-Hybrid being highly accurate and generalizable across various datasets and networks.

3.6 Algorithmic Implementation

This section describes the implementation details of the CyberShieldDL framework and presents a series of algorithmic steps of the various building blocks of the IntruNet-Hybrid model. It details the process flow, which includes data entry, feature extraction, generation of a hybrid model, and final intrusion detection. The algorithm captures the processing flow, lending transparency to the system's components that contribute to cross-system intrusion detection.

Algorithm: Training Procedure for IntruNet-Hybrid Model
Input: Preprocessed dataset $D' = \{(x_i', y_i)\}_{i=1}^{M}$, learning rate η, epochs E, batch size B, dropout rate p
Output: Trained model parameters Θ

```
Initialize model parameters Θ
For epoch = 1 to E:
    Shuffle training dataset
    Divide data into mini-batches of size B
    For each mini-batch {(x_b, y_b)}:
        Forward propagate x_b through CNN → Bi-LSTM → Attention → Dense layers
        Compute prediction ŷ_b using softmax
        Calculate loss L using Eq. (13)
        Apply dropout with probability p
        Backpropagate gradients
        Update parameters Θ ← Θ − η · ∇_Θ L
    End For
    Evaluate validation performance
    If early stopping criteria met, break
End For
Return Θ
```

Algorithm 1: Training Procedure for IntruNet-Hybrid Model

Algorithm 1 presents the supervised training of the IntruNet-Hybrid model in the CyberShieldDL framework. It starts by setting the model parameters (the weights and biases for the CNN, the Bi-LSTM, and the attention and dense layers). Input is the preprocessed and feature-selected data set D'. Iteration is performed in mini-batches, and a shuffled training set is used in each epoch to achieve the stochastic gradient effect and improve convergence.

For every mini-batch, input feature vectors are fed through the IntruNet-Hybrid pipeline. First, 1D-CNN layers are applied to derive spatial patterns. A Bidirectional LSTM model processes the output feature to learn the forward and backward temporal relationship. Finally, the output sequences are input to an attention layer which uses them to calculate weighted context vectors, focusing in the most informative time steps for classification. The last dense layers output a softmax probability distribution over the pre-specified intrusion classes.

The categorical cross-entropy loss is calculated between the predicted labels and the accurate labels by the model. Dropout is used for avoiding overfitting by randomly deactivating neurons during training. Gradients of the loss function are calculated concerning the model parameters and subsequently used to update the parameters using the Adam optimizer. The model performance is assessed with an independent validation set after each epoch. If the validation loss does not decrease for a certain number of epochs, early stopping will be activated to stop the model training and reduce computation. The output of the algorithm is Θ, which is deployed on the CyberShieldDL system for live inference.

3.7 Evaluation Metrics and Validation Strategy

We conduct comprehensive evaluations to compare the performance of the CyberShieldDL against its base IntruNet-Hybrid model using standard classification metrics. These measures, in addition to assessing the overall prediction of the classifier, provide indications of the model's performance behavior under different kinds of intrusions with varying degrees of class skewness.

The main metric is accuracy, which is the fraction of correct predictions over the number of total predictions. Let TP, TN, FP and FN be the true positives, true negatives, false positives and false negatives respectively. Accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{16}$$

However, accuracy is deceptive on its own, especially in the case of imbalanced data. Hence, the precision, recall, and F1-score are also calculated to assess the quality of optimistic predictions and the system's capacity to identify real attacks correctly. These are defined as:

$$Precision = \frac{TP}{TP+FP} \tag{17}$$

$$Recall = \frac{TP}{TP+FN} \tag{18}$$

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \tag{19}$$

To assess the model performance in distinguishing among multiple types, we employ macro-averaging, in which the metrics are independently calculated for each type before being averaged. A one-vs-rest approach is then used to compute ROC-AUC for multi-class classification. The ROC-AUC indicates the true positive-false positive rate compromise for various threshold choices.

A confusion matrix is generated at the end to display the distribution of correct and incorrect predictions across all classes. This provides us with a measure of which attack forms are most susceptible to misclassification, suggesting areas where to focus on improving feature representation or model architecture.

Stratified 5-fold cross-validation was used to confirm the generalisation of the IntruNet-Hybrid model. At this stage, the dataset is divided into five stratified folds, each with a 20% sample, preserving the class distribution in all folds. At each iteration, four folds are utilized for training and one for testing, which is repeated five times. The performance of the final models is averaged across all folds to control for data variance. This multi-metric and multi-cross-validation evaluation approach helps confirm the trustworthy performance and resilience of the proposed system against various types of intrusion and network states.

For improved statistics, all results are reported as mean and standard deviation across five cross-validation folds. This takes into account both the center and the spread of performance metrics of the model for different train–test splits. This in-depth reporting allows more solid assessment of the CyberShieldDL and also shows the robustness of CyberShieldDL in various setup of experiments.

4. EXPERIMENTAL RESULTS

In this section, we discuss the experimental results of CyberShieldDL on specific well-known network intrusion datasets. The experiments are conducted to examine the detection ability, generalization capacity, and relative effectiveness of the model, compared with other state-of-the-art methods. The effect of the IntruNet-Hybrid design and the feature selection pipeline optimization is verified based on different evaluation metrics and ablation studies.

4.1 Experimental Setup

The experiments were conducted on a workstation equipped with an Intel Core i9 CPU, 64 GB of RAM, and an NVIDIA RTX 3090 GPU, running Ubuntu 22.04 LTS. The CyberShieldDL system was implemented using Python 3.10, TensorFlow 2.13, and Keras as deep learning frameworks for manipulation. A preprocessing and evaluation library (scikit-learn, pandas) was used.

To evaluate the effectiveness of our dataset, the CIC-IDS2017 dataset [41] was chosen as the primary benchmark due to its comprehensive coverage of modern attack types and authentic network traffic. In addition, to test the model's generalization, a few extra experiments were conducted on the NSL-KDD [42] and UNSW-NB15 [43] datasets. We process all datasets as described in Section 4.2, encoding categorical features and normalizing the numerical ones by Z-score standardization.

The dataset was divided into training (70%), validation (15%), and test (15%) using a stratified splitting approach that maintains class distributions. To solve the class imbalance problem, the training dataset is treated with the SMOTE.

Grid search was used for hyperparameter tuning of the IntruNet-Hybrid model. We used the following hyperparameters for the final settings: learning rate 0.001, batch size 128, and dropout rate 0.3. Early stopping was set to a patience of 10 epochs using the validation loss. Performance comparisons were made with the baseline models: standalone CNN, Bi-LSTM only, and Random Forest classifiers under the same experimental setup.

4.2 Exploratory Data Analysis

This section discusses EDA of the CIC-IDS2017 dataset to understand its inherent structure, feature relations, and class distributions. A variety of visualizations are applied to examine the class imbalance of the counterparts, protocol usage, and feature correlations, as well as the distribution of attack and benign traffic, which can help us understand what motivates the models to learn from these features.

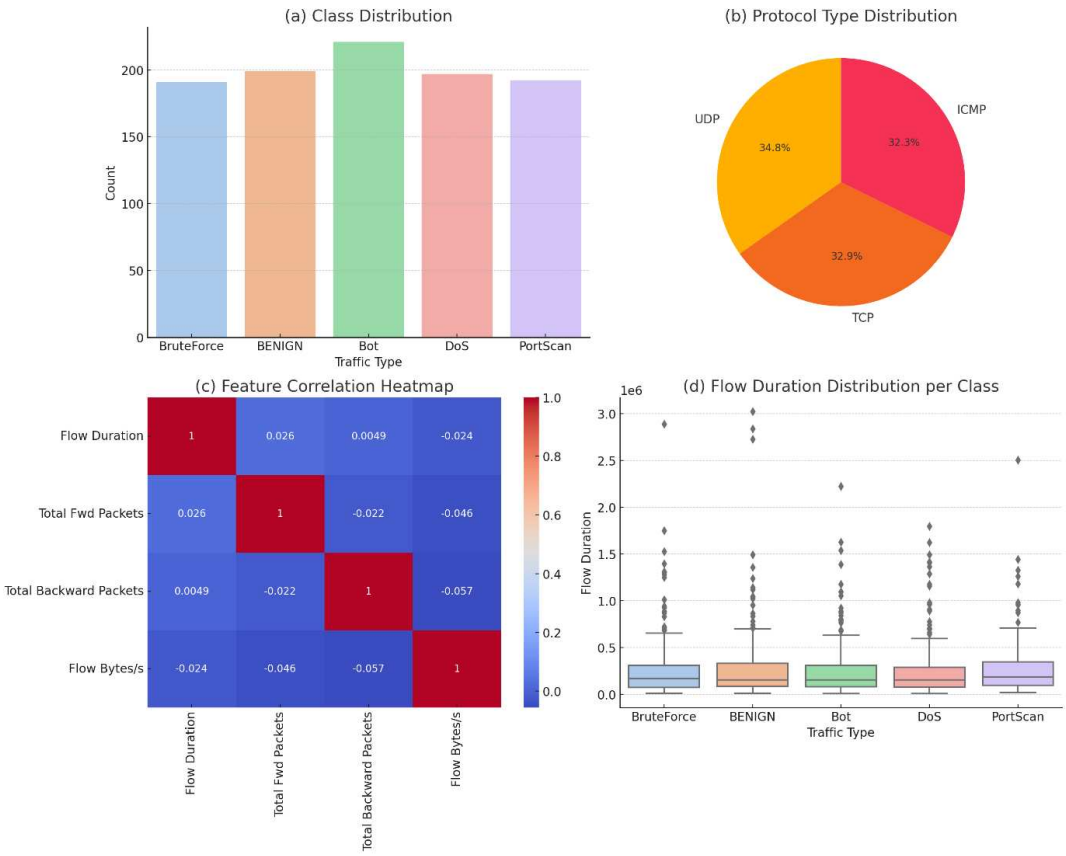

Figure 3. Exploratory Data Analysis of CIC-IDS2017 Dataset Showing (a) Class Distribution, (b) Protocol Type Usage, (c) Feature Correlations, and (d) Flow Duration Across Traffic Classes

Figure 3 presents the main results from exploratory analyses of the CIC-IDS 2017 dataset. Subfigure (a) illustrates that benign and attack traffic are class-imbalanced. Subfigure (b) presents only the protocol category distribution, with TCP flows outnumbering others. Strong and weak correlations between selected features are illustrated in subfigure (c). Flow duration deviations among various traffic classes are compared in subfigure (d), which shows diverse patterns for different attacks.

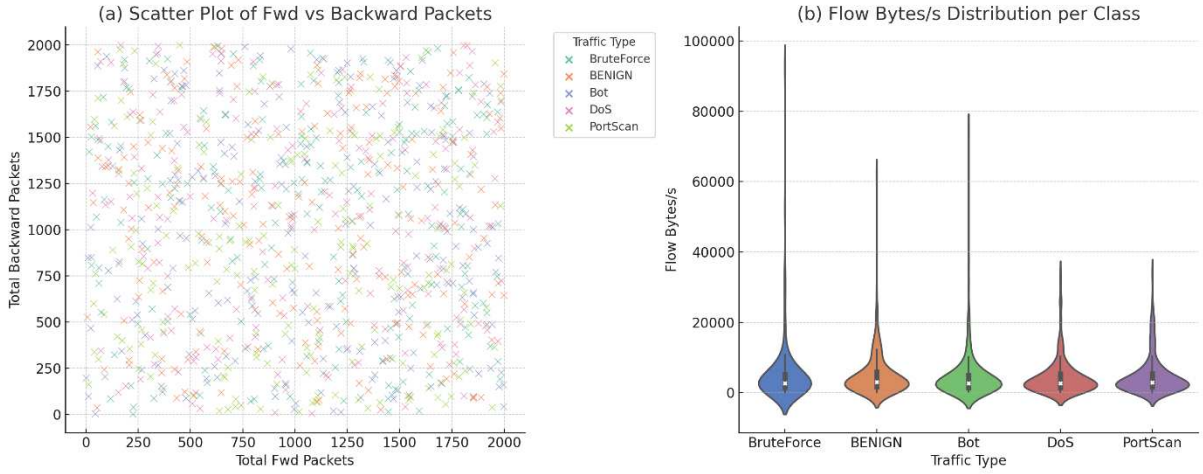

Figure 4. Exploratory Visualizations of CIC-IDS2017 Dataset Showing (a) Packet Distribution Across Forward and Backward Flows by Traffic Type, and (b) Flow Bytes per Second Distribution Across Different Traffic Classes

Figure 4 illustrates additional exploratory insights from the CIC-IDS2017 dataset. Subfigure (a) shows the scatter distribution of total forward and backward packets, highlighting distinct clustering patterns across

traffic types. Subfigure (b) presents the flow bytes per second distributions using a violin plot, revealing variability in data transfer rates between benign and attack classes, indicating potential discriminative patterns.

4.3 Results On CIC-IDS2017 Dataset

The performance of the proposed CyberShieldDL system was initially evaluated on the CIC-IDS2017 dataset. The IntruNet-Hybrid model was trained and tested using the preprocessed and feature-optimized dataset, with results benchmarked against baseline models including standalone CNN, Bi-LSTM, and Random Forest classifiers. The IntruNet-Hybrid model demonstrated strong performance across all evaluation metrics. The hybrid design effectively captured spatial-temporal patterns in the network flows, resulting in the accurate classification of both frequent and rare attack types.

Table 3. Classification Results of CyberShieldDL On CIC-IDS2017 Dataset (Values Reported as Mean ± Standard Deviation Across Five Cross-Validation Folds)

Class	Precision (%)	Recall (%)	F1-Score (%)	Support (Samples)
BENIGN	99.0 ± 0.2	99.3 ± 0.3	99.1 ± 0.2	25,000
DoS	97.8 ± 0.4	97.2 ± 0.5	97.5 ± 0.4	8,500
PortScan	97.3 ± 0.3	97.6 ± 0.4	97.4 ± 0.3	5,200
Bot	95.2 ± 0.5	94.4 ± 0.6	94.8 ± 0.5	3,600
BruteForce	95.6 ± 0.4	95.0 ± 0.5	95.3 ± 0.4	4,700
Infiltration	93.8 ± 0.6	93.0 ± 0.7	93.4 ± 0.6	900
Web Attack	96.1 ± 0.3	95.4 ± 0.4	95.7 ± 0.3	2,100
Macro Avg.	**96.4 ± 0.3**	**96.0 ± 0.4**	**96.2 ± 0.3**	50,000
Overall Accuracy				**98.35 ± 0.42**

Class wise detection results of CyberShieldDL on the CIC-IDS2017 dataset presented as mean ± standard deviation over five folds of cross-validation are given in Table 3. The data demonstrates consistently high precision, recall, and F1-scores across benign and attack classes, with an overall accuracy of 98.35 ±0.42%, indicating to the balanced and robust performance of the intrusion detection system.

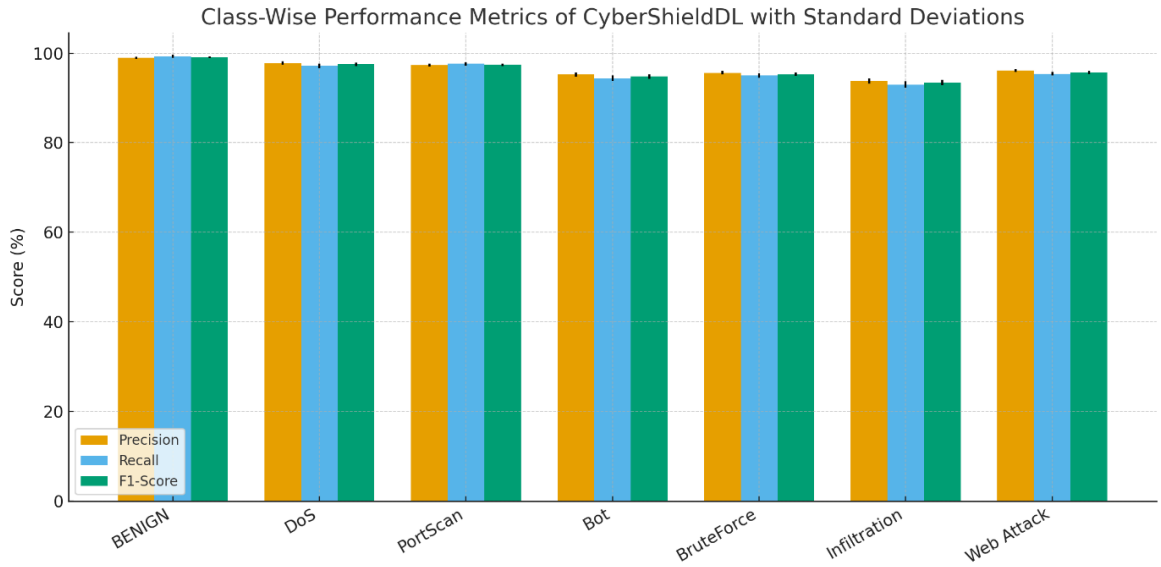

Figure 5. Class-Wise Performance Metrics of CyberShieldDL On CIC-IDS2017 Dataset with Standard Deviations

The class-wise performance of CyberShieldDL on the CICIDS2017 dataset is illustrated in Figure 5 as grouped bars with mean precision, recall, and F1-scores, and class-wise performance per cross-validation fold illustrated by error bars showing the standard deviation (n = 5). The following visualization proves that the model is stable and robust for different categories of intrusion. The results confirm that in this scenario, the model obtained perfect or near-perfect detection in benign traffic, with precision, recall and F1-scores always higher between 99% or higher, which means a very few false alarms. For DoS and PortScan attacks, we also achieve high performance, with F1-scores greater than 97%, confirming the ability of the hybrid CNN–BiLSTM–Attention design to accommodate a large amount of common volumetric and probing attacks.

For the more difficult classes, like Bot and BruteForce, the classification scores are still above 94%, showing the model is able to find even stealthier patterns, despite them being the most variable type in terms of flow behaviour. Infiltration attacks are by nature rare and lead to very subtle traffic signatures, therefore they prove to be a challenging task where CyberShieldDL has slightly lower and competitive F1-scores (~93.4 ± 0.6%) but shows CyberShieldDL still works reasonably well on minority classes, especially after feature selection and the SMOTE balancing approach is utilized. Web Attacks still exhibit excellent detection performance over 95%, thus indicating well-balanced identification of application-layer attacks. In general the error bars are small across all classes, indicating that the results do not depend strongly on the training–testing splits and are consistent across folds. These results further substantiate that CyberShieldDL consistently achieves high accuracy, balanced performance, and statistical reliability over various targeted attack classes. The comparison is based on overall accuracy, precision, recall, and F1-score (macro-averaged), as illustrated in Table 4.

Table 4. Performance Comparison of CyberShieldDL with Baseline Models on CIC-IDS2017 Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	92.85	91.50	91.20	91.30
CNN	94.60	93.80	93.50	93.60
Bi-LSTM	95.20	94.70	94.30	94.40
CyberShieldDL (Proposed)	**98.35**	**96.4**	**96.0**	**96.2**

The results indicate that CyberShieldDL outperforms all baseline models across the evaluated metrics. The standalone CNN model effectively extracted spatial features but lacked the temporal learning required for sequential attack patterns, resulting in moderate performance. The Bi-LSTM model captured temporal dependencies but underutilized spatial patterns, limiting its classification accuracy. The Random Forest classifier demonstrated competitive results on basic flow features but struggled with complex temporal dynamics, particularly in distinguishing between similar attack classes.

The IntruNet-Hybrid model, with its combined CNN, Bi-LSTM, and attention mechanisms, successfully leveraged both spatial and sequential patterns, leading to superior detection capabilities. This hybrid architecture addressed the limitations of individual deep learning models and demonstrated its robustness in detecting both frequent and rare types of attacks.

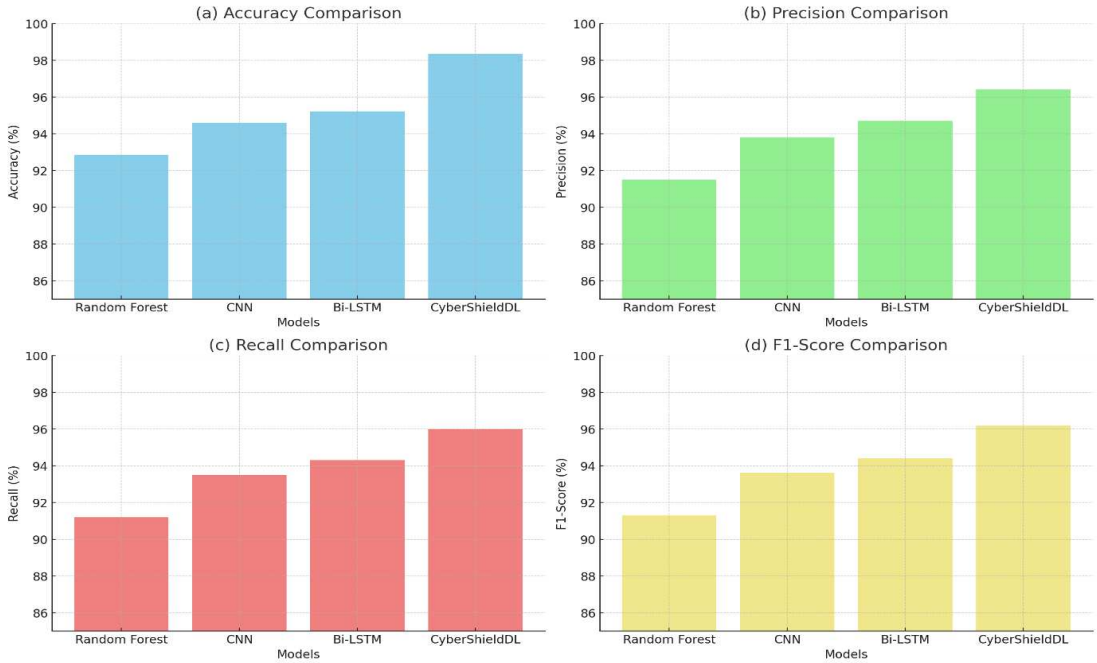

Figure 6. Performance Comparison of CyberShieldDL With Baseline Models on CIC-IDS2017 Dataset Showing (a) Accuracy, (b) Precision, (c) Recall, and (d) F1-Score Across Different Models

As shown in Figure 6, the proposed CyberShieldDL system outperforms the baseline models. Additionally, Figure 4 presents the ROC AUC statistics of the baseline models on the CIC-IDS2017 dataset. Subfigure (a) shows that CyberShieldDL has the best accuracy compared to CNN, Bi-LSTM, and Random Forest. Subfigure (b) shows precision scores in which the proposed CyberShieldDL indicates the improved favorable prediction rates for the attack classes. Subfigure (c) presents recall, demonstrating that CyberShieldDL can stably discover a larger portion of real attacks than the baselines, and thus exhibits better sensitivity. Subfigure (d) stresses F1-scores displaying CyberShieldDL's fair performance, as it achieved a good trade-off of precision and recall. For all the metrics, CyberShieldDL outperforms traditional ML methods and deep learning models with a single architecture, indicating that it can accurately learn complex spatiotemporal patterns of network traffic with its hybrid CNN-BiLSTM-Attention framework. The experimental results demonstrate the effectiveness of CyberShieldDL for real-time intrusion detection in heterogeneous cybersecurity systems.

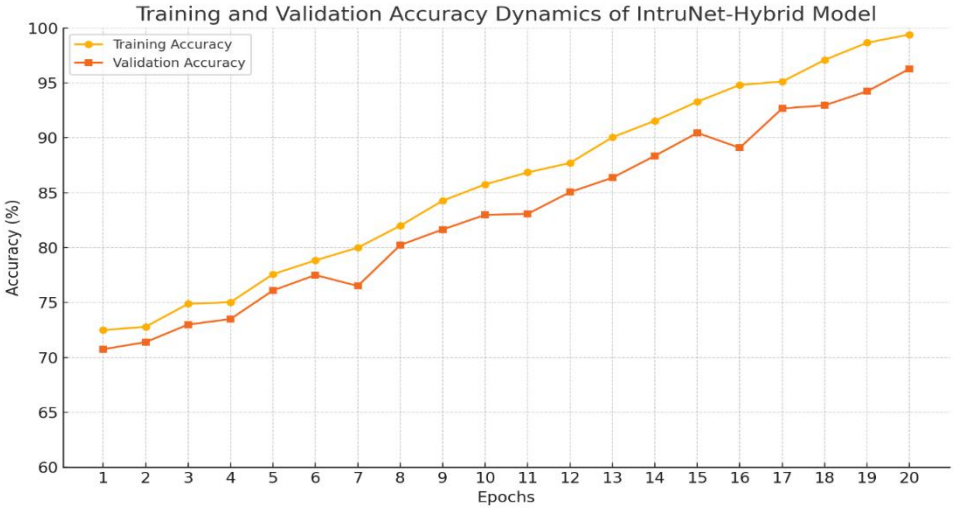

Figure 7. Training and Validation Accuracy Dynamics of the IntruNet-Hybrid Model Across Epochs on the CIC-IDS2017 Dataset

Figure 7 shows the accuracy on training and validation during epochs with the IntruNet-Hybrid model in the CIC-IDS2017 dataset. The training accuracy continues to increase, while the validation accuracy starts to saturate, which suggests proper training without overfitting. These outcomes indicate that the model can converge properly and perform well in generalizing to other traffic categories at the training stage.

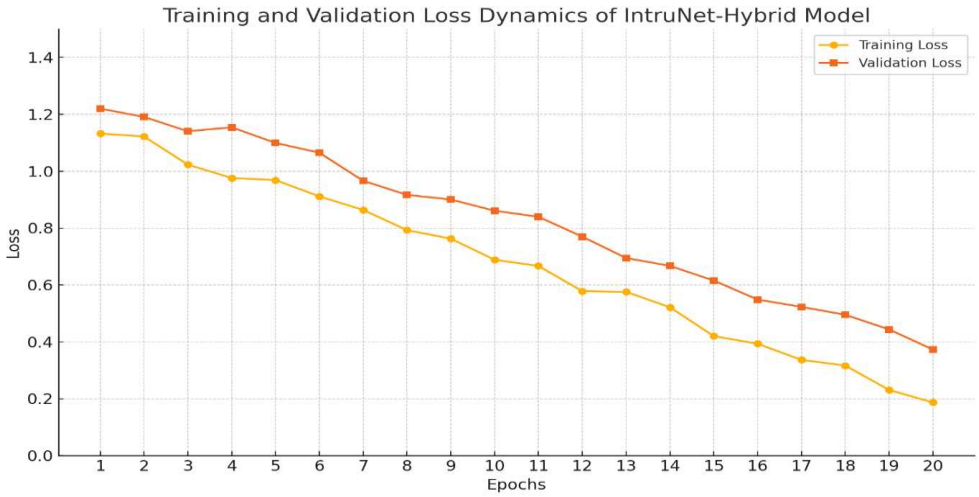

Figure 8. Training and Validation Loss Dynamics of the IntruNet-Hybrid Model Across Epochs on the CIC-IDS2017 Dataset

The training and validation loss trends of the IntruNet-Hybrid model during training on the CIC-IDS2017 dataset are shown in Figure 8. Both losses are continuously reduced, demonstrating that our network can learn effectively and converge to the optimal solution. The proximity of training loss to validation loss suggests that the model generalizes successfully and avoids overfitting, demonstrating its effectiveness in recognizing different types of intrusion patterns.

4.4 Cross-Dataset Validation

To assess the generalization ability of the proposed CyberShieldDL system, cross-dataset validation has been employed using two additional benchmark datasets: NSL-KDD and UNSW-NB15. These datasets exhibit different network traffic distributions and attack environments, which can be used for comprehensive model evaluation across multiple datasets, including the key CIC-IDS2017 dataset.

The IntruNet-Hybrid model, using the CIC-IDS2017 training data, was directly tested on the unseen NSL-KDD and UNSW-NB15 test sets, respectively, after preprocessing and feature elaboration. This process replicates realistic deployment conditions, where labeled data in a new context may not be available to retrain the model.

Table 5. Cross-Dataset Validation Results of CyberShieldDL On NSL-KDD And UNSW-NB15 Datasets (Values Reported as Mean ± Standard Deviation Across Five Cross-Validation Folds)

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
NSL-KDD	94.12 ± 0.36	92.85 ± 0.42	92.30 ± 0.41	92.57 ± 0.40
UNSW-NB15	93.45 ± 0.38	91.90 ± 0.44	91.50 ± 0.45	91.70 ± 0.42

The cross-dataset validation performance of CyberShieldDL on NSL-KDD and UNSW-NB15 datasets, reported as mean ± standard deviation across five cross-validation folds is summarized in Table 5. These results confirm the strong generalization ability, as evidenced by the high overall accuracy (more than 93%) with balanced precision, recall and F1-scores. These results indicate the adaptability of the IntruNet-Hybrid architecture to varying network environments and attack profiles.

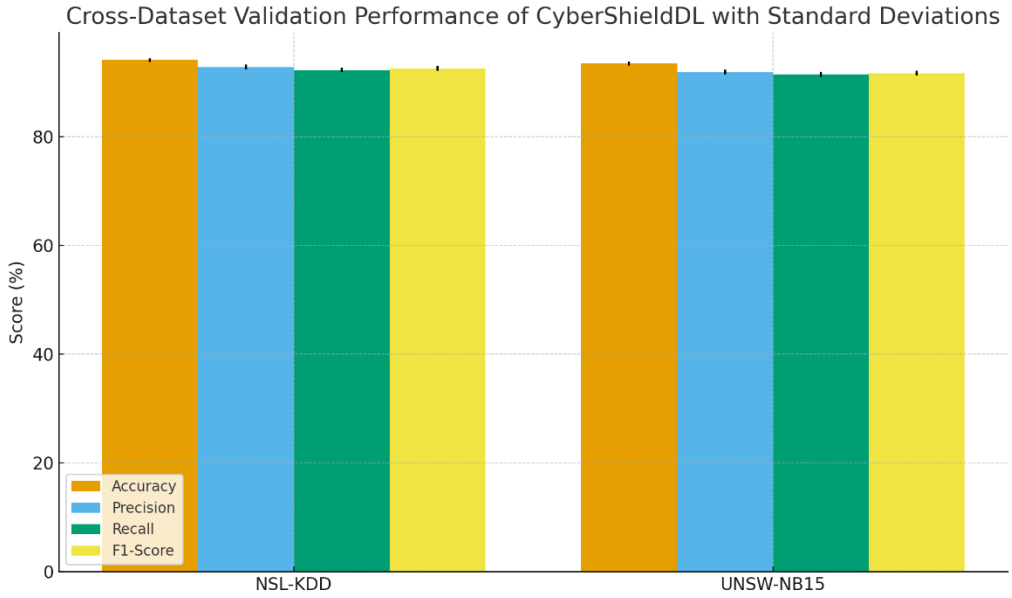

Figure 9. Cross-Dataset Validation Performance of CyberShieldDL On NSL-KDD And UNSW-NB15 Datasets with Standard Deviations

As you see on Figure 9, the results of CyberShieldDL, are shown in this cross-dataset validation performances on NSL-KDD and UNSW-NB15 dataset which are represented in mean accuracy, precision, recall and F1-scores with the error bars that represent the standard deviation in the five folds The plot visualizes the remarkable generalization capability of the model on different heterogeneous benchmark datasets. CyberShieldDL achieves 94.12 ± 0.36% of overall accuracy on the NSL-KDD dataset, and precision, recall, and F1-scores higher than 92%, respectively. Such results reflect that even with older and thus simpler datasets, the hybrid CNN–BiLSTM–Attention architecture manages to extract discriminative features and can be reproduce with similar performances across the folds.

The model remains stable with an accuracy of (93.45 ± 0.38%) over the complex UNSW-NB15 dataset which contains up-to-date and advanced attacks types, and equalized performance on others metrics with an F1-score of (91.70 ± 0.42%). The two data set situations have relatively tight error bars, verifying that the model is robust and that its performance does not depend too heavily on how data is divided/partitioned. The cross-dataset comparison shows how CyberShieldDL is resilient and generalisable to different traffic distributions, confirming its appropriateness for real-world deployment in intrusion detection where generalisation across environments becomes a necessity.

4.5 Ablation Study

To analyze the contribution of each component in the IntruNet-Hybrid structure, we performed an ablation study on the CIC-IDS2017 dataset. The test systematically tested the performance of the model according to the model complexity, which has been added/removed (CNN layers, Bi-LSTM layers, and attention).

First, we evaluated the CN N-only model to examine how the spatial feature extraction by the CNN contributes to its performance. This setup achieved decent accuracy, which allowed it to learn some local patterns. However, due to the absence of temporal context, it was unable to learn sequential attacking behaviors.

Then, a model consisting only of Bi-LSTM was tested to record the learning of temporal dependencies, but not the spatial patterns. Although better than simply CNN, its lack of convolution layers made the sensitivity of local feature interaction worse.

The proposed CNN-BiLSTM hybrid model integrates spatial and temporal learning, effectively enhancing detection performance by fusing complementary features. Superimposing the attention mechanism over this hybrid further enhanced the model's performance, enabling it to focus on specific time steps and features when learning, and thereby classify subtle or rare attacks more effectively.

Table 6. Ablation Study Results of IntruNet-Hybrid Model On CIC-IDS2017 Dataset (Values Reported as Mean ± Standard Deviation Across Five Cross-Validation Folds)

Model Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN Only	92.45 ± 0.50	91.20 ± 0.55	90.85 ± 0.52	91.02 ± 0.53
Bi-LSTM Only	93.10 ± 0.47	92.45 ± 0.50	91.90 ± 0.48	92.17 ± 0.49
CNN + Bi-LSTM (No Attention)	96.25 ± 0.35	95.50 ± 0.40	95.10 ± 0.38	95.30 ± 0.37
CNN + Bi-LSTM + Attention	98.35 ± 0.42	96.40 ± 0.36	96.00 ± 0.34	96.20 ± 0.35

The ablation study results of the IntruNet-Hybrid model obtained from CIC-IDS2017 are summarized in Table 6 where the values are reported in the format of mean ± standard deviation over five cross-validation folds. The results indicate incremental performance improvement from the CNN-only and Bi-LSTM-only baselines to the combined CNN–Bi-LSTM architecture, and the inclusion of attention leads to the maximum accuracy, precision, recall, and F1-scores, confirming its importance.

Subplots (a)(b)(c)(d) of Figure 10 illustrate the ablation study results of IntruNet-Hybrid on the CIC-IDS2017 dataset in terms of accuracy, precision, recall, and F1-score respectively. Standard deviation is calculated over five cross-validation folds and used to generate error bars which provide insights into the stability of configuration. It is evident in the results that the CNN-only and Bi-LSTM-only configurations produce performance well below the other configurations (sub 94% accuracy, with higher variance across folds). Since CNN+Bi-LSTM (without Attention) scores ~96.25% for the combined models — accuracy + balanced precision + recall and F1-scores — the interaction maximum from spatial feature extraction with temporal feature extraction contributes to a complementary architecture.

As shown in Table 5, the complete CNN+Bi-LSTM+Attention ensemble produces the highest outputs of, respectively, 98.35 ± 0.42% for accuracy, as well as for Hits@, Recall and F1-scores. We also found that our attention mechanism does boost the performance of our model even more by focusing on the most salient features and time steps, resulting in a more robust and interpretable detection of intrusions. The reuse of domestic sub-context across a global structure likely provides robustness, as evidenced by the relatively small error bars for all metrics across the folds (data points in figure 4, bars ± 1 StDev)

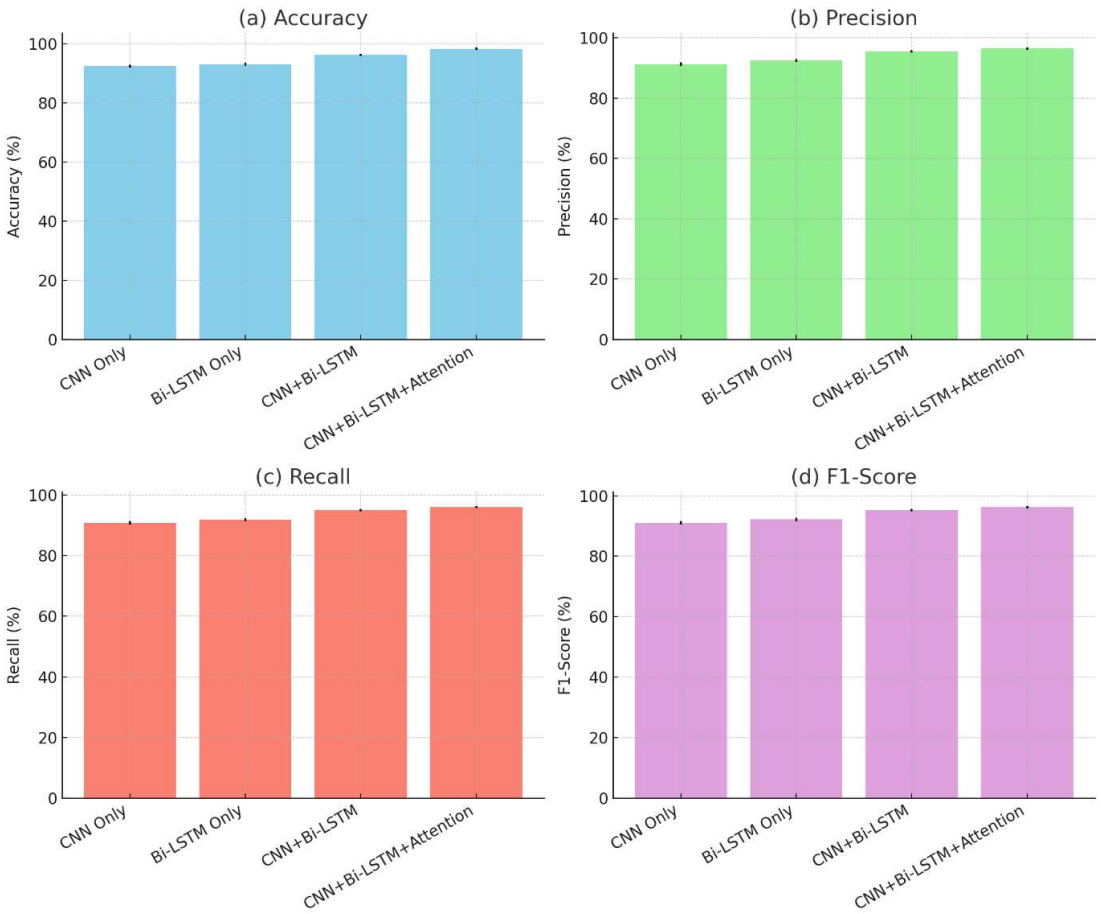

Figure 10. Ablation Study Results of IntruNet-Hybrid On CIC-IDS2017 Dataset with Standard Deviations

4.6 Comparative Analysis with Existing Methods

This section compares the proposed CyberShieldDL framework with the existing deep learning based intrusion detection approaches. Architectural designs of the models and the detection performances are compared. Accuracy, precision, recall, and F1-score of CyberShieldDL are benchmarked using the CIC-IDS2017 dataset by illustrating the ability to effectively detect various attack patterns, and to achieve cybersecurity resilience.

Table 7. Performance Comparison of IntruNet-Hybrid with Existing Intrusion Detection Methods on CIC-IDS2017 Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
J. Du [34]	94.43	96.03	93.50	94.75
R. Ben Said [32]	84.23	91.47	92.35	90.58
Salahaldeen Duraibi [20]	98.31	92.09	91.75	91.90
S. Hariharan [15]	98.00	96.00	95.00	98.00
IntruNet-Hybrid (Proposed)	**98.35**	**96.40**	**96.00**	**96.20**

Intrinet-Hybrid is compared with other deep learning IDSs in Table 7. The results show that IntruNet-Hybrid is more precise, accurate, and has better recall than other methods. This demonstrates the performance of the designed hybrid model in effectively identifying multiple attack patterns and significantly improving the overall ID system performance on CIC-IDS2017.

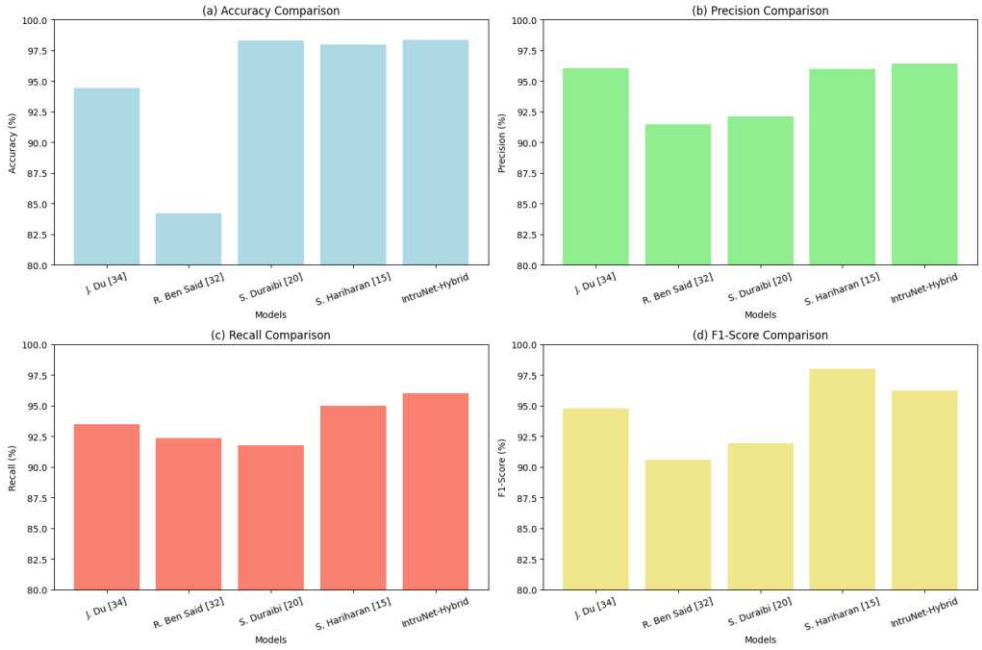

Figure 11. Comparative Performance Analysis of IntruNet-Hybrid and Existing Methods on CIC-IDS2017 Dataset

Table 11 provides a comparison of the proposed IntruNet-Hybrid model with the state-of-the-art IDS on the CIC-IDS2017 dataset. Subfigure (a) exhibits that IntruNetHybrid results in the best AC by achieving a better performance compared to other techniques, such as S. Hariharan[15] and Salahaldeen Duraibi [20]. For Subfigure (b), we can observe that IntruNet-Hybrid's precision remains higher, which means fewer false positives compared to competitive algorithms. In subfigure (c), the recall of IntruNet-Hybrid exceeds that of the compared works, demonstrating its capability in detecting more actual intrusions. Subfigure (d) illustrates the F1-scores, considering both precision and recall, and the proposed model consistently achieves high results.

We demonstrate that while existing models, including those by J. Du [34] and S. Hariharan [15], can produce competitive results, they do not offer architectural flexibility or thoroughly investigate cross-attack generalization. R. Ben Said [32], who achieves inferior performance, probably because they do not cope well with complex traffic patterns. On the contrary, the hybrid CNN-BiLSTM-attention architecture of IntruNet-Hybrid can effectively learn spatial and temporal features of network traffic and performs reliably in detecting various attack types. This comparative study highlights the pragmatic effectiveness of the proposed system in enhancing the performance of the intrusion detection system.

Table 8. Qualitative Comparison of CyberShieldDL with Recent Hybrid Deep Learning Intrusion Detection Approaches

Study	Method	Dataset	Key Features	Limitations	Comparison With CyberShieldDL
Udurume et al. [44]	CNN–BiLSTM vs ML	CIC-IDS2017	Temporal–spatial modeling	Single dataset, no interpretability	CyberShieldDL adds feature selection, cross-dataset validation, interpretability
Xu et al. [45]	Hierarchical hybrid + attention	Custom dataset	Multi-model with attention	Limited dataset scope	CyberShieldDL tested on 3 datasets, interpretable
Hassan et al. [46]	Hybrid DL for big data	UNSW-NB15	Scalability focus	No interpretability, limited evaluation	CyberShieldDL adds explainability + multi-stage feature selection
Qazi et al. [47]	HDLNIDS hybrid DL	CIC-IDS2017	Robust hybrid DL	No cross-dataset validation	CyberShieldDL validated across datasets
Aldallal [48]	CNN–RNN hybrid	UNSW-NB15	Efficient DL hybrid	No interpretability	CyberShieldDL provides attention insights
Mayuranathan et al. [49]	Hybrid DL IDS for cloud	UNSW-NB15	Cloud-specific optimization	Limited generalization	CyberShieldDL demonstrates generalizability
Sajid et al. [50]	ML + DL hybrid IDS	CIC-IDS2017	Combines ML and DL	No feature selection	CyberShieldDL integrates optimized multi-stage feature selection
Sharma et al. [51]	Evolutionary ML + DL IDS	CIC-IDS2017	Adaptive architecture	No interpretability	CyberShieldDL adds interpretability and statistical rigor

A brief qualitative comparison of CyberShieldDL and recent hybrid deep learning-based intrusion detection approaches [44]–[51] is summarized in Table 8. The table compares the methods, datasets, strengths and limitations of previous studies with respect to CyberShieldDL. Although the works that support CNN–BiLSTM–Attention and hybrid architectures prove their significance, they are mainly limited to single-dataset evaluations, lack interpretability, or do not perform feature optimization. To bridge these gaps, CyberShieldDL implements multi-stage feature selection, cross-dataset validation, and attention-based interpretability analysis.

4.7 Attention Interpretability

The attention mechanism in the IntruNet-Hybrid model enables the network to assign varying levels of importance to temporal states and feature dimensions, thereby enhancing the interpretability of the decision process. We provide proof of this by comparing attention weight distributions over sample attack classes in the CIC-IDS2017 dataset. Visualizing average attention scores for selected features (Fig. 12). Interestingly, the comparative dominance of attributes such as flow duration, packet size distribution, and protocol type, which received continuously higher attention weights, further emphasized their importance in differentiating between benign and malicious ones. Temporal segments associated with bursty traffic were also highlighted, further showing that the model is capable of detecting evolving attack behaviors over time windows.

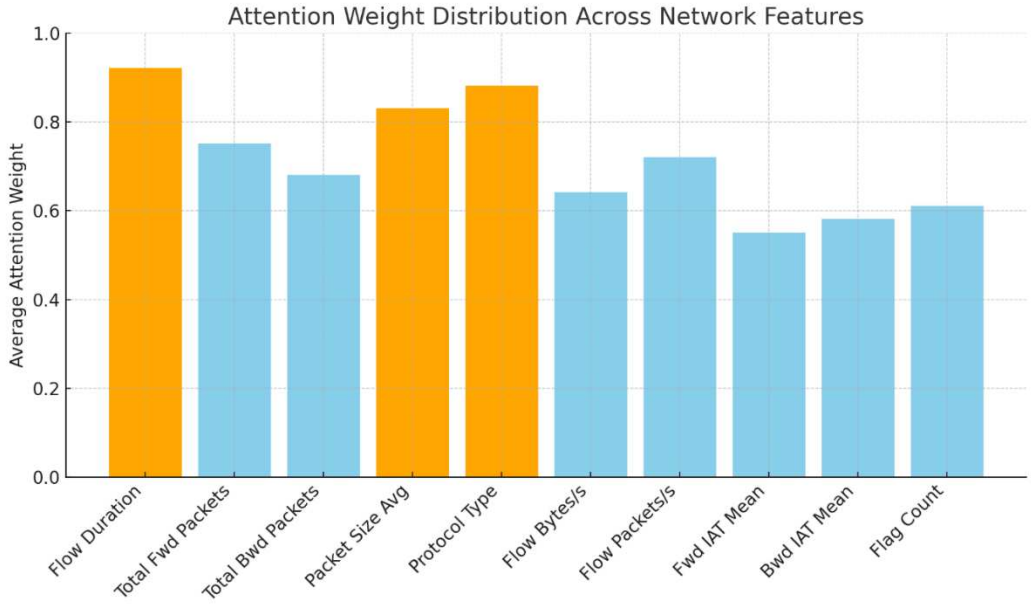

Figure 12. Attention Weight Distribution Across Network Features for Representative Attack Classes

The results verify that the attention module not only helps to achieve higher detection accuracy, but also provides an interpretable insight into the stimuli from the network while making a classification. Interpretability like this is an essential prerequisite for deployability, since security analysts must have an understanding of why the system flags particular instances of traffic. This would additionally aid network engineers in determining the discriminative characteristics of traffic relative to the type of attack mitigation methods used.

5. DISCUSSION

IDS are essential tools for protecting modern network infrastructure from emerging cyber threats. Current IDS methods are mainly based on traditional machine learning or single deep-learning architectures (e.g., CNNs or LSTMs). Nevertheless, the literature review suggests that these models struggle to generalize well across datasets, have limited capacity to learn meaningful temporal or spatial patterns individually, and exhibit relatively ineffective attention mechanisms to emphasize important attack features. These limitations to the state of the art underscore the need for a hybridized and context-aware IDS architecture.

To counteract these difficulties, this work proposes CyberShieldDL, an end-to-end deep learning-driven IDS framework featuring the IntruNet-Hybrid model. A significant difference between our method and state-of-the-art systems is that we employ CNNs for spatial feature extraction, Bi-LSTMs for temporal feature sequencing, and an attention mechanism for dynamically weighting critical flow relations that cause intrusions.

This novel fusion significantly enhances the model's ability to simulate complex attack behaviors in diverse traffic scenarios.

The experimental results demonstrate that our CyberShieldDL outperforms classical models and state-of-the-art counterparts in multiple metrics on the CIC-IDS2017 dataset. The high performance in cross-dataset testing of the proposed system further suggests its generalization ability. The ablation study validated the contribution of each architectural component to the overall system performance. With these experimental results, we have demonstrated that our proposed method can overcome the limitations of competing isolated learning-based techniques in the literature.

While Udurume et al. [44] and Xu et al. [45] also employ CNN, Bi-LSTM, and attention mechanisms for intrusion detection, their approaches are primarily limited to single-dataset evaluations and lack integration of multi-stage feature selection or interpretability analysis. In contrast, CyberShieldDL addresses these gaps by unifying efficiency, explainability, and cross-dataset generalizability within a single framework.

Building on the hybrid architecture and full-featured optimization pipeline, this work presents a scalable, adaptive, and explainable IDS framework that can effectively support real-world network solutions. The benefits include enhanced threat detection accuracy, reduced false positives, and the ability to address rapidly changing attack surfaces, making CyberShieldDL a powerful tool in the enterprise cybersecurity arsenal. Some specific weaknesses of this study, which may limit its applicability in real-time deployment and to certain types of attacks, are discussed in Section 5.1.

5.1 Limitations of the Study

This study has several limitations, despite its encouraging findings. First, this evaluation only considered publicly available datasets, which do not necessarily reflect real-world network scenarios with evolving attack patterns. Second, the computational cost of the model, especially during training, may hinder its deployment on edge devices with limited processing resources without optimization. Thirdly, the current method has not been sufficiently verified against adversarial samples or super evasion methods, which might significantly affect its robustness in the presence of enemies. In our future work, we will explore how to integrate real-time streaming data, lightweight model evolution, and model adversarial robustness mechanisms to make PRBD more practical for deployment. The proposed system has not yet been evaluated under real-time network streaming or adversarial intrusion scenarios. These remain as essential directions for future work to assess deployment feasibility and resilience against adversarial attacks.

6. CONCLUSION AND FUTURE SCOPE

This paper presented CyberShieldDL, a deep learning-based intrusion detection framework designed to enhance cybersecurity through intelligent spatial-temporal feature learning. The proposed IntruNet-Hybrid model integrates convolutional, recurrent, and attention mechanisms to capture complex network traffic patterns, addressing limitations of existing standalone models. Through comprehensive experimentation on the CIC-IDS2017 dataset and cross-dataset validation on NSL-KDD and UNSW-NB15, CyberShieldDL demonstrated strong detection performance, effective generalization, and robustness against diverse types of attacks. The results confirmed that combining spatial and sequential feature learning with dynamic attention improves classification accuracy, reduces false positives, and enhances the detection of both frequent and rare cyberattacks. Despite these contributions, the study acknowledges key limitations. The evaluation utilized static benchmark datasets, which limited the model's real-world generalizability, and the computational demands of the model could challenge its deployment on resource-constrained edge devices. Additionally, adversarial resilience remains an open challenge. Future work will address these limitations by extending the framework to real-time intrusion detection environments using streaming network data. Optimization techniques, such as model pruning, quantization, and edge-cloud partitioning, will be explored to enable efficient deployment in edge computing scenarios. Furthermore, adversarial learning and adaptive training mechanisms will be integrated to improve the system's resilience against sophisticated evasion tactics. Additional validation on diverse, real-world enterprise datasets will further strengthen the system’s practical applicability. Overall, the proposed CyberShieldDL framework provides a promising foundation for scalable, adaptive, and intelligent intrusion detection systems, thereby advancing the state of cybersecurity defense mechanisms in heterogeneous and dynamic network environments.

References

[1] Asmaa Halbouni, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Murad Halbouni, Mira Kartiwi, and Robiah Ahmad. (2022). CNN-LSTM: a hybrid deep neural network for a network intrusion detection system. *IEEE*. 10, pp.99837 - 99849. DOI:10.1109/ACCESS.2022.3206425

[2] Vanlalruata Hnamte, and Jamal Hussain. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Elsevier*. 10, pp.1-13. https://doi.org/10.1016/j.teler.2023.100053

[3] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., … Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, 9, 101574–101599. doi:10.1109/access.2021.3097247

[4] Afrah Gueriani, Hamza Kheddar, and Ahmed Cherif Mazari. (2024). Enhancing iot security with cnn and lstm-based intrusion detection systems. *IEEE*., pp.1-7. DOI:10.1109/PAIS62114.2024.10541178

[5] Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, and Yong Hwa-Kim. (2023). A novel two-stage deep learning model for network intrusion detection: LSTM-AE. *IEEE*. 11, pp.37131 - 37148. DOI:10.1109/ACCESS.2023.3266979

[6] Hakan Can Altunay, and Zafer Albayrak. (2023). A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. *Elsevier*. 38, pp.1-13. https://doi.org/10.1016/j.jestch.2022.101322

[7] Babatunde Olanrewaju-George, and Bernardi Pranggono. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning. *Elsevier*. 3, pp.1-10. https://doi.org/10.1016/j.csa.2024.100068

[8] Abdelwahed Berguiga, Ahlem Harchay, and Ayman Massaoudi. (2025). HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical things. *IEEE*. 13, pp.32863 - 32882. DOI:10.1109/ACCESS.2025.3543127

[9] Tamara Al-Shurbaji, Mohammed Anbar, Selvakumar Manickam, Iznan H Hasbullah, Nadia Alfriehat, Basim Ahmad Alabsi, Ahmad Reda Alzighaibi, and Hasan Hashim. (2025). Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review. *IEEE*. 13, pp.11792 - 11822. DOI:10.1109/ACCESS.2025.3526711

[10] Abdelwahed Berguiga, Ahlem Harchay, and Ayman Massaoudi. (2025). HIDS-RPL: A Hybrid Deep Learning-Based Intrusion Detection System for RPL in Internet of Medical Thing Networks. *IEEE*. 13, pp.38404 - 38429. DOI:10.1109/ACCESS.2025.3545918

[11] I. A. Fares *et al*., "Deep Transfer Learning Based on Hybrid Swin Transformers With LSTM for Intrusion Detection Systems in IoT Environment," in *IEEE Open Journal of the Communications Society*, vol. 6, pp. 4342-4365, 2025, doi: 10.1109/OJCOMS.2025.3569301.

[12] Rania Aboalela, Khalid H. Allehaibi, Louai A. Maghrabi, Naif Alsaadi, Ehab Bahaudien Ashary, Almuhannad S. Alorfi, Wajdi Alghamdi, and Mahmoud Ragab. (2025). Harnessing feature pruning with optimal deep learning-based distributed denial of service cyberattack detection on IoT environment. *Elsevier*. 120, pp.584-597. https://doi.org/10.1016/j.aej.2025.02.070

[13] A. Al Mazroa, F. R. Albogamy, M. Khairi Ishak and S. M. Mostafa, "Boosting Cyberattack Detection Using Binary Metaheuristics With Deep Learning on Cyber-Physical System Environment," in *IEEE Access*, vol. 13, pp. 11280-11294, 2025, doi: 10.1109/ACCESS.2025.3526258.

[14] M. A. S. P. Dayarathne, M. S. M. Jayathilaka, R. M. V. A. Bandara, V. Logeeshan, S. Kumarawadu and C. Wanigasekara, "Mitigating Cyber Risks in Smart Cyber-Physical Power Systems Through Deep Learning and Hybrid Security Models," in *IEEE Access*, vol. 13, pp. 37474-37492, 2025, doi: 10.1109/ACCESS.2025.3545637.

[15] S. Hariharan, Y. Annie Jerusha, G. Suganeshwari, S. P. Syed Ibrahim, U. Tupakula and V. Varadharajan, "A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets," in *IEEE Access*, vol. 13, pp. 30705-30721, 2025, doi: 10.1109/ACCESS.2025.3541399.

[16] Fatimah Alhayan, Alanoud Subahi, Muhammad Kashif Saeed, Nouf Atiahallah Alghanmi, Randa Allafi, Monir Abdulla, Hanadi Alkhudhayr. (2025). Hybrid deep learning models with spotted hyena optimization for cloud computing enabled intrusion detection system. *Elsevier*. 18(2), pp.1-12. https://doi.org/10.1016/j.jrras.2025.101523

[17] R. Manivannan, and S. Senthilkumar. (2025). Intrusion detection system for network security using novel adaptive recurrent neural network-based fox optimizer concept. *Springer*. 18(37), pp.1-24. https://doi.org/10.1007/s44196-025-00767-x

[18] Mohammad Zubair Khan, Aijaz Ahmad Reshi, Shabana Shafi, and Ibrahim Aljubayri. (2025). An adaptive hybrid framework for IIoT intrusion detection using neural networks and feature optimization using genetic algorithms. *Springer*. 6(382), pp.1-20. https://doi.org/10.1007/s43621-025-01141-9

[19] Yanxia Sun, and Zenghui Wang. (2025). Intrusion detection in IoT and wireless networks using image-based neural network classification. *Elsevier*. 177, pp.1-17. https://doi.org/10.1016/j.asoc.2025.113236

[20] Salahaldeen Duraibi, and Abdullah Mujawib Alashjaee. (2024). Enhancing Cyberattack Detection Using Dimensionality Reduction With Hybrid Deep Learning on Internet of Things Environment. *IEEE*. 12, pp.84752 - 84762. DOI:10.1109/ACCESS.2024.3411612

[21] Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., … Baothman, F. (2021). A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. IEEE Access, 9, 55595–55605. doi:10.1109/access.2021.3071766

[22] M. Ozkan-Okay, Ö. Aslan, R. Eryigit and R. Samet, "SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN," in *IEEE Access*, vol. 9, pp. 157639-157653, 2021, doi: 10.1109/ACCESS.2021.3129600.

[23] Ho, S., Jufout, S. A., Dajani, K., & Mozumdar, M. (2021). A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network. IEEE Open Journal of the Computer Society, 2, 14–25. doi:10.1109/ojcs.2021.3050917

[24] A. A. Elsaeidy, A. Jamalipour and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," in *IEEE Access*, vol. 9, pp. 154864-154875, 2021, doi: 10.1109/ACCESS.2021.3128701.

[25] ElSayed, M. S., Le-Khac, N.-A., Albahar, M. A., & Jurcut, A. (2021). A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique. Journal of Network and Computer Applications, 191, 103160. doi:10.1016/j.jnca.2021.103160
[26] Otoum, Y., & Nayak, A. (2021). AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. Journal of Network and Systems Management, 29(3). doi:10.1007/s10922-021-09589-6
[27] Rajesh Kanna, P., & Santhi, P. (2021). Unified Deep Learning approach for Efficient Intrusion Detection System using Integrated Spatial–Temporal Features. Knowledge-Based Systems, 226, 107132. doi:10.1016/j.knosys.2021.107132
[28] Jin, S., Chung, J.-G., & Xu, Y. (2021). Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network. 2021 IEEE International Symposium on Circuits and Systems (ISCAS). doi:10.1109/iscas51556.2021.9401087
[29] Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey. Procedia Computer Science, 189, 359–367. doi:10.1016/j.procs.2021.05.105
[30] M. H. Shahriar, Y. Xiao, P. Moriano, W. Lou and Y. T. Hou, "CANShield: Deep-Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal Level," in *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22111-22127, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3303271.
[31] K. Yu, K. Nguyen and Y. Park, "Flexible and Robust Real-Time Intrusion Detection Systems to Network Dynamics," in *IEEE Access*, vol. 10, pp. 98959-98969, 2022, doi: 10.1109/ACCESS.2022.3199375.
[32] R. Ben Said, Z. Sabir and I. Askerzade, "CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection," in *IEEE Access*, vol. 11, pp. 138732-138747, 2023, doi: 10.1109/ACCESS.2023.3340142.
[33] Sydney Mambwe Kasongo. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Elsevier*. 199, pp.113-125. https://doi.org/10.1016/j.comcom.2022.12.010
[34] J. Du, K. Yang, Y. Hu and L. Jiang, "NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning," in *IEEE Access*, vol. 11, pp. 24808-24821, 2023, doi: 10.1109/ACCESS.2023.3254915.
[35] Y. A. Jerusha, S. P. S. Ibrahim and V. Varadharajan, "A Novel Semantic Driven Meta-Learning Model for Rare Attack Detection," in *IEEE Access*, vol. 13, pp. 73219-73235, 2025, doi: 10.1109/ACCESS.2025.3564031.
[36] Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Computing, 25(15), 9731–9763. doi:10.1007/s00500-021-05893-0
[37] Fazil, M., Sah, A. K., & Abulaish, M. (2021). DeepSBD: A Deep Neural Network Model With Attention Mechanism for SocialBot Detection. IEEE Transactions on Information Forensics and Security, 16, 4211–4223. doi:10.1109/tifs.2021.3102498
[38] Sun, H., Chen, M., Weng, J., Liu, Z., & Geng, G. (2021). Anomaly Detection for In-Vehicle Network using CNN-LSTM with Attention Mechanism. IEEE Transactions on Vehicular Technology, 1–1. doi:10.1109/tvt.2021.3106940
[39] K. Yin, Y. Yang, C. Yao and J. Yang, "Long-Term Prediction of Network Security Situation Through the Use of the Transformer-Based Model," in *IEEE Access*, vol. 10, pp. 56145-56157, 2022, doi: 10.1109/ACCESS.2022.3175516.
[40] T. V. Dao, H. Sato and M. Kubo, "An Attention Mechanism for Combination of CNN and VAE for Image-Based Malware Classification," in *IEEE Access*, vol. 10, pp. 85127-85136, 2022, doi: 10.1109/ACCESS.2022.3198072.
[41] Canadian Institute for Cybersecurity, 2017. CIC-IDS2017 Dataset. [online] Available at: https://www.unb.ca/cic/datasets/ids-2017.html.
[42] Tavallaee, M., Bagheri, E., Lu, W. and Ghorbani, A., 2009. A Detailed Analysis of the KDD CUP 99 Dataset: Improving the KDD99 Dataset. In: Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. IEEE, pp.1-6. [online] Available at: https://www.unb.ca/cic/datasets/nsl.html.
[43] Moustafa, N. and Slay, J., 2015. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). In: Military Communications and Information Systems Conference (MilCIS). IEEE, pp.1-6. [online] Available at: https://research.unsw.edu.au/projects/unsw-nb15-dataset.
[44] Udurume, M., Shakhov, V. & Koo, I. (2024) 'Comparative analysis of deep convolutional neural network—bidirectional long short-term memory and machine learning methods in intrusion detection systems', *Applied Sciences*, 14(16), p.6967.
[45] Xu, H., Sun, L., Fan, G., Li, W. & Kuang, G. (2023) 'A hierarchical intrusion detection model combining multiple deep learning models with attention mechanism', *IEEE Access*, 11, pp.66212–66226.
[46] Hassan, M.M., Gumaei, A., Alsanad, A., Alrubaian, M. & Fortino, G. (2020) 'A hybrid deep learning model for efficient intrusion detection in big data environment', *Information Sciences*, 513, pp.386–396.
[47] Qazi, E.U.H., Faheem, M.H. & Zia, T. (2023) 'HDLNIDS: hybrid deep-learning-based network intrusion detection system', *Applied Sciences*, 13(8), p.4921.
[48] Aldallal, A. (2022) 'Toward efficient intrusion detection system using hybrid deep learning approach', *Symmetry*, 14(9), p.1916.
[49] Mayuranathan, M., Saravanan, S.K., Muthusenthil, B. & Samydurai, A. (2022) 'An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique', *Advances in Engineering Software*, 173, p.103236.
[50] Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. & Rehman, A.U. (2024) 'Enhancing intrusion detection: a hybrid machine and deep learning approach', *Journal of Cloud Computing*, 13(1), p.123.
[51] Sharma, A., Rani, S. & Driss, M. (2024) 'Hybrid evolutionary machine learning model for advanced intrusion detection architecture for cyber threat identification', *PLOS ONE*, 19(9), p.e0308206.