International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Hybrid Deep Learning Framework with Multi-Scale Temporal Convolutions, Attention, and Uncertainty Quantification for Network Intrusion Detection

Yakub Reddy[1]. K , G. Shankar Lingam[2]

Submitted: 08/01/2024 **Revised:** 18/02/2024 **Accepted:** 26/02/2024

Abstract. This paper presents a novel hybrid deep learning framework for network intrusion detection that addresses the limitations of existing systems in detecting both known and novel attacks. The proposed architecture integrates six sequential modules: data preprocessing, adaptive feature selection, Multi-Scale Temporal Convolutional Network (MS-TCN), Bidirectional LSTM with attention mechanism, ensemble anomaly detector, and uncertainty-aware classifier. The framework employs parallel 1D convolution layers with varying kernel sizes (3, 5, 7) to capture temporal patterns of different complexities, while BiLSTM processes sequential dependencies bidirectionally. An ensemble of three anomaly detectors (Isolation Forest, DBSCAN, One-Class SVM) handles zero-day attacks through majority voting. Experimental results demonstrate superior performance with 91% accuracy, 0.9783 ROC-AUC, and 0.9895 average precision. The adaptive feature selection reduces dimensionality by 50% while maintaining discriminative power. The model effectively balances precision (0.99 for attacks) and recall (0.81 for attacks), showing robust generalization without overfitting across ten training epochs.

Keywords. *Network Intrusion Detection, Hybrid Deep Learning, Multi-Scale Temporal Convolutional Network, Bidirectional LSTM, Ensemble Anomaly Detection.*

1. Introduction

In the era of hyperconnectivity and massive digital transformation, network infrastructures have become the lifeline of every sector, including finance, healthcare, transportation, and government. As organizations increasingly rely on interconnected devices, cloud services, and intelligent systems, the attack surface for malicious actors has grown exponentially. Cyberattacks such as Distributed Denial of Service (DDoS), ransomware, phishing, and zero-day exploits are not only increasing in frequency but also evolving in sophistication. This alarming trend necessitates the development of more intelligent, adaptive, and robust Network Intrusion Detection Systems (NIDS) that can identify and neutralize potential threats in real-time.

Traditional intrusion detection systems, often based on rule sets or classical machine learning algorithms, struggle to cope with the dynamic nature of modern cyber threats. These systems typically rely on handcrafted features and static patterns, rendering them ineffective against unknown or polymorphic attacks. Furthermore, they often generate high false positive rates and are unable to provide insights into the confidence of their predictions, a critical requirement in high-stakes environments. Consequently, researchers and practitioners have increasingly turned toward deep learning to address the limitations of conventional approaches.

1Research Scholar, Department of Computer Science and Engineering, Chaitanya Deemed to be university, Warangal, Telangana, India
Orcid:0009-0002-5998-4166
2Professor, Department of Computer Science and Engineering, Chaitanya deemed to be University ,Warangal, Telangana, India.
Orcid:0009-0005-6809-6728
Yakubreddy1245@gmail.com 1 , shankar@chaitanya.edu.in2

Deep learning models have shown great promise in the field of intrusion detection due to their ability to learn hierarchical representations directly from raw or minimally processed data. Architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers have demonstrated remarkable success in capturing spatial, temporal, and contextual patterns in network traffic data. However, standalone models often fall short when tasked with detecting nuanced attack behaviors that may manifest across multiple temporal or spatial resolutions.

In response to these challenges, we propose a Novel Hybrid Deep Learning Framework [5, 6] that integrates the strengths of multiple deep learning paradigms, anomaly detection algorithms, and interpretability techniques to deliver a comprehensive, accurate, and robust intrusion detection solution. The proposed architecture is designed to overcome five fundamental limitations of existing methods:

1. Most current models either use simple LSTM or 1D CNNs [7 and 8] to capture sequential dependencies. These fail to effectively capture multi-scale temporal patterns in network traffic. Our framework addresses this by introducing Multi-Scale Temporal Convolutional Networks (MS-TCNs), which apply multiple convolutional filters of varying lengths in parallel, allowing the system to simultaneously learn both short-term and long-term temporal dependencies.
2. Recurrent models often suffer from vanishing gradients and limited attention to distant dependencies. To tackle this, we incorporate a Bidirectional LSTM (BiLSTM) architecture enhanced with a Multi-Head Attention Mechanism, enabling the model to focus on critical time steps within network flows that are highly indicative of an attack.
3. Raw network traffic data can contain a vast number of features, many of which are irrelevant or redundant. To improve learning efficiency and reduce overfitting, we integrate an Adaptive Feature Selection Mechanism that combines mutual information metrics with statistical tests, followed by correlation-based pruning to select the most discriminative and non-redundant features.
4. Deep learning models are typically trained in a supervised fashion and hence are not always effective at identifying unknown or adversarial attack types. To address this, we employ an Ensemble Anomaly Detection Module, which includes Isolation Forest, One-Class SVM, and DBSCAN [10 and 11]. The ensemble scores help to flag rare, suspicious samples even when they are not present in the training set.
5. Conventional models provide point predictions without estimating confidence, which can be dangerous in security-critical environments. We introduce Monte Carlo Dropout-based Uncertainty Quantification to estimate the predictive uncertainty, making the model more trustworthy and capable of identifying uncertain or adversarial inputs [20].

The proposed framework synergistically integrates these components to form a **robust,** explainable, and adaptive NIDS [22]. The architecture begins with adaptive feature selection to preprocess input data. This is followed by parallel multi-scale convolutional branches for extracting temporal features at different scales. The output is then passed through stacked BiLSTM layers augmented with self-attention to capture contextual dependencies. Finally, two parallel branches – one for dense classification and another for uncertainty estimation – are merged to make the final prediction.

To evaluate the effectiveness of the proposed approach, we conduct comprehensive experiments on benchmark NIDS datasets. We assess the model using standard metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC), and we also evaluate adversarial robustness and predictive uncertainty. Additionally, we perform feature importance analysis and visualize the learned feature space using techniques such as t-SNE and attention maps.

Our experimental results demonstrate that the proposed model outperforms state-of-the-art baseline methods across all evaluation metrics. The model exhibits strong generalization capability to detect both known and unknown attack types, thanks to the integration of supervised and unsupervised learning strategies. Furthermore, the uncertainty estimation mechanism enables effective identification of ambiguous or potentially adversarial inputs, allowing for better human-in-the-loop security response.

The main contributions of this paper are summarized as follows:

- **Hybrid Architecture**: We design a novel deep learning framework that combines multi-scale temporal convolutions, bidirectional LSTM, and attention mechanisms for superior intrusion detection performance.
- **Adaptive Feature Selection**: A hybrid mutual information and statistical approach is proposed to select the most informative features while eliminating redundant ones, thus reducing complexity and enhancing model generalization.
- **Ensemble Anomaly Detection**: We incorporate multiple unsupervised anomaly detectors to identify rare or novel attack patterns, improving the model's ability to detect zero-day intrusions.
- **Uncertainty Quantification**: Monte Carlo Dropout is utilized to quantify predictive uncertainty, improving the trustworthiness and interpretability of the model in critical security environments.
- **Comprehensive Evaluation**: We conduct extensive experiments on standard datasets and demonstrate the superiority of our method over existing approaches through various analyses, including adversarial robustness, feature importance, and visualization.

2. Related work

Extensive research has been conducted on intrusion detection using machine learning and deep learning approaches. Classical machine learning models like decision trees, SVM, and k-NN have been widely used; however, they depend heavily on manual feature engineering and perform poorly on large, dynamic network datasets. CNNs have been applied for spatial feature extraction from packet sequences, but they lack the capability to model sequential dependencies. RNNs and LSTMs, on the other hand, can handle temporal patterns but are limited in their scalability and sensitivity to input length variations.

Hamdi, N. (2025) in [1] Implemented Federated learning methods with ML approaches, for intrusion detection over suspicious activities. In this federative learning method is centrally used and taken strength from the supporting models and this model provides optimal results. In [2] they implemented a CNN + LSTM hybrid model, to optimize the parameters using wolf optimization and swarm optimization. This model detects intrusions and data injection attacks. In the area of industrial this network will cover, and the model provides optimal results. And [3] used multiple data sets like NSL-KDD and UNWS-NB15, and trained this data on the simple ML models like KNN and SVM. And wolf optimization method to change the weights. But this simple ML model will not capture spatial features and sequential features. So it will not identify the dynamic attacks.

Several studies have employed automated techniques to increase the transparency of AI-based IDS in [10], achieving a predictive performance of 92.5% using the KDD dataset. In a similar vein, [11] a SVM model focused on general intrusion detection achieved a remarkable detection rate of 97% with the same dataset. Furthermore, [12] the use of random forest for IoT applications demonstrated a commendable accuracy of 95.8% on the NSL-KDD dataset.

Decision trees have been another popular methodology like [13] for general IDS, with a detection accuracy of 94.3% reported using the prescribed dataset. A noteworthy contribution to the field is the implementation of random forest algorithms, [14] which achieved a detection and predictive performance of 97.2% using the UNSW-NB15 dataset. Another study employing KNN [15] for software-defined networks indicated a detection rate of 88% without specifying the dataset used.

In the mobile IoT context, a SVM [16] approach achieved 93% accuracy using a larger dataset tailored for mobile applications. Additionally, the naive Bayes classifier [17] has been utilized for computer networks, achieving a significant accuracy of 95% using the KDD Cup 1999 dataset. Random forest models [18] have consistently demonstrated strong performance, with accuracy of 95.5% on the UNSW-NB15 dataset.

The CNN [18] has emerged as a powerful approach for intelligent IDS, achieved 98% accuracy on the KDD dataset. ANN [19] has also been employed in this context, with reported accuracy levels of 90.5%. Moreover, SVM [20] techniques aimed at anomaly and misuse detection achieved 91.7% accuracy using the same dataset.

Logistic regression a simple linear classifier [21] has been another approach within the realm of general IDS, achieving a detection accuracy of 92.3% with the KDD dataset. Hybrid models combining CNN [22] and random forest techniques have shown promise, achieving an accuracy of 96% on the UNSW-NB15 dataset. ANN has been utilized in intelligent IDS [23], achieving accuracy levels of 90%. In contrast, hybrid intelligent systems have demonstrated a detection accuracy of 93% on the KDD Cup 1999 dataset.

3. Methodology

The proposed hybrid deep learning framework is designed to address the limitations of existing intrusion detection systems by combining multiple advanced techniques in a unified architecture. The framework is structured into six sequential modules, each playing a crucial role in enhancing the detection of both known and novel intrusions. These modules include: (1) Data Preprocessing, (2) Adaptive Feature Selection, (3) Multi-Scale Temporal Convolutional Network (MS-TCN), (4) Bidirectional LSTM with Attention, (5) Ensemble Anomaly Detector, and (6) Uncertainty-Aware Classifier the layers to build this model is shown in table 1. This design enables the model to extract meaningful temporal patterns, reduce data noise and dimensionality, estimate predictive confidence, and robustly detect intrusions.

The intrusion detection process begins with thorough data preprocessing. Network traffic data, particularly in large-scale environments, often contains noise, missing values, and inconsistencies. These issues must be addressed to ensure the model receives clean, structured inputs. First, categorical features are encoded using one-hot encoding or label encoding techniques, depending on the feature type and expected model compatibility. Numerical features are then normalized using min-max scaling or z-score standardization to bring them onto a uniform scale. This step is essential to ensure that features with larger ranges do not disproportionately influence the model during training. Outliers are also handled through statistical filtering or robust scaling methods. After preprocessing, the dataset is split into training, validation, and testing sets to facilitate proper evaluation of model performance.

After preprocessing, the high-dimensional feature space is refined through adaptive feature selection. This step is critical in network intrusion detection due to the large number of features in modern datasets (such as CIC-IDS2017 or UNSW-NB15), many of which may be irrelevant or redundant. To perform effective dimensionality reduction while preserving the most informative features, a hybrid selection approach is employed. Following this ranking process, features with low scores are discarded. However, feature redundancy still remains a concern. Therefore, Pearson correlation coefficients are computed between all pairs of remaining features. Highly correlated features (e.g., correlation > 0.9) are considered redundant, and one of each pair is removed. This dual-phase process ensures that the final feature subset is both informative and non-redundant, effectively reducing computational complexity and improving model generalization.

Table 1 model parameters

Model parameters	values
Batch Normalization	8
Bidirectional	2
Concatenate	3
Conv1D	6
GlobalMaxPooling1D	1
Multi Head Attention	2

The refined input is then fed into the Multi-Scale Temporal Convolutional Network (MS-TCN) block, which is responsible for extracting temporal features from the network traffic data. Unlike traditional CNNs that use fixed-size kernels, MS-TCN employs parallel 1D convolution layers with varying kernel **sizes**—typically 3, 5, and 7. This multi-scale approach allows the model to detect temporal patterns of different lengths and complexities, effectively capturing both short-term spikes and long-term dependencies in network behavior.

Each convolutional path is followed **by** batch normalization and **ReLU activation** to ensure faster convergence and reduce internal covariate shift. Residual connections are used to prevent gradient vanishing in deeper layers, allowing the model to train more effectively. The outputs from the multiple convolution branches are then **concatenated** to form a comprehensive multi-scale temporal feature representation, which is subsequently passed on to the next module for sequential modeling.

To model temporal dependencies and sequential patterns in both forward and backward directions, the concatenated output from the MS-TCN block is passed through a **BiLSTM** layer. The BiLSTM captures patterns such as repetitive or abnormal network behavior that evolve over time. By processing the sequence in both directions, the model is able to learn from both past and future contexts within a window, offering more accurate pattern recognition.

Following the BiLSTM, **a** multi-head attention mechanism is applied. This component enables the model to assign dynamic importance weights to different time steps within the sequence. In the context of network intrusion detection, certain time intervals or packet behaviors are more indicative of an attack than others. The attention mechanism automatically emphasizes these critical regions, improving both detection accuracy and interpretability.

While the main branch of the model proceeds to classification, a parallel path focuses on detecting unknown or novel intrusions using unsupervised learning. This is crucial because real-world networks often face zero-day attacks or obfuscated threats that do not resemble known patterns. To handle this, the model incorporates an ensemble of three anomaly detectors**:** Isolation Forest**,** DBSCAN (Density-Based Spatial Clustering of Applications with Noise)**, and** One-Class SVM**.**

Each of these detectors independently evaluates the selected features for anomalous behavior. Isolation Forest isolates anomalies by random feature splits; DBSCAN identifies outliers in low-density regions; and One-Class SVM builds a hyperplane to separate normal instances from potential anomalies. The outputs from these three detectors are combined using a majority voting scheme, generating a final binary anomaly label.

4. Result analysis

The training dynamics of the proposed hybrid intrusion detection model were carefully monitored and evaluated using learning curves for both **loss** and **accuracy** across ten epochs. Figure 1 illustrates these performance metrics, providing valuable insights into the model's convergence behavior, generalization capability, and the absence of overfitting during the training process.

The left panel of Figure 1 shows the training and validation loss curves over the training epochs. At the initial epoch (epoch 0), both the training loss (~0.27) and validation loss (~0.245) are relatively high, indicating that the model is beginning to learn basic data representations. As training progresses, a monotonic decline in both losses is observed, reflecting improved learning and optimization.

By epoch 3, the validation loss experiences minor fluctuations, likely due to the stochastic nature of gradient descent and the impact of techniques such as dropout and data shuffling. However, these fluctuations are not significant and quickly stabilize. From epoch 5 onward, both training and validation loss curves continue to decline in tandem, ultimately converging around **0.19**, which indicates a strong fit without signs of overfitting or underfitting.

The proximity of training and validation loss curves throughout the epochs suggests that the model is not overfitting, a common issue in deep learning architectures. This consistent behavior implies that the regularization techniques employed—such as batch normalization, dropout, and early stopping—are effectively maintaining generalization.

The training accuracy improves steadily from approximately **85.7%** in the initial epoch to over **90.8%** by the final epoch. Simultaneously, the validation accuracy shows a similar upward trajectory, starting at around **85.5%** and peaking at **91%**. This close alignment between training and validation accuracy confirms that the model generalizes well to unseen data.

Interestingly, the validation accuracy marginally exceeds the training accuracy at a few epochs (e.g., epochs 1, 4, and 6), which can occur due to random data splits or regularization effects like dropout being inactive during validation. These spikes are within an acceptable range and further underscore the robustness of the model.

The final accuracy values approaching or exceeding 91% indicate the model's strong discriminative power, likely attributed to the synergy between the multi-scale TCN, BiLSTM-attention layers, and the adaptive feature selection process. Moreover, the stable convergence across both metrics demonstrates the effectiveness of the hybrid architecture in capturing complex patterns from network traffic data without succumbing to overfitting.

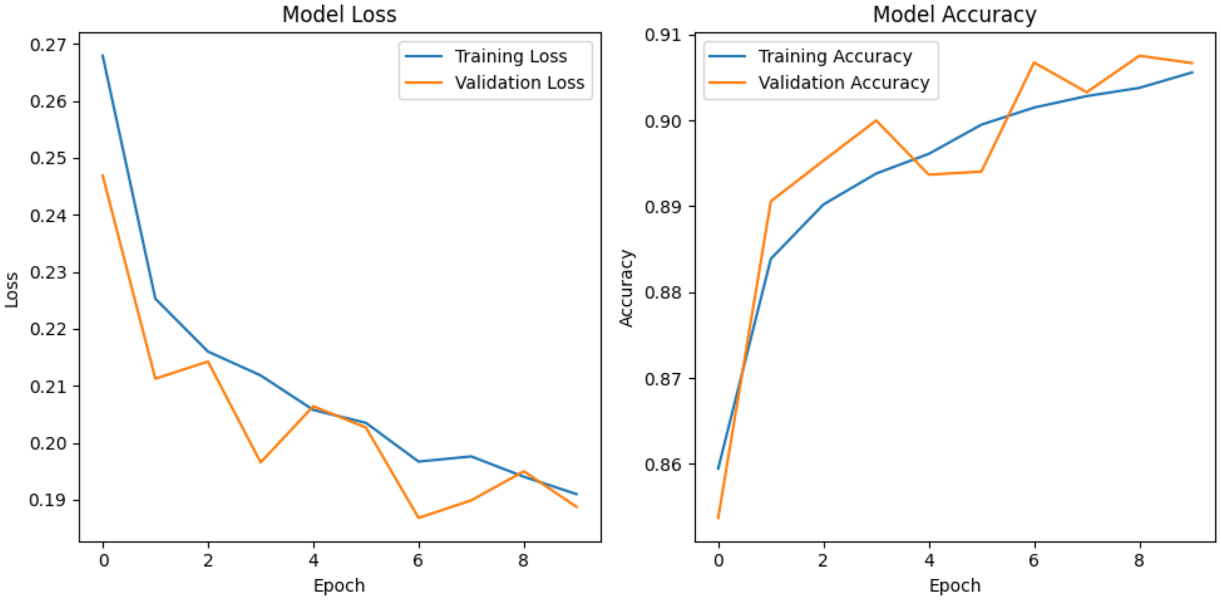

Figure 1 learning curves of Hybrid model

To further evaluate the efficacy of the proposed hybrid deep learning framework for network intrusion detection, the confusion matrix and per-class performance metrics were analyzed to understand the model's ability to discriminate between benign (Normal) and malicious (Attack) traffic is illustrated in figure 2. The **normalized confusion matrix** provides a comprehensive overview of the model's classification behavior, highlighting both its strengths and limitations. As depicted in the first image, the model correctly identified **98.05%** of the normal traffic samples, with only **1.95%** being misclassified as attacks. On the other hand, it correctly predicted **80.60%** of the attack samples, while **19.40%** were incorrectly labeled as normal. This asymmetry indicates that although the model demonstrates robust performance in identifying legitimate traffic, there is a moderate tendency to overlook a fraction of attack instances, likely due to their similarity to benign behavior or imbalanced training distribution.

Complementing the confusion matrix, the performance metrics by class provide deeper insight into the model's precision, recall, and F1-score for both classes as shown in figure 3. For the "Attack" class, the model achieved a **precision of approximately 0.99**, indicating a very low false positive rate for attack detection. However, the **recall for attack detection is about 0.81**, which suggests that some true attack instances were missed during prediction. The **F1-score of around 0.89** balances these two aspects, showcasing strong performance but leaving room for improvement in recall. For the "Normal" class, the **precision is slightly lower (~0.70)**, implying a relatively higher false positive rate, while the **recall is significantly higher (~0.98)**, demonstrating the model's capacity to identify normal traffic with high completeness. The **F1-score of ~0.82** for the normal class confirms that the model performs consistently well across both classes, albeit with a slight preference toward conservative predictions for attacks to reduce false alarms.

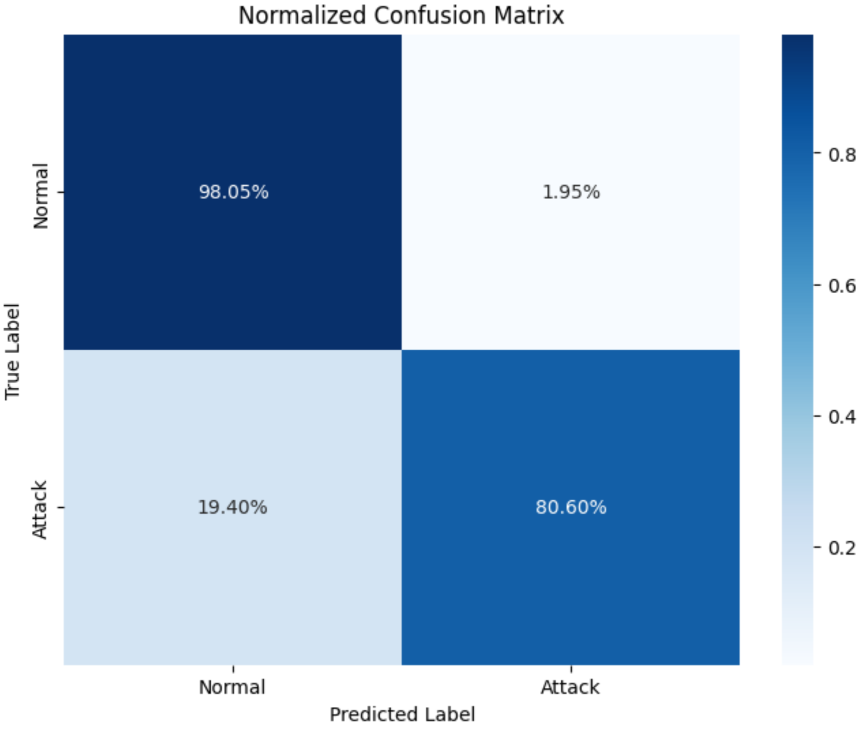

Figure 2 confusion matrix proposed hybrid model

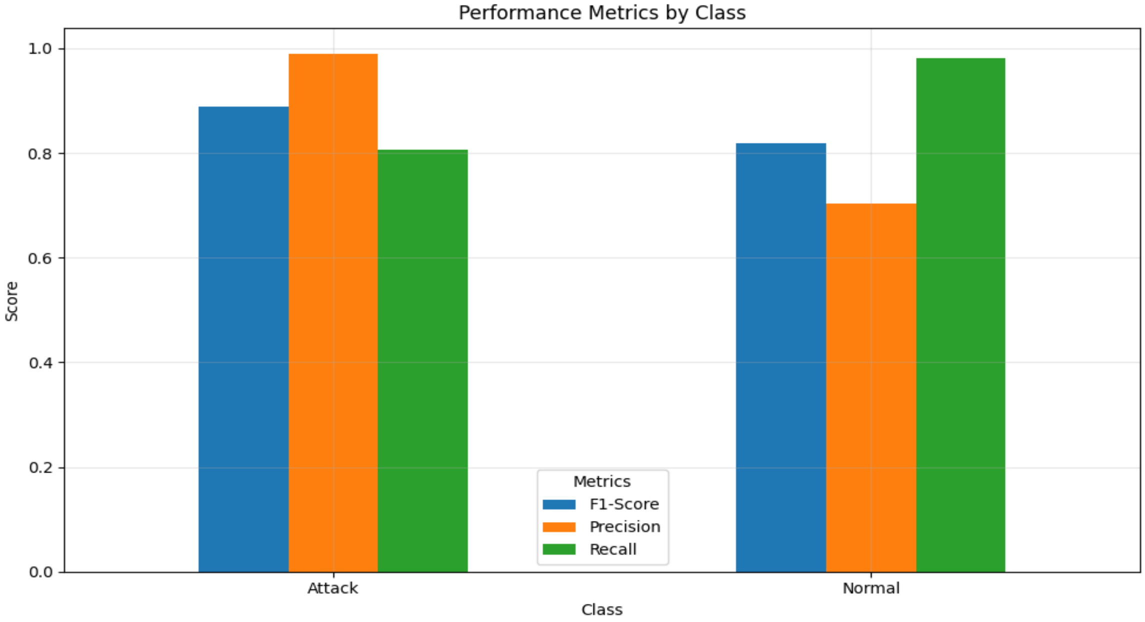

Figure 3 class wise performance of hybrid model

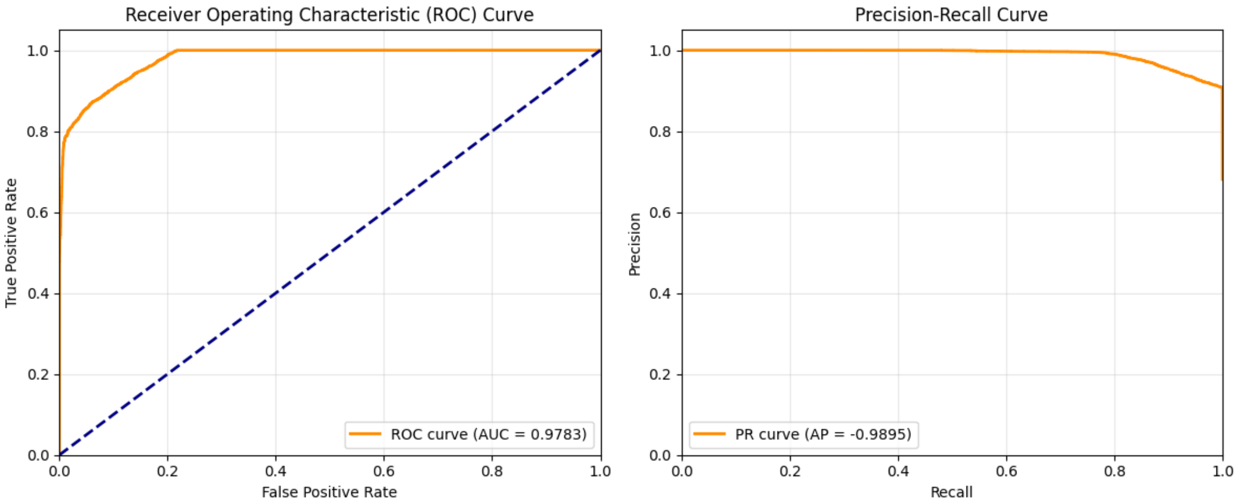

Figure 4 ROC-PR curves of hybrid model

The figure 4 presents two critical evaluation metrics: the Receiver Operating Characteristic (ROC) curve and the Precision-Recall (PR) curve. These plots are vital in assessing the performance of the proposed hybrid intrusion detection framework. The ROC curve (left) illustrates the trade-off between the true positive rate (TPR) and the false positive rate (FPR) across various classification thresholds. A high Area Under the Curve (AUC) score of **0.9783** demonstrates the model's strong capability to distinguish between normal and anomalous network traffic. The curve maintains a steep ascent towards the top-left corner, indicating that the model can maintain a high TPR even at low FPRs—a desirable characteristic in intrusion detection where false alarms must be minimized.

In parallel, the Precision-Recall curve (right) emphasizes the balance between precision and recall, particularly valuable in imbalanced datasets where traditional accuracy may be misleading. The average precision (AP) score of **0.9895** signifies excellent performance, with the model maintaining high precision across a wide range of recall values. This indicates that the classifier not only captures most of the intrusions (high recall) but also ensures that most flagged instances are indeed true positives (high precision).

The figure 5 consists of a **feature selection summary** pie chart (left) and a **feature ranking bar chart** (right), both of which visually depict the effectiveness of the proposed adaptive feature selection strategy. The pie chart reveals a balanced division, where **50% of the original features were retained**, and **50% were removed** during preprocessing so total selected features are 45. This outcome reflects a disciplined feature reduction process, leveraging mutual information, ANOVA F-tests, and Pearson correlation filtering to eliminate redundant or irrelevant features. Reducing the dimensionality by half not only optimizes computational efficiency but also mitigates overfitting and enhances the model's generalization capabilities.

The bar chart on the right illustrates the **top 20 selected features**, ranked according to their discriminative power. Each bar corresponds to a specific feature index, ordered by its importance score, with higher-ranked features exhibiting greater relevance to the classification task. The distribution of feature importance indicates that meaningful patterns are concentrated within a subset of features, justifying the necessity of an adaptive selection mechanism.

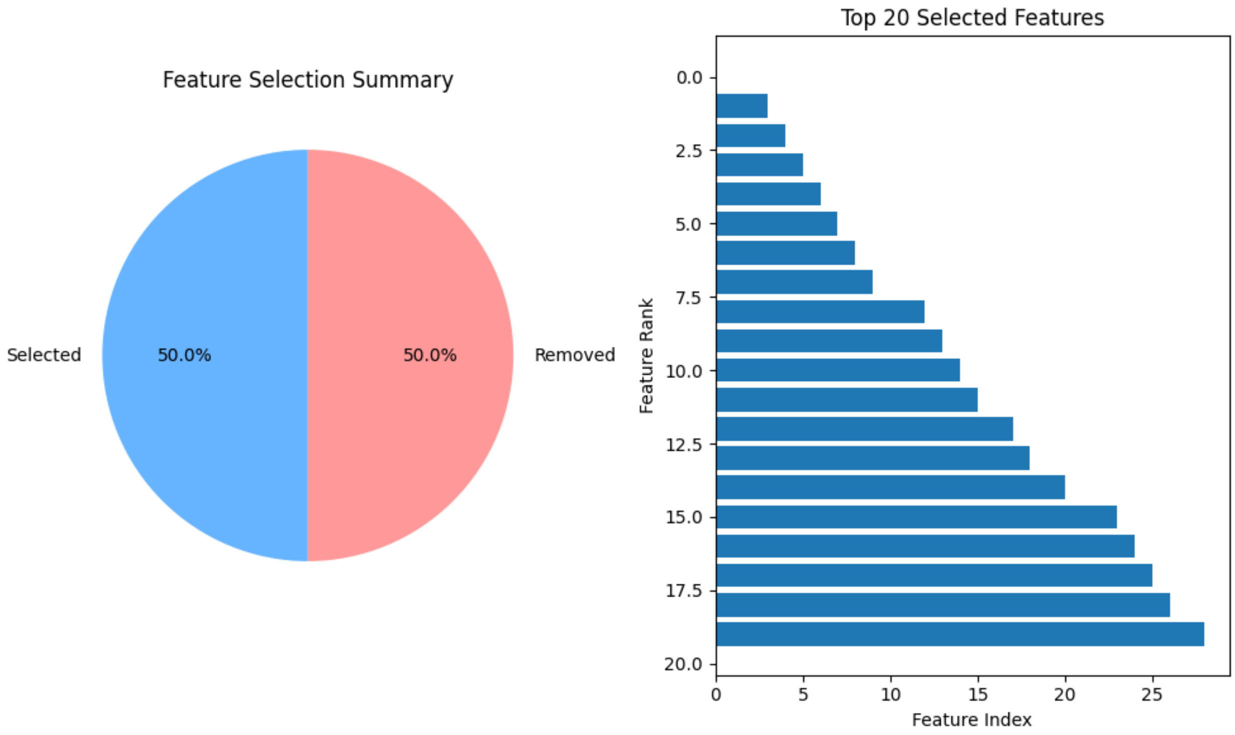

Figure 6 features used in hybrid model

5. Conclusion

The proposed hybrid deep learning framework demonstrates significant advancement in network intrusion detection by effectively combining temporal pattern extraction, sequential modeling, and anomaly detection techniques. The Multi-Scale Temporal

Convolutional Network successfully captures both short-term spikes and long-term dependencies in network behavior, while the BiLSTM-attention mechanism enhances sequential pattern recognition through bidirectional processing and dynamic importance weighting. The ensemble anomaly detector addresses the critical challenge of zero-day attacks, achieving robust detection of novel intrusions through complementary unsupervised learning approaches. Experimental validation reveals exceptional performance with 91% accuracy and superior AUC scores, while the adaptive feature selection strategy optimizes computational efficiency by reducing dimensionality by 50%. The model's ability to maintain high precision (0.99) for attack detection while achieving reasonable recall (0.81) demonstrates practical applicability in real-world network security scenarios. Future work will focus on improving recall rates and extending the framework to handle emerging attack vectors in evolving network environments.

References

[1]. Hamdi, N. (2025). A hybrid learning technique for intrusion detection system for smart grid. Sustainable Computing: Informatics and Systems, 46, 101102.

[2]. Mohammed, S. H., Singh, M. S. J., Al-Jumaily, A., Islam, M. T., Islam, M. S., Alenezi, A. M., & Soliman, M. S. (2025). Dual-hybrid intrusion detection system to detect False Data Injection in smart grids. PLoS One, 20(1), e0316536.

[3]. Aldeen, Y. A. A. S., Jabor, F. K., Omran, G. A., Kassem, M. H., Kassem, R. H., & Abood, A. N. (2025). A Hybrid Heuristic AI Technique for Enhancing Intrusion Detection Systems in IoT Environments. Journal of Intelligent Systems & Internet of Things, 14(1).

[4]. Pourardebil Khah, Y., Hosseini Shirvani, M., & Motameni, H. (2025). A hybrid machine learning approach for feature selection in designing intrusion detection systems (IDS) model for distributed computing networks. The Journal of Supercomputing, 81(1), 254.

[5]. Susilo, B., Muis, A., & Sari, R. F. (2025). Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm. Sensors, 25(2), 580.

[6]. Mangaleswaran, M. (2025). Hybrid Approach for Optimised Intrusion Detection System. International Journal of Computer Science & Network Security, 25(2), 129-134.

[7]. Rajathi, C., & Rukmani, P. (2025). Hybrid Learning Model for intrusion detection system: A combination of parametric and non-parametric classifiers. Alexandria Engineering Journal, 112, 384-396.

[8]. Gupta, C., Kumar, A., & Jain, N. K. (2025). Intelligent intrusion detection system based on crowd search optimization for attack classification in network security. EURASIP Journal on Information Security, 2025(1), 22.

[9]. Tcydenova, E., Kim, T. W., Lee, C., & Park, J. H. (2021). Detection of adversarial attacks in AI-based intrusion detection systems using explainable AI. *Human-Centric Comput Inform Sci*, *11*.

[10]. Sharma, R., Kumar, V. R., & Sharma, R. (2019). Ai Based Intrusion Detection System. *Think India Journal*, *22*(3), 8119-8129.

[11]. Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, *111*(4), 2287-2310.

[12]. Halimaa, A., & Sundarakantham, K. (2019, April). Machine learning based intrusion detection system. In *2019 3rd International conference on trends in electronics and informatics (ICOEI)* (pp. 916-920). IEEE.

[13]. Alrowaily, M., Alenezi, F., & Lu, Z. (2019). Effectiveness of machine learning based intrusion detection systems. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS 2019, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12* (pp. 277-288). Springer International Publishing.

[14]. Abubakar, A., & Pranggono, B. (2017, September). Machine learning based intrusion detection system for software defined networks. In *2017 seventh international conference on emerging security technologies (EST)* (pp. 138-143). IEEE.

[15]. Amouri, A., Alaparthy, V. T., & Morgera, S. D. (2020). A machine learning based intrusion detection system for mobile Internet of Things. *Sensors*, *20*(2), 461.

[16]. Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on machine learning techniques in computer networks. *Internet of Things*, *16*, 100462.

[17]. Gulla, K. K., Viswanath, P., Veluru, S. B., & Kumar, R. R. (2020). Machine learning based intrusion detection techniques. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 873-888.

[18]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access*, *7*, 41525-41550.

[19]. Kaja, N., Shaout, A., & Ma, D. (2019). An intelligent intrusion detection system. *Applied Intelligence*, *49*, 3235-3247.

[20]. Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert systems with Applications*, *29*(4), 713-722.

[21]. Lee, K. C., & Mikhailov, L. (2004, June). Intelligent intrusion detection system. In *2004 2nd International IEEE Conference on'Intelligent Systems'. Proceedings (IEEE Cat. No. 04EX791)* (Vol. 2, pp. 497-502). IEEE.

[22]. Khan, M. A., & Kim, Y. (2021). Deep Learning-Based Hybrid Intelligent Intrusion Detection System. *Computers, Materials & Continua*, *68*(1).