IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Dual-Stage Data Fusion And Hybrid Deep Learning Framework For Robust Intrusion Detection In Network Traffic

Ram Naresh Sharma[1], Jitendra Singh Kushwah[2] and Pritaj Yadav[3]

[1,3]Department of Computer Science and Engineering, Rabindranath Tagore University, Bhopal, India.
[2]Department of Information Technology, Institute of Technology and Management, Gwalior, India.

Abstract- This study presents a cutting-edge intrusion detection framework that leverages a dual-stage data fusion strategy combined with hybrid deep learning models to improve the detection and classification of cyberattacks in network traffic. The proposed approach integrates behavioral ratio-based features, traffic intensity metrics, temporal activity patterns, and protocol-level interactions to construct a comprehensive fused feature space. A neural encoder network further refines these features, enabling the models to capture both spatial correlations and temporal dependencies, thereby enhancing discrimination between benign and malicious traffic. Two hybrid architectures FusionNet-BiLSTM IDS (CNN–BiLSTM) and FusionNet-GRU IDS (CNN–GRU) were implemented and evaluated on the CIC-IDS 2018 dataset. Severe class imbalance, a common challenge in intrusion detection, was effectively addressed using SMOTE-ENN, which synthetically oversamples minority classes and removes noisy majority-class samples, improving generalization and detection of low-frequency attacks. Exploratory data analysis guided feature engineering and model design. Performance evaluation demonstrated that FusionNet-BiLSTM achieved high accuracy (0.9871), precision (0.9872), recall (0.9871), F1-score (0.9871), and low loss (0.04), while FusionNet-GRU provided competitive metrics with faster training. The results confirm that the proposed hybrid deep learning and dual-stage feature fusion framework, combined with SMOTE-ENN, offers robust, scalable, and reliable intrusion detection suitable for dynamic cybersecurity environments**.**

Keyword- Intrusion Detection System, Hybrid Deep Learning, Data Fusion, Network Security, Cyberattack Detection, Temporal and Spatial Features, Feature Engineering

1. INTRODUCTION

In today's digital era, the rapid expansion of internet-connected devices, cloud computing, and large-scale network infrastructures has significantly increased the exposure of systems to cyber threats. Organizations across industries are increasingly facing sophisticated attacks, including malware, ransomware, denial-of-service (DoS) attacks, insider threats, and advanced persistent threats (APTs). These attacks often lead to severe financial losses, operational disruptions, and reputational damage. Traditional security measures, such as firewalls, antivirus software, and signature-based intrusion detection systems (IDS), have proven inadequate in identifying advanced and evolving cyber threats due to their reliance on pre-defined signatures and static rules. As cyber-attacks become more complex and dynamic, there is an urgent need for intelligent and adaptive intrusion detection techniques capable of accurately identifying malicious activities in real time while minimizing false positives[1]-[4].

One promising approach to address this challenge is the integration of data fusion with hybrid deep learning (DL) algorithms. Data fusion refers to the process of systematically combining information from multiple heterogeneous sources such as network traffic logs, protocol metadata, and system event records to create a richer and more informative feature set. By aggregating diverse data sources, the detection model gains a comprehensive understanding of network behavior, allowing it to capture subtle anomalies and sophisticated attack patterns that might be missed when analyzing single-source data. This enriched feature representation enhances the overall effectiveness and robustness of intrusion detection systems, making them capable of handling increasingly complex cyber-attack scenarios[5]-[9].

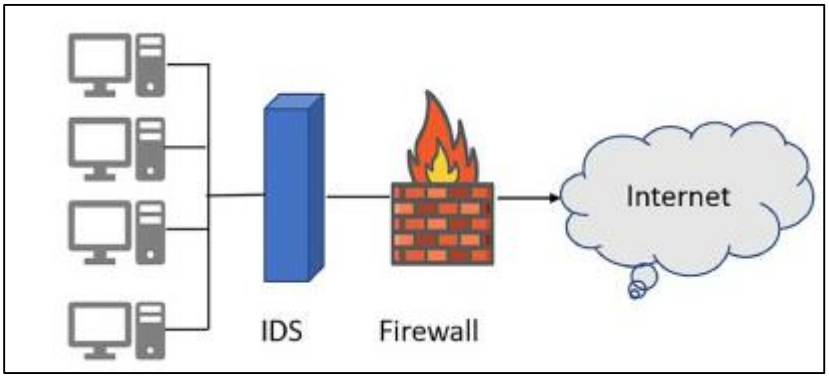

Figure 1 IDS System

Hybrid deep learning models further enhance detection capabilities by leveraging the complementary strengths of different architectures. Convolutional neural networks (CNNs) are highly effective in extracting spatial features and identifying patterns within structured network traffic data, whereas recurrent neural networks (RNNs) such as long short-term memory (LSTM) networks and gated recurrent units (GRUs) excel at modeling temporal dependencies and sequential patterns in time-series data. By integrating CNNs with LSTMs or GRUs, hybrid models can simultaneously capture both spatial and temporal characteristics of network traffic. This combination enables the detection system to identify not only known attacks but also zero-day intrusions and novel threat patterns that evolve over time, significantly improving detection accuracy and resilience against a wide range of cyber threats[10].

Another crucial aspect of developing an effective IDS is handling the problem of class imbalance in cybersecurity datasets, where attack instances are often underrepresented compared to normal traffic. Techniques such as SMOTE (Synthetic Minority Oversampling Technique) and SMOTEENN (a combination of oversampling and edited nearest neighbors) help generate balanced datasets, ensuring that the hybrid model is trained on sufficient examples of minority classes. This approach mitigates bias toward majority classes and enhances the system's ability to detect rare but critical attack types, which is essential for high-risk environments such as critical infrastructure, healthcare networks, and financial systems[11]-[14].

The proposed framework is evaluated using the CIC-IDS 2018 dataset, a comprehensive and widely recognized benchmark containing diverse attack types, including DoS, DDoS, botnets, web attacks, and infiltration attempts. Extensive exploratory data analysis (EDA) is conducted to understand traffic patterns, feature distributions, and attack characteristics, guiding the design of the feature fusion strategy. The hybrid models are trained and tested on the balanced dataset, with performance metrics including accuracy, precision, recall, F1-score, and loss providing a holistic assessment of detection capabilities[15]-[19]. This study introduces a high-performance intrusion detection technique that integrates domain-driven data fusion with hybrid deep learning architectures and class balancing techniques. The approach is designed to address critical challenges in IDS, including feature representation, temporal dependency modeling, and class imbalance, resulting in enhanced detection accuracy and robustness. By explicitly modeling directional asymmetries, temporal behavior, and interaction-based traffic patterns, the proposed IDS framework demonstrates strong potential for real-world deployment, offering scalable, reliable, and efficient protection against evolving cyber threats in complex network environments. Developing a cutting-edge intrusion detection technique using data fusion and hybrid learning represents a significant advancement in cybersecurity research. By combining multi-source data integration with hybrid deep learning architectures, this approach offers a robust, adaptive, and intelligent solution for identifying both known and emerging cyber threats. The proposed methodology promises improved detection accuracy, reduced false positive rates, and enhanced overall

network security. As cyber threats continue to grow in complexity and frequency, such innovative IDS frameworks are essential for safeguarding critical digital infrastructure and maintaining the integrity, availability, and confidentiality of networked systems[20].

2. LITERATURE REVIEW

Hozouri 2025 et.al Recent advancements in artificial intelligence (AI) and machine learning (ML) have significantly enhanced connectivity and operational efficiency across multiple domains. However, these developments have simultaneously amplified cyber threats, challenging governments, enterprises, and societies. Intrusion Detection Systems (IDS) play a crucial role in monitoring and analyzing network traffic to identify malicious activities and respond promptly. Traditional IDS approaches often struggle with evolving attacks, motivating researchers to leverage ML and deep learning (DL) techniques to enhance detection accuracy. The study provides a comprehensive overview of IDS architectures, operation, and popular datasets such as CIC-IDS2017, KDDCup99, and UNSW-NB15, which include diverse attack scenarios and normal traffic. By analyzing these datasets, IDS models can be trained to detect emerging threats effectively. The research emphasizes that constant innovation in AI-driven IDS is essential to counter sophisticated cyberattacks, enhance network security, and ensure the reliability of digital infrastructures in modern interconnected environments [21]

Kandasamy 2025 et.al The proliferation of connected devices in smart home environments has intensified security risks, particularly Man-in-the-Middle (MitM) attacks, which intercept and manipulate communications. Traditional rule-based detection methods often fail to address such sophisticated attacks, necessitating adaptive approaches. This study introduces the AEXB model, a hybrid deep learning IDS combining AutoEncoder-based feature extraction with XGBoost classification, leveraging the strengths of both techniques. Robust preprocessing including data cleaning, scaling, dimensionality reduction, and feature selection via Recursive Feature Elimination (RFE) and correlation analysis enhances model reliability. Applied to the Intrusion Detection in Smart Home (IDSH) dataset, the model achieves a high accuracy of 97.24%, demonstrating its efficacy in identifying anomalous network behavior. Furthermore, the AEXB model enables real-time detection, allowing rapid responses to threats and continuous protection in dynamic smart home networks. This research underscores the potential of hybrid DL-ML frameworks for mitigating complex IoT security threats [22].

Buyuktanir 2025 et.al Federated Learning (FL) has emerged as a promising paradigm for privacy-preserving distributed machine learning, addressing data confidentiality and integrity in sectors like IoT, healthcare, finance, and cybersecurity. This study explores the integration of FL into Intrusion Detection Systems (IDS) to improve privacy and detection accuracy in decentralized networks. FL allows multiple clients to collaboratively train models without centralizing sensitive data, mitigating the risk of data breaches. The research reviews FL-based IDS solutions incorporating Generative Adversarial Networks (GANs), artificial immune systems, and hybrid deep learning techniques, highlighting their effectiveness in enhancing intrusion detection while preserving confidentiality. Key challenges, including aggregation procedures and non-independent, identically distributed (non-IID) data, are also discussed. The study concludes by proposing future directions to improve scalability, resilience, and accuracy of FL-based IDS, emphasizing its importance for privacy-preserving cybersecurity in distributed and sensitive data environments [23]

Mughaid 2024 et.al With the advent of 5G technology, the Internet of Things (IoT) has become the backbone of pervasive connectivity, particularly in smart cities. However, this widespread integration increases vulnerability to cyberattacks, threatening privacy, integrity, and system functionality. This research focuses on securing IoT-based urban networks through an IDS tailored to SYNFLOOD Denial-of-Service attacks. Using k-fold cross-validation, the model classifies, trains, and validates the imported attack data. Enhanced preprocessing and data balancing steps improve detection capability, ensuring robust network communication without compromising privacy. The proposed system was evaluated across six machine learning algorithms, with Decision Tree and Neural Network models achieving 92.3% accuracy, demonstrating the effectiveness of the approach. This work highlights the importance of adaptive IDS for IoT networks in smart cities, addressing security and privacy concerns while enabling reliable communication among densely connected devices in real-time operational environments [24]

Viboonsang 2024 et.al Network Intrusion Detection Systems (NIDS) analyze network traffic to identify potential attacks and alert security teams. To enhance predictive accuracy, this study applies both machine

learning (ML) and deep learning (DL) techniques on the NSL-KDD dataset. ML algorithms such as Random Forest, Decision Tree, Logistic Regression, KNN, GaussianNB, CatBoost, and XGBoost were evaluated alongside a Recurrent Neural Network (RNN) model. Data preprocessing included Standard Scaling, label and one-hot encoding, and imbalanced data handling through SMOTE-Tomek Links, ensuring robust feature representation. Pearson correlation analysis was used for feature selection. The results indicate that Random Forest achieved the highest accuracy of 99.71%, while the RNN attained 97.67%, demonstrating the effectiveness of hybrid ML-DL approaches in NIDS. This study reinforces the role of advanced algorithms and data preprocessing in improving intrusion detection performance, enabling accurate identification of diverse attack patterns in network traffic [25].

Table 1 Literature Summary

Author & Year	Methodology / Technique	Research Gap	Key Findings	Limitations
Kheddar et al., 2025 [26]	Deep Reinforcement Learning (DRL)-based IDS for Industrial Control Systems (ICS)	Limited comprehensive reviews on DRL-based IDS for diverse ICS and IoT environments	Provided a detailed taxonomy of DRL-IDS approaches, datasets used, types of DRL, pretrained networks, IDS techniques, evaluation metrics, and performance improvements	The study is primarily a review; lacks experimental validation of proposed frameworks
Afnan Birahim et al., 2025 [27]	Particle Swarm Optimization (PSO) + Ensemble ML (Random Forest, Decision Tree, KNN) with SMOTE-Tomek and XAI (LIME, SHAP)	Imbalanced datasets and evolving network attacks limit IDS accuracy in WSN	Achieved 99.73% accuracy, with precision, recall, and F1 score of 99.72% on WSN-DS dataset; interpretable results using LIME and SHAP	Focused only on WSN; scalability in large heterogeneous networks not tested
Gulzar & Mustafa, 2025 [28]	DeepCLG hybrid model (CNN + LSTM + GRU + Capsule Network) for IIoT IDS	Existing IIoT IDS models often fail on minority attack classes due to imbalanced real-world data	High accuracy (99.82% CICIoT 2023, 95.55% UNSW_NB15), precision, F1-score, MCC, and very low false alarm rates; effective in detecting multiple attack types	Performance on highly dynamic IIoT networks under real-time traffic conditions remains to be validated
Karthikeyan et al., 2024 [1]	Firefly Algorithm + ML (SVM) for WSN-IoT security	Existing IoT-WSN IDS models lack optimization and effective parameter tuning	Achieved 99.34% accuracy on NSL-KDD; outperformed KNN-PSO and XGBoost; improved intrusion detection in WSN-IoT	Tested only on NSL-KDD dataset; practical deployment and latency not analyzed
Kumar et al., 2024 [3]	Data Fusion + SVM with Binary Grasshopper Optimization (BGO-SVM)	Previous works suffered from overfitting and non-optimized	Effective intrusion detection on fused IoT-23 and IoTID20 datasets; improved detection rate,	Limited evaluation on dynamic or streaming IoT traffic; real-time

		detection using single datasets	accuracy, recall, and F-measure	performance not analyzed
Tawfik, 2024 [29]	Stacked Autoencoder + CatBoost + Transformer-CNN-LSTM ensemble for Fog/IoT IDS	Resource constraints at fog nodes hinder traditional IDS	Achieved >95% accuracy across NSL-KDD, UNSW-NB15, and AWID datasets; integrated edge preprocessing and cloud-based ensemble learning for efficient anomaly detection	Computational complexity may be high for low-power IoT devices; deployment overhead not assessed
Hazman et al., 2023 [30]	Ensemble Learning IDS (AdaBoost + feature selection: Boruta, MI, correlation) for smart cities	IoT networks in smart cities are vulnerable due to device mobility and attack surface	Achieved ~95.9% detection accuracy and low detection time; evaluated on IoT-23, BoT-IoT, and Edge-IIoT datasets	Limited focus on real-time intrusion handling; performance under high-volume traffic not evaluated

3. RESEARCH METHODOLOGY

This study proposes a cutting-edge intrusion detection technique that integrates data fusion strategies with hybrid deep learning architectures to enhance the accuracy and robustness of cyberattack detection. The methodology is implemented using a sampled version of the CIC-IDS 2018 dataset, which contains realistic network traffic representing both benign activities and multiple attack categories. The core objective of the proposed framework is to improve detection performance particularly for complex and low-frequency attacks by combining behavior-aware feature fusion, class imbalance handling, and hybrid CNN-based deep learning models.

3.1 DATA COLLECTION

The data used in this study are obtained from the CSE-CIC-IDS2018 dataset, a widely recognized and benchmark intrusion detection dataset developed jointly by the Canadian Institute for Cybersecurity (CIC), University of New Brunswick, and the Communications Security Establishment (CSE), Canada. The dataset is publicly available and can be accessed from the official CIC repository at: https://www.unb.ca/cic/datasets/ids-2018.html. This dataset was specifically designed to reflect realistic modern network environments, making it highly suitable for evaluating advanced intrusion detection systems. It contains labeled network traffic representing both benign activities and diverse cyberattacks, captured over multiple days in a controlled yet realistic infrastructure.

The dataset includes flow-based features extracted using the CICFlowMeter-V3 tool, resulting in approximately 80 numerical attributes describing packet counts, byte statistics, flow duration, inter-arrival times, and protocol-level behavior. It covers a wide range of attack categories such as Brute Force, Botnet, DoS, DDoS, Web Attacks, Infiltration, and Heartbleed, along with normal traffic. This diversity allows the proposed intrusion detection framework to learn both high-volume and stealthy attack behaviors. For this study, the dataset is accessed in CSV format, facilitating seamless integration with machine learning and deep learning pipelines. Due to its large scale, controlled sampling is applied to ensure computational efficiency and balanced class representation.

3.2 Data Cleaning and Preprocessing

To ensure model stability and prevent learning bias, several preprocessing operations are applied. First, infinite values produced by division-based traffic metrics are replaced with NaN values. Missing values are then handled appropriately, either through removal or imputation, to prevent disruption during model training.

Non-informative identifiers such as Flow ID, Source IP, Destination IP, and Timestamp are removed from the dataset. These attributes do not contribute to attack behavior modeling and may introduce data leakage if retained.

The original attack labels are subsequently mapped into major attack categories, creating a structured classification hierarchy that simplifies multi-class learning while preserving semantic distinctions between attack types. After label mapping, the dataset is separated into a feature matrix (X) and a target vector (y), ensuring that only meaningful numerical traffic attributes are supplied to the learning models.

3.3 Feature Scaling and Dataset Preparation

All features are normalized using MinMaxScaler, which scales values into the range [0,1]. This step is essential for CNN-based architectures, as it ensures numerical stability and accelerates convergence during training. The dataset inherently represents fused traffic behavior features, as packet-level and flow-level characteristics are jointly encoded within the CIC-IDS 2018 records.

To control computational cost and avoid dominance of majority classes, the dataset is capped at a maximum number of samples per class. This controlled sampling ensures balanced representation across attack categories and enables fair comparative evaluation of the proposed models.

3.4 EDA

Exploratory Data Analysis (EDA) is a critical step in understanding the structure, characteristics, and inherent patterns within the dataset before applying machine learning models. For this study, the CIC-IDS 2018 dataset was analyzed to examine both the overall distribution of attack classes and the impact of class balancing using SMOTE-ENN.

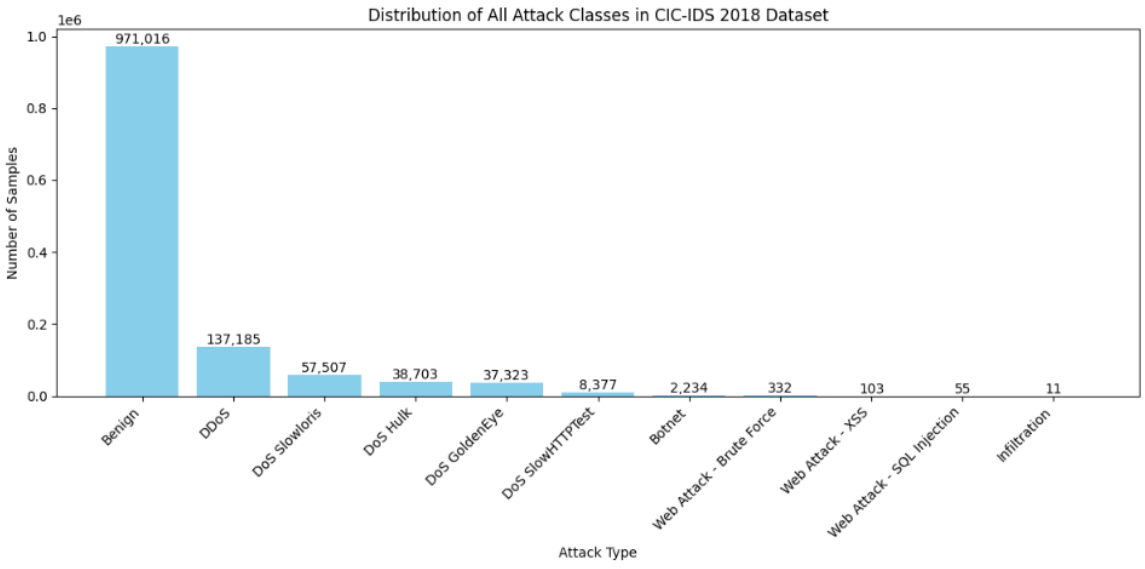

Figure 2 Distribution of All Attacks Classes

Figure illustrates the distribution of all attack classes in the dataset. The graph shows that the dataset is highly imbalanced, with the majority of samples belonging to benign traffic, followed by DoS/DDoS attacks. Minority classes such as Botnet, Web Attacks, and Infiltration are severely underrepresented, highlighting the challenge of detecting low-frequency attacks and the potential for biased model learning.

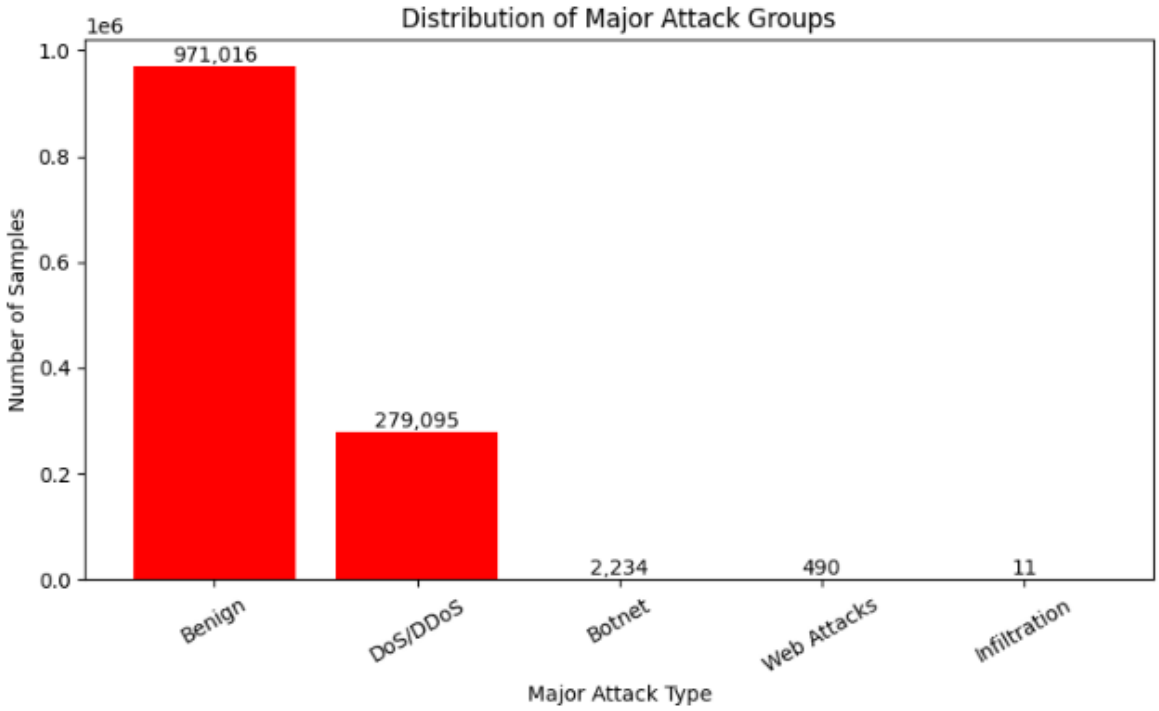

Figure 3 Distribution of Major Attack Groups

Figure presents the distribution of major attack groups after grouping the original attack classes into five broader categories: Benign, DoS/DDoS, Botnet, Web Attacks, and Infiltration. This grouping provides a clearer overview of traffic patterns, showing that DoS/DDoS attacks constitute a significant proportion of malicious traffic, while Infiltration and Web Attacks remain minimal.

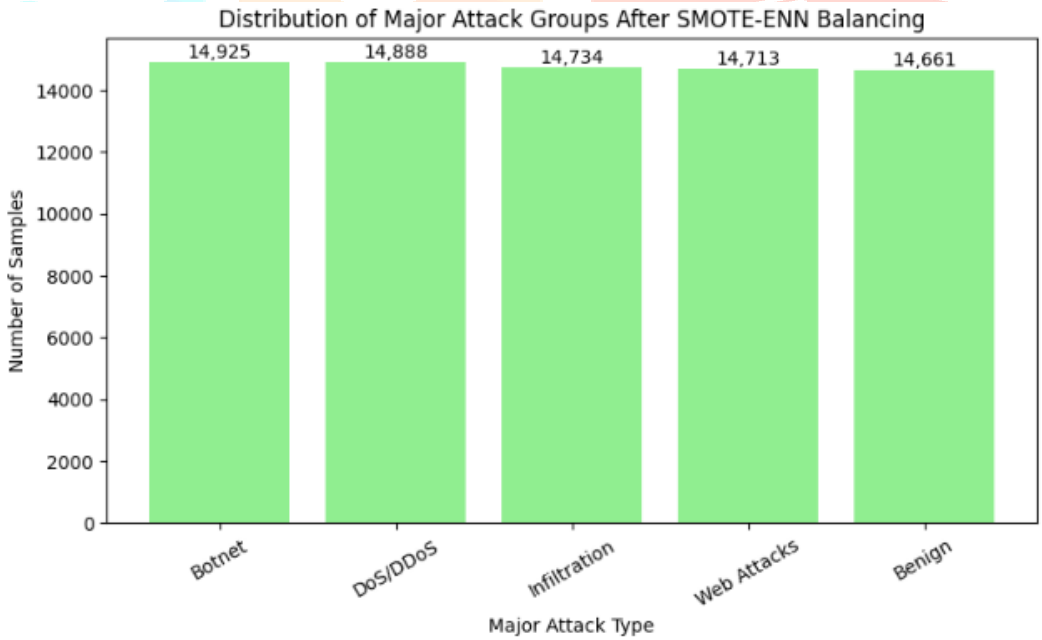

Figure 4 Major attacks Groups After SMOTE-ENN Balancing

Figure demonstrates the effect of SMOTE-ENN balancing on major attack groups. After resampling, the dataset achieves near-uniform representation across all classes, mitigating class imbalance and ensuring that the deep learning models can effectively learn features from minority attack categories. This balanced distribution is crucial for improving the generalization performance and detection accuracy of the proposed hybrid IDS models.

3.5 Proposed Feature Fusion Strategy

A hybrid data-level and neural-level feature fusion strategy is proposed to enhance the discriminative power of the intrusion detection system. Unlike conventional IDS approaches that rely solely on raw or independently treated features, the proposed method introduces a two-stage fusion mechanism combining domain-driven behavioral modeling with data-driven representation learning.

3.5.1 Behavioral Ratio-Based Feature Fusion

In the first fusion stage, raw network traffic features are mathematically combined to form behavior-aware fused features. These ratio-based metrics capture directional asymmetry, aggressiveness, and temporal imbalance key indicators of malicious activity.

- **Packet Direction Asymmetry**

Packet Direction Asymmetry is computed as the ratio between total forward packets and total backward packets. This fused feature effectively distinguishes scanning and flooding attacks from normal bidirectional communication patterns.

$$\textbf{\textit{Pkt Direction Ratio}} = \frac{Total\ Forward\ Packets}{Total\ Backward\ Packets+1} \quad (1)$$

This feature fuses forward and backward packet counts into a single directional behavior indicator, effectively distinguishing scanning and flooding attacks from normal bidirectional traffic.

- **Byte Direction Asymmetry**

Byte Direction Asymmetry integrates forward and backward byte volumes into a single metric, capturing payload imbalance commonly observed in denial-of-service and data exfiltration attacks.

$$\textbf{\textit{Byte Direction Ratio}} = \frac{Forward\ Bytes}{Backward\ Bytes+1} \quad (2)$$

This fusion captures payload imbalance, which is common in data exfiltration and denial-of-service scenarios.

- **Inter-Arrival Time Direction Fusion**

Inter-Arrival Time Direction Ratio fuses forward and backward inter-arrival time statistics, highlighting abnormal latency and response behaviors that characterize stealthy or protocol abuse attacks.

$$\textbf{\textit{IAT Direction Ratio}} = \frac{Fwd\ IAT\ Mean}{Bwd\ IAT\ Mean+1} \quad (3)$$

This feature integrates temporal behavior from both directions, highlighting abnormal delays and response patterns.

3.5.2 Traffic Intensity and Variability Fusion

To model traffic aggressiveness and burstiness, interaction-based fusion features are introduced. Flow Intensity combines throughput and packet rate into a single metric, providing a stronger indicator of high-impact attack flows than individual attributes. Packet Variability Fusion captures bursty transmission behavior, which is a known signature of botnet-driven and brute-force attacks. Beyond directional metrics, the study introduces interaction-based fused features to model traffic aggressiveness and burstiness.

- **Flow Intensity**:

$$\textit{Flow Intensity} = \text{Flow Bytes/s} \times \text{Flow Packets/s} \quad (4)$$

This feature fuses throughput and packet rate, capturing high-impact attack flows more effectively than individual metrics.

- **Packet Variability**:

$$Pkt_{Variability} = \frac{\text{Packet Length Std}}{\text{Packet Length Mean}+1} \quad (5)$$

This ratio-based fusion measures packet burstiness, a key signature of botnet and brute-force attacks.

3.5.3 Protocol and Temporal Activity Fusion

Protocol-level and temporal behaviors are incorporated through additional fusion metrics. TCP Flag Fusion aggregates multiple TCP control flags into a single protocol activity indicator, reducing feature dimensionality while preserving semantic meaning. Furthermore, the Active–Idle Time Ratio fuses active and idle flow durations, enabling detection of low-rate and stealthy attacks that alternate between activity and dormancy.

3.5.4 Robust Scaling for Fusion Stability

All engineered and original features are normalized using RobustScaler, which leverages median and interquartile range statistics. This scaling strategy ensures stability of fusion features in the presence of extreme outliers a common characteristic of real-world network traffic data.

3.6 Neural Feature Fusion via Encoder Network

In the second stage of the proposed feature fusion framework, a neural encoder-based fusion learner is employed to further enhance the representational capability of the engineered feature set. While the first-stage fusion constructs behavior-aware and interaction-based features using domain knowledge, this stage leverages deep learning to automatically learn nonlinear and high-level feature interactions that are difficult to capture through manual design alone.

The scaled feature matrix is provided as input to a multi-layer fully connected encoder network. This encoder progressively transforms and compresses the high-dimensional fused feature space into a lower-dimensional latent representation. Each dense layer applies nonlinear activation functions, enabling the network to model complex interdependencies among traffic features such as directional asymmetry, temporal imbalance, protocol behavior, and flow intensity. By stacking multiple dense layers, the encoder learns hierarchical abstractions, where lower layers capture basic feature interactions and higher layers represent more discriminative behavioral patterns.

The encoder network is designed to gradually reduce dimensionality, thereby eliminating redundant and less informative components while preserving the most salient characteristics of network traffic. The final encoding layer produces a 32-dimensional fused feature embedding, which serves as a compact yet information-rich representation of each traffic instance. This embedding effectively balances dimensionality reduction and information retention, ensuring computational efficiency without compromising detection performance.

A key advantage of this neural fusion mechanism is its ability to transform handcrafted behavioral features into learned latent representations. Unlike traditional feature selection methods that rely on static statistical criteria, the encoder dynamically adapts feature representations based on underlying data distributions. This results in enhanced class separability, particularly in scenarios where attack patterns exhibit overlapping characteristics or subtle variations.

Furthermore, the encoder-based fusion improves the model's robustness to noise and outliers, which are prevalent in real-world network traffic datasets. By learning smooth and generalized embeddings, the network reduces sensitivity to anomalous spikes and measurement inconsistencies. Consequently, the

fused feature space generated by the encoder provides a strong foundation for subsequent classification stages, enabling more accurate and reliable intrusion detection. The neural feature fusion via encoder network acts as a critical bridge between domain-driven feature engineering and data-driven learning, significantly strengthening the proposed intrusion detection framework.

3.7 Class Imbalance Handling

Class imbalance is a critical challenge in intrusion detection systems, as real-world network traffic datasets typically contain a disproportionately large number of benign samples compared to certain attack categories. In the CIC-IDS 2018 dataset, several malicious traffic classes particularly rare and stealthy attacks are severely underrepresented. If not addressed, this imbalance can bias learning algorithms toward majority classes, resulting in poor detection performance for minority attacks and an increased false-negative rate, which is highly undesirable in security-critical environments.

To mitigate this issue, the proposed framework employs SMOTE-ENN, a hybrid resampling technique that combines Synthetic Minority Over-sampling Technique (SMOTE) with Edited Nearest Neighbors (ENN). This integrated approach effectively balances the dataset while simultaneously reducing noise, thereby enhancing the robustness of the learning process.

1. In the first stage, SMOTE is applied to oversample minority classes by generating synthetic samples through interpolation between existing minority instances and their nearest neighbors. Unlike random oversampling, SMOTE reduces overfitting by introducing diverse yet realistic samples, allowing the model to better capture the intrinsic characteristics of rare attack patterns.

2. In the second stage, the ENN algorithm performs data cleaning by removing ambiguous and misclassified samples from both majority and minority classes. ENN evaluates each instance based on its nearest neighbors and eliminates those that do not conform to local class consistency. This step is particularly effective in eliminating overlapping samples near class boundaries, which are common in high-dimensional network traffic data.

By combining oversampling and noise reduction, SMOTE-ENN produces a cleaner and more balanced training dataset. This significantly improves the model's ability to learn discriminative features for minority attack classes while maintaining strong performance on majority classes. As a result, the proposed intrusion detection models achieve improved generalization, higher recall for rare attacks, and enhanced overall detection reliability making SMOTE-ENN a crucial component of the proposed IDS framework.

3.8 Deep Learning Data Reshaping

After resampling, the dataset is divided into training and testing subsets. Feature matrices are reshaped into a 3D tensor format (samples, features, 1), making them compatible with 1D convolutional layers. This transformation enables the models to capture local feature correlations and interaction patterns within network traffic data.

3.9 Hybrid Deep Learning Models

To effectively learn complex spatial–temporal patterns embedded in fused network traffic features, this study proposes and evaluates two hybrid deep learning architectures: the FusionNet-BiLSTM IDS Model and the FusionNet-GRU IDS Model. Both models are designed to leverage the strengths of convolutional feature extraction and recurrent sequence learning, enabling robust detection of diverse cyberattack behaviors.

1. FusionNet-BiLSTM IDS Model (CNN–BiLSTM)

The FusionNet-BiLSTM IDS model integrates one-dimensional Convolutional Neural Networks (1D-CNN) with Bidirectional Long Short-Term Memory (BiLSTM) layers to jointly capture spatial feature interactions and bidirectional temporal dependencies in network traffic data.

In this architecture, the CNN component serves as an automated feature extractor that operates on the fused and encoded traffic features. By applying multiple convolutional filters, the CNN layers learn

localized feature correlations and interaction patterns that emerge from the proposed data fusion strategy. These patterns represent meaningful combinations of packet behavior, flow intensity, and temporal imbalance that are difficult to capture using traditional machine learning approaches.

The output of the CNN block is then fed into BiLSTM layers, which model sequential dependencies in both forward and backward directions. This bidirectional processing allows the model to consider past and future traffic contexts simultaneously, improving its ability to detect complex and evolving attack behaviors such as multi-stage intrusions and slow-rate attacks.

Following the BiLSTM layers, fully connected dense layers are applied for high-level feature abstraction and classification. Dropout regularization is incorporated to mitigate overfitting and enhance generalization. The model is trained using the Adam optimizer and sparse categorical cross-entropy loss function, ensuring efficient convergence. To further improve training stability, early stopping and learning rate reduction on plateau are employed.

2. FusionNet-GRU IDS Model (CNN–GRU)

The second proposed architecture, termed the FusionNet-GRU IDS model, replaces the BiLSTM layers with Gated Recurrent Units (GRU) to achieve a more computationally efficient design while preserving effective temporal modeling capabilities.

Similar to the FusionNet-BiLSTM model, the CNN component in FusionNet-GRU performs automatic extraction of spatial feature patterns from the fused feature space. The GRU layers then model temporal dependencies using a simpler gating mechanism compared to LSTM, resulting in reduced parameter count and faster training times.

Despite its lower computational complexity, the GRU-based model maintains strong sequence learning performance, making it suitable for real-time or resource-constrained intrusion detection environments. The training configuration, optimization strategy, and evaluation pipeline remain consistent with the BiLSTM-based model, enabling a fair and reliable comparative performance analysis.

Table 2 Key Hyperparameters of the Proposed Hybrid IDS Models

Parameter	FusionNet-BiLSTM IDS (CNN–BiLSTM)	FusionNet-GRU IDS (CNN–GRU)
CNN Filters (Layers 1 & 2)	64, 128	64, 128
Kernel Size	3	3
Recurrent Layer Type	Bidirectional LSTM	GRU
Recurrent Units	64, 32	64, 32
Dropout Rate	0.3 (Recurrent), 0.4 (Dense)	0.3 (Recurrent), 0.4 (Dense)
Optimizer & Learning Rate	Adam (0.001)	Adam (0.001)
Batch Size	256	256
Epochs	100	100

3.10 Evaluation and Performance Analysis

Both hybrid models are evaluated on unseen test data using accuracy, confusion matrix, precision, recall, and F1-score. Special emphasis is placed on minority attack detection performance. Comparative analysis highlights the effectiveness of the proposed dual-stage fusion strategy and hybrid learning architectures.

3.11 Novelty and Contribution

The novelty of this study lies in its dual-stage feature fusion framework, which combines domain-driven behavioral interaction modeling with neural representation learning. By explicitly modeling directional asymmetries, traffic aggressiveness, and temporal behaviors, and refining them through an encoder-based fusion learner, the proposed IDS significantly enhances detection accuracy and robustness especially for complex and low-frequency cyberattacks.

4. Results and Discussion

The Results section presents the performance evaluation of the proposed hybrid intrusion detection models FusionNet-BiLSTM IDS (CNN–BiLSTM) and FusionNet-GRU IDS (CNN–GRU) on the CIC-IDS 2018 dataset. The evaluation focuses on multiple quantitative metrics, including accuracy, precision, recall, F1-score, and loss, to comprehensively assess the models' ability to detect and classify network attacks. Initially, Exploratory Data Analysis (EDA) highlighted significant class imbalance across various attack categories, which was subsequently mitigated using SMOTE-ENN resampling to ensure fair representation of minority classes. The hybrid models, incorporating CNN layers for spatial feature extraction and BiLSTM/GRU layers for temporal dependency modeling, were trained on the balanced dataset. Performance results demonstrate that both models achieve high detection capabilities, with the BiLSTM-based architecture slightly outperforming the GRU-based model in terms of accuracy and F1-score. These findings validate the effectiveness of the proposed dual-stage feature fusion and hybrid deep learning approach for robust intrusion detection in complex network environments.

1) Accuracy

Accuracy measures the overall correctness of the model by calculating the proportion of correctly classified instances out of the total samples. In intrusion detection, high accuracy indicates that the model reliably differentiates between benign and malicious traffic across all attack categories.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{6}$$

2) Loss

Loss reflects the model's error during training, calculated using sparse categorical cross-entropy for multi-class classification. Lower loss values indicate that the predicted probability distribution closely matches the true class labels, signifying effective learning and stable convergence of the deep learning model.

$$Loss = -\frac{1}{m}\sum_{i=1}^{m} yi.\log(yi) \tag{7}$$

3) Precision

Precision quantifies the proportion of true positive predictions among all samples predicted as positive. In IDS, high precision ensures that the model minimizes false alarms, meaning attacks flagged by the system are highly likely to be actual threats, reducing unnecessary alerts for network administrators.

$$Precision = \frac{TP}{TP+FP} \tag{8}$$

4) Recall

Recall, or sensitivity, measures the proportion of actual positive instances correctly identified by the model. In intrusion detection, high recall is crucial as it ensures that most attacks, including low-frequency or stealthy attacks, are detected, improving the security coverage of the system.

$$Recall = \frac{TP}{TP+FN} \tag{9}$$

5) F1 Score

F1-Score is the harmonic mean of precision and recall, balancing both false positives and false negatives. In IDS evaluation, a high F1-score indicates that the model achieves both high detection accuracy and minimal false alarms, making it robust for real-world cybersecurity applications.

$$F1 - score = \frac{2}{\frac{1}{precision} + \frac{1}{recall}} \quad (10)$$

This section presents the performance evaluation of the proposed hybrid intrusion detection models, namely FusionNet-BiLSTM IDS (CNN–BiLSTM) and FusionNet-GRU IDS (CNN–GRU), using multiple standard metrics. The evaluation includes accuracy, precision, recall, F1-score, and loss, providing a comprehensive comparison of their detection capabilities. Detailed analyses are supported by confusion matrices and classification reports, highlighting each model's effectiveness in distinguishing benign and malicious traffic. Both quantitative metrics and visualizations demonstrate the models' robustness, with BiLSTM slightly outperforming GRU while GRU offers computational efficiency suitable for real-time IDS deployment.

Table 3 Performance Evaluation of Proposed Hybrid IDS Models

Model	Accuracy	Precision	Recall	F1-Score	Loss
FusionNet-BiLSTM IDS (CNN–BiLSTM)	0.9871	0.9872	0.9871	0.9871	0.04
FusionNet-GRU IDS (CNN–GRU)	0.9700	0.9795	0.9788	0.9789	0.05

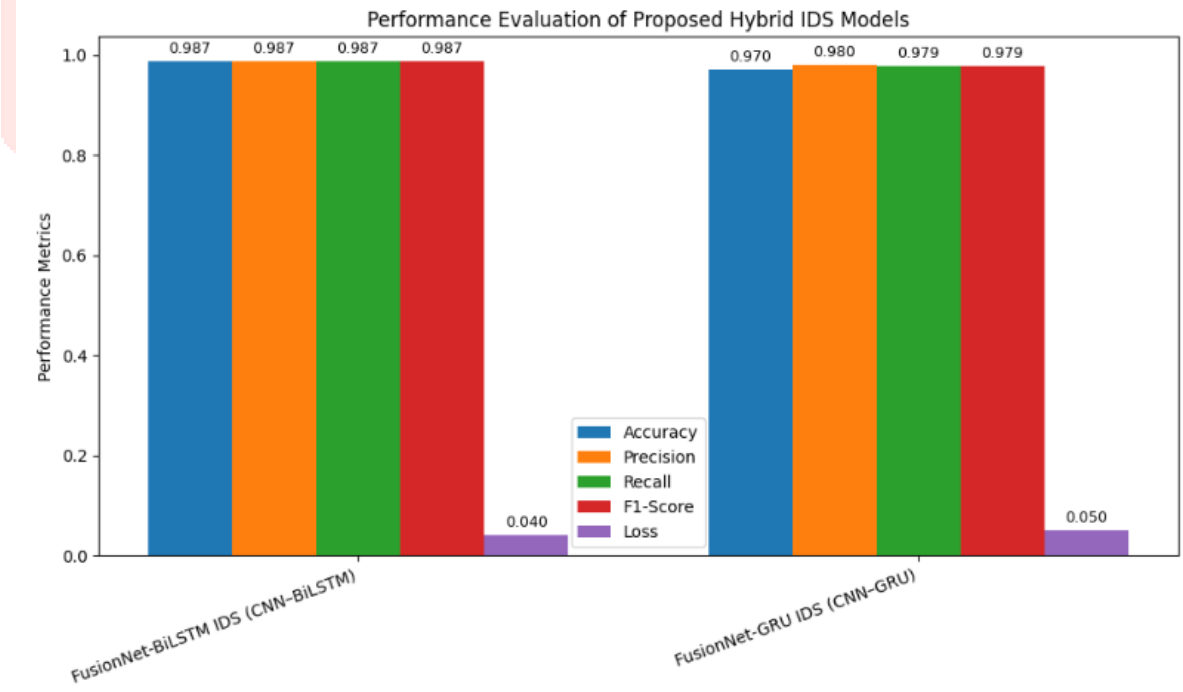

Figure 5 Performance Evaluation Graph

Table 3 presents the comprehensive performance evaluation of the proposed hybrid IDS models, FusionNet-BiLSTM IDS (CNN–BiLSTM) and FusionNet-GRU IDS (CNN–GRU), based on multiple standard metrics. The table summarizes five key indicators accuracy, precision, recall, F1-score, and loss allowing a clear comparison of detection effectiveness and reliability between the two architectures.

The FusionNet-BiLSTM IDS model demonstrates superior performance with an accuracy of 0.9871, slightly higher than the FusionNet-GRU model at 0.9700, indicating a stronger overall capability in

correctly classifying both benign and malicious network traffic. Precision, recall, and F1-score for the BiLSTM model are consistently high (0.9872, 0.9871, 0.9871 respectively), highlighting its ability to detect attacks accurately while minimizing false positives and false negatives. In contrast, the GRU-based model shows slightly lower but still competitive metrics (Precision: 0.9795, Recall: 0.9788, F1-score: 0.9789), reflecting a minor trade-off for reduced computational complexity and faster training.

The loss values further support these findings, with the BiLSTM model achieving a lower loss (0.04) compared to the GRU model (0.05), indicating more stable learning and better convergence during training. Figure 4 visually complements this table, illustrating the performance comparison across all metrics, emphasizing the effectiveness of the proposed hybrid deep learning framework for robust intrusion detection in diverse network environments.

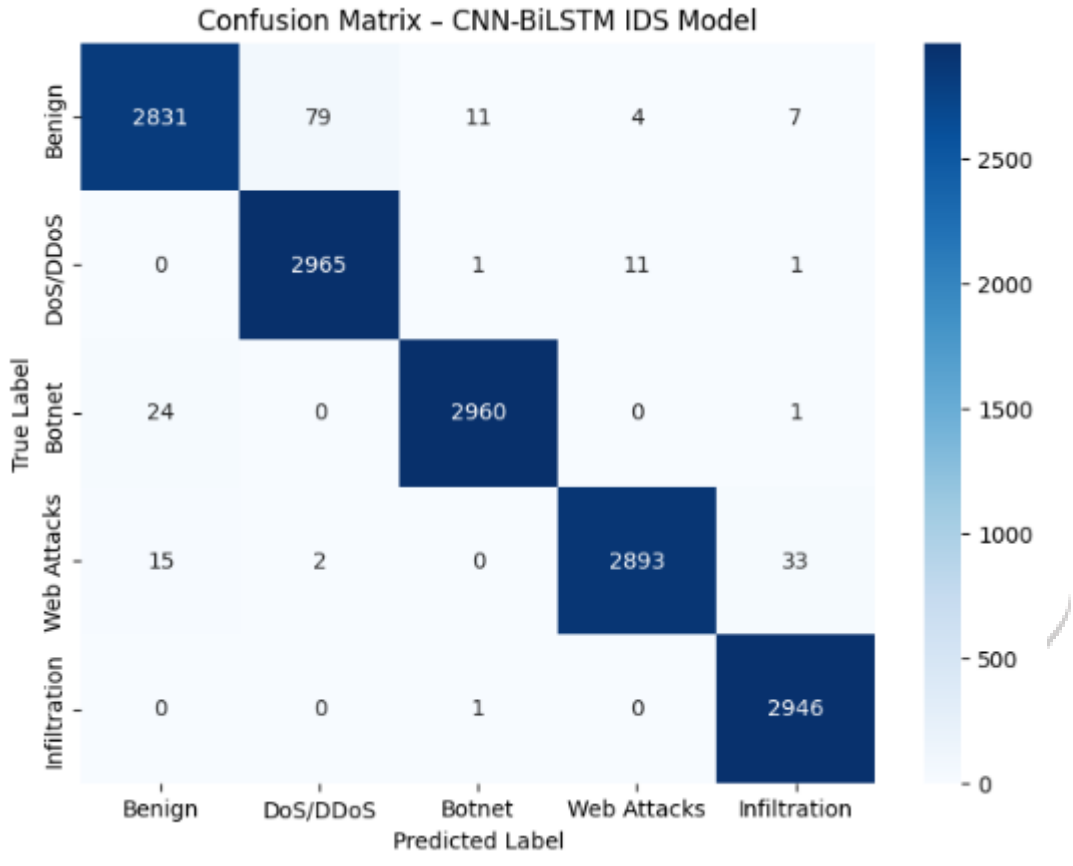

Figure 6 Confusion Matrix of FusionNet-BiLSTM IDS (CNN–BiLSTM)

This figure visualizes the prediction performance of the FusionNet-BiLSTM IDS model across all major attack categories. The confusion matrix displays true positives, true negatives, false positives, and false negatives, allowing an assessment of how well the model distinguishes between benign and various malicious traffic types. High values along the diagonal indicate that the model accurately classifies the majority of samples, including minority attack classes, demonstrating effective learning from the fused feature set.

	precision	recall	f1-score	support
Benign	0.9864	0.9656	0.9759	2932
DoS/DDoS	0.9734	0.9956	0.9844	2978
Botnet	0.9956	0.9916	0.9936	2985
Web Attacks	0.9948	0.9830	0.9889	2943
Infiltration	0.9859	0.9997	0.9928	2947
accuracy			0.9871	14785
macro avg	0.9872	0.9871	0.9871	14785
weighted avg	0.9872	0.9871	0.9871	14785

Figure 7 Classification Report of FusionNet-BiLSTM IDS (CNN–BiLSTM)

The classification report presents precision, recall, F1-score, and support for each attack class predicted by the FusionNet-BiLSTM model. It provides a detailed performance analysis for every category, highlighting both the model's accuracy in identifying attacks and its ability to minimize false alarms. The report confirms that the BiLSTM-based architecture maintains high metrics across all classes, including low-frequency attacks, indicating robust generalization and strong detection capabilities.

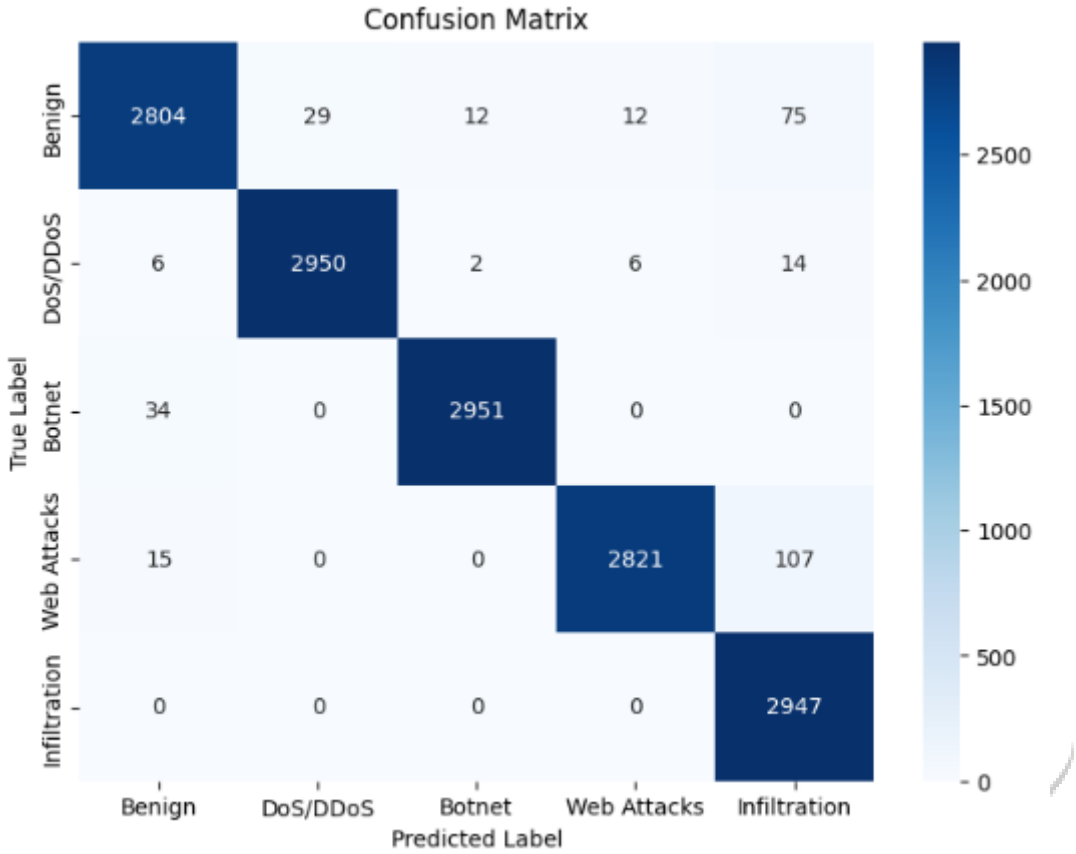

Figure 8 Confusion Matrix of FusionNet-GRU IDS (CNN–GRU)

This confusion matrix illustrates the classification outcomes of the FusionNet-GRU IDS model. It shows the model's ability to correctly identify benign traffic and malicious attacks while highlighting any misclassifications. Compared to the BiLSTM-based model, the GRU matrix demonstrates slightly higher off-diagonal elements, reflecting minor misclassifications. Nonetheless, the majority of samples are correctly predicted, confirming that the GRU model effectively captures temporal dependencies with reduced computational complexity.

CLASSIFICATION REPORT

	precision	recall	f1-score	support
Benign	0.9808	0.9563	0.9684	2932
DoS/DDoS	0.9903	0.9906	0.9904	2978
Botnet	0.9953	0.9886	0.9919	2985
Web Attacks	0.9937	0.9585	0.9758	2943
Infiltration	0.9376	1.0000	0.9678	2947
accuracy			0.9789	14785
macro avg	0.9795	0.9788	0.9789	14785
weighted avg	0.9796	0.9789	0.9789	14785

Figure 9 Classification report of FusionNet-GRU IDS (CNN–GRU) Model

The classification report provides a per-class evaluation of precision, recall, F1-score, and support for the FusionNet-GRU IDS model. It highlights the model's ability to detect different attack categories while minimizing false positives and negatives. Although slightly lower than the BiLSTM-based model, the GRU model maintains strong performance metrics across all classes, demonstrating that it is a

computationally efficient alternative with reliable detection capability for real-time intrusion detection scenarios.

5. CONCLUSION

This study proposed a cutting-edge intrusion detection framework leveraging a dual-stage data fusion strategy combined with hybrid deep learning models to enhance the detection and classification of cyberattacks in network traffic. The framework integrated behavioral ratio-based features, traffic intensity, temporal activity, and protocol-level interactions to create a comprehensive fused feature space, which was further refined using a neural encoder network. This approach allowed the models to capture both spatial correlations and temporal dependencies, improving discrimination between benign and malicious traffic. Two hybrid architectures, FusionNet-BiLSTM IDS (CNN–BiLSTM) and FusionNet-GRU IDS (CNN–GRU), were implemented and evaluated on the CIC-IDS 2018 dataset. Severe class imbalance, a critical challenge in intrusion detection, was effectively mitigated using SMOTE-ENN. SMOTE synthetically oversamples minority attack classes while ENN removes noisy and misclassified samples from majority classes, ensuring balanced representation across all attack types. This significantly improved the models' generalization performance and ability to detect low-frequency and stealthy attacks. Extensive exploratory data analysis (EDA) provided insights into dataset composition, attack distribution, and protocol behavior, guiding feature engineering and model design. Performance evaluation revealed that the FusionNet-BiLSTM IDS achieved superior metrics accuracy (0.9871), precision (0.9872), recall (0.9871), F1-score (0.9871), and loss (0.04) demonstrating robust detection across all attack categories. The FusionNet-GRU IDS offered slightly lower metrics but provided computational efficiency and faster training, making it suitable for real-time deployment. The results validate that the proposed hybrid deep learning and dual-stage feature fusion approach, combined with SMOTE-ENN balancing, significantly enhances intrusion detection accuracy, robustness, and reliability. By explicitly modeling directional asymmetries, interaction-based behaviors, and temporal patterns, this study presents a scalable, high-performance IDS framework, with potential extensions to multi-source datasets, adaptive attacks, and online learning scenarios, further strengthening cybersecurity resilience.

References

[1] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection," *Sci. Rep.*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-023-50554-x.

[2] N. Ahmed, B. Zahran, B. Ayyoub, A. R. Alzoubaidi, and A. Ngadi, "Classifiers and Optimum Feature Selection in Internet of Things (IoT)," vol. 14, no. April, pp. 51–61, 2024.

[3] D. Kumar, P. P. Pawar, B. Ananthan, S. Rajasekaran, and T. V. Prabhakaran, "Optimized Support Vector Machine Based Fused IoT Network Security Management," *2024 3rd Int. Conf. Artif. Intell. Internet Things, AIIoT 2024*, pp. 0–4, 2024, doi: 10.1109/AIIoT58432.2024.10574673.

[4] S. Hussain and T. Shehzadi, "Machine Learning-Powered Intrusion Detection: Safeguarding Networks In the Digital Era," *MZ J. Artif. Intell.*, vol. 1, no. 1, pp. 6–15, 2024.

[5] S. Muneer, U. Farooq, A. Athar, M. A. Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *J. Eng. (United Kingdom)*, vol. 2024, 2024, doi: 10.1155/2024/3909173.

[6] D. Jayalatchumy, R. Ramalingam, A. Balakrishnan, M. Safran, and S. Alfarhood, "Improved Crow Search-Based Feature Selection and Ensemble Learning for IoT Intrusion Detection," *IEEE Access*, vol. 12, no. January, pp. 33218–33235, 2024, doi: 10.1109/ACCESS.2024.3372859.

[7] J. Saini and R. Kait, "Exploring Machine Learning Strategies for Intrusion Detection in Wireless Sensor Networks," *2024 IEEE 9th Int. Conf. Converg. Technol. I2CT 2024*, pp. 1–8, 2024, doi: 10.1109/I2CT61223.2024.10543320.

[8] M. S. Mohammed and H. A. Talib, "Using Machine Learning Algorithms in Intrusion Detection Systems: A Review," *Tikrit J. Pure Sci.*, vol. 29, no. 3, pp. 63–74, 2024, doi: 10.25130/tjps.v29i3.1553.

[9] M. Bakro *et al.*, "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms

Along With Random Forest Model," *IEEE Access*, vol. 12, no. January, pp. 8846–8874, 2024, doi: 10.1109/ACCESS.2024.3353055.

[10] A. Algarni, Z. Ahmad, and M. Alaa Ala'anzy, "An Edge Computing-Based and Threat Behavior-Aware Smart Prioritization Framework for Cybersecurity Intrusion Detection and Prevention of IEDs in Smart Grids with Integration of Modified LGBM and One Class-SVM Models," *IEEE Access*, vol. 12, no. May, pp. 104948–104963, 2024, doi: 10.1109/ACCESS.2024.3435564.

[11] C. P. Kaliappan, K. Palaniappan, D. Ananthavadivel, and U. Subramanian, "Advancing IoT security: a comprehensive AI-based trust framework for intrusion detection," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 5, pp. 2737–2757, 2024, doi: 10.1007/s12083-024-01684-0.

[12] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, "Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 3, pp. 3512–3521, 2024, doi: 10.11591/ijece.v14i3.pp3512-3521.

[13] S. S. Vellela *et al.*, "Improving Network Security Using Intelligent Ensemble Techniques: An Integrated System for Detecting and Managing Intrusions in Computer Networks," *2024 Int. Conf. Adv. Mod. Age Technol. Heal. Eng. Sci. AMATHE 2024*, pp. 1–7, 2024, doi: 10.1109/AMATHE61652.2024.10582198.

[14] F. Sharif, "The Role of Ensemble Learning in Strengthening Intrusion Detection Systems: A Machine Learning Perspective," 2024, [Online]. Available: https://www.researchgate.net/publication/384366905

[15] P. Amin, G. D, A. Gantra, and P. Singhal, "Improved human identification by multi-biometric image sensor integration with a deep learning approach," *Int. J. Syst. Assur. Eng. Manag.*, pp. 1–20, 2024, doi: 10.1007/s13198-024-02573-8.

[16] H. Mohammed Fadhil, Z. O. Dawood, and A. Al Mhdawi, "Enhancing Intrusion Detection Systems Using Metaheuristic Algorithms," *Diyala J. Eng. Sci.*, vol. 17, no. 3, pp. 15–31, 2024, doi: 10.24237/djes.2024.17302.

[17] B. Konatham, T. Simra, F. Amsaad, M. I. Ibrahem, and N. Z. Jhanjhi, "A Secure Hybrid Deep Learning Technique for Anomaly Detection in IIoT Edge Computing," 2024, [Online]. Available: https://www.techrxiv.org/users/662346/articles/706122-a-secure-hybrid-deep-learning-technique-for-anomaly-detection-in-iiot-edge-computing?commit=e4d90929f9887c6d4c70d2e54cde6348880c8865

[18] W. K. Mohammed, M. A. Taha, and S. M. Mohammed, "A Novel Hybrid Fusion Model for Intrusion Detection Systems Using Benchmark Checklist Comparisons," *Mesopotamian J. CyberSecurity*, vol. 4, no. 3, pp. 216–232, 2024, doi: 10.58496/MJCS/2024/024.

[19] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00886-w.

[20] U. Ahmed *et al.*, *Explainable AI-based innovative hybrid ensemble model for intrusion detection*, vol. 13, no. 1. Springer Berlin Heidelberg, 2024. doi: 10.1186/s13677-024-00712-x.

[21] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discov. Artif. Intell.*, vol. 5, no. 1, pp. 1–38, 2025, doi: 10.1007/s44163-025-00578-1.

[22] V. Kandasamy and A. A. Roseline, "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks," *Sci. Rep.*, vol. 15, no. 1, pp. 1–26, 2025, doi: 10.1038/s41598-025-85547-5.

[23] B. Buyuktanir, Ş. Altinkaya, G. Karatas Baydogmus, and K. Yildiz, "Federated learning in intrusion detection: advancements, applications, and future directions," *Cluster Comput.*, vol. 28, no. 7, 2025, doi: 10.1007/s10586-025-05325-w.

[24] A. Mughaid, A. Alnajjar, S. M. El-Salhi, K. Almakadmeh, and S. AlZu'bi, "A cutting-edge intelligent cyber model for intrusion detection in IoT environments leveraging future generations

networks," *Cluster Comput.*, vol. 27, no. 8, pp. 10359–10375, 2024, doi: 10.1007/s10586-024-04495-3.

[25] P. Viboonsang and S. Kosolsombat, "Network Intrusion Detection System Using Machine Learning and Deep Learning," *Int. Conf. Cybern. Innov. ICCI 2024*, no. April, 2024, doi: 10.1109/ICCI60780.2024.10532673.

[26] H. Kheddar, D. W. Dawoud, A. I. Awad, Y. Himeur, and M. K. Khan, *Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review*, vol. 27, no. 4. IEEE, 2025. doi: 10.1109/COMST.2024.3484491.

[27] S. Afnan Birahim *et al.*, "Intrusion Detection for Wireless Sensor Network Using Particle Swarm Optimization Based Explainable Ensemble Machine Learning Approach," *IEEE Access*, vol. 13, no. January, pp. 13711–13730, 2025, doi: 10.1109/ACCESS.2025.3528341.

[28] Q. Gulzar and K. Mustafa, "Enhancing network security in industrial IoT environments: a DeepCLG hybrid learning model for cyberattack detection," *Int. J. Mach. Learn. Cybern.*, vol. 16, no. 7–8, pp. 4797–4815, 2025, doi: 10.1007/s13042-025-02544-w.

[29] M. Tawfik, *Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection*, vol. 19, no. 8 August. 2024. doi: 10.1371/journal.pone.0304082.

[30] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Comput.*, vol. 26, no. 6, pp. 4069–4083, 2023, doi: 10.1007/s10586-022-03810-0.