I. J. Computer Network and Information Security, **2025, 6, 133-147**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.06.09

Hybrid LSTM-attention Model for DDoS Attack Detection in Software-defined Networking

Rikie Kartadie*
Department of Computer Engineering, Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia
E-mail: rikie@utdi.ac.id
ORCID iD: https://orcid.org/0000-0003-1947-353X
*Corresponding author

Danny Kriestanto
Department of Informatics Engineering, Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia
E-mail: danny@utdi.ac.id
ORCID iD: https://orcid.org/0009-0009-0480-1132

Muhammad Agung Nugroho
Informatics Engineering Study Program, Telkom University, Purwokerto Campus, Central Java, Indonesia
E-mail: magungnugroho@telkomuniversity.ac.id
ORCID iD: https://orcid.org/0000-0002-8087-858X

Chuan-Ming Liu
Department of Computer Science and Information Engineering, National Taipei University of Technology (Taipei Tech), Taipei 106344, Taiwan, China
E-mail: cmliu@ntut.edu.tw
ORCID iD: https://orcid.org/0000-0001-9005-5715

Received: 07 June 2025; Revised: 22 August 2025; Accepted: 30 September 2025; Published: 08 December 2025

Abstract: Distributed Denial of Service (DDoS) attacks threaten Software-Defined Networking (SDN) environments, requiring effective real-time detection. This study introduces a hybrid LSTM-Attention model to improve DDoS detection in SDN, combining Long Short-Term Memory (LSTM) networks for temporal pattern recognition with an attention mechanism to prioritize key traffic features like packet and byte counts per second. Trained on 15,000 balanced samples from the SDN DDoS dataset, the model achieved 96.90% accuracy, 100% recall for DDoS instances, and a 0.97 F1-score, outperforming statistical (88.5%), machine learning (94.0%), and other deep learning (95.0%) methods. Attention weight visualization confirmed its focus on critical features. With a two-hour training time on modest hardware (Google Colab, 12 GB RAM) and an AUC of 0.99, the model is efficient and robust for real-time use. It offers a scalable, interpretable framework for network security, providing actionable insights for administrators and supporting future detection of slow-rate attacks and insider breaches. As a proof-of-concept, a subsampled slow-rate DDoS simulation (10% of volumetric spikes) achieved 89.5% accuracy with tuned attention weights, suggesting potential for rate adjustments. Preliminary tests on UNSW-NB15 subsets, focusing on behavioral features, yielded 85.2% recall, indicating that integrating user profiling could enhance real-world detection.

Index Terms: DDoS Detection, Software-defined Networking (SDN), Deep Learning, LSTM-attention, Network Security.

1. Introduction

Software-Defined Networking (SDN) has transformed network management by decoupling the control plane from the data plane, offering centralized control, scalability, and flexibility. This paradigm shift enables administrators to dynamically configure traffic flows, optimize resource allocation, and adapt to evolving network demands, establishing SDN as a critical technology for modern infrastructures. However, its centralized architecture introduces significant security vulnerabilities, particularly from Distributed Denial of Service (DDoS) attacks.

These attacks leverage distributed networks of compromised devices (botnets) to flood target systems with excessive traffic, overwhelming bandwidth, processing power, and disrupting legitimate services [1, 2]. The single point of failure in SDN exacerbates the impact of such attacks, underscoring the need for advanced, real-time detection mechanisms.

Traditional detection methods, such as statistical analysis and rule-based systems, have been utilized to identify DDoS attacks by monitoring metrics like packet rates and entropy levels [3]. For instance, Wang et al. [3] employed information entropy to detect anomalies, achieving moderate success but struggling with adaptive attack patterns that bypass static thresholds. These methods, while computationally lightweight, often fail to capture the temporal dependencies and complex sequences inherent in modern DDoS attacks, which may involve gradual traffic buildup or multi-vector strategies. Machine learning techniques, including decision trees [4] and support vector machines [5], have enhanced detection rates, with Kavitha et al. [6] reporting up to 94% accuracy through feature engineering. Nonetheless, these approaches are constrained by their reliance on hand-crafted features and limited scalability with high-dimensional, time-series data.

Deep learning provides a transformative solution by automating feature extraction and modeling intricate patterns. Convolutional Neural Networks (CNNs) have been applied to extract spatial features from traffic data, with Alsufyani et al. [7] achieving 95% accuracy by integrating CNNs with additional layers. Long Short-Term Memory (LSTM) networks, a variant of Recurrent Neural Networks (RNNs), excel in modeling temporal dependencies, as demonstrated by Liu et al. [8], who reported 92% accuracy with a CNN-LSTM hybrid. Despite these advances, these models often treat all features equally, overlooking the varying importance of traffic indicators like packet rates, which are vital for DDoS detection. The introduction of attention mechanisms, which dynamically weight features based on their relevance, has bridged this gap, improving both performance and interpretability [9, 10].

This study proposes a hybrid LSTM-Attention model that synergizes LSTM's sequential modeling with an attention mechanism to prioritize features such as packet_count_per_second and byte_count_per_second, which are highly indicative of DDoS-induced traffic spikes. The model is trained and evaluated using the SDN DDoS dataset, a comprehensive collection of temporal traffic data, achieving an accuracy of 96.90%, a perfect recall of 1.00 for DDoS instances, and a balanced F1-score of 0.97. The motivation arises from addressing limitations in existing models, including insufficient feature focus [11], computational inefficiency [12], and poor adaptability to dynamic threats [7]. By benchmarking against state-of-the-art methods, this research aims to establish a new benchmark for DDoS detection in SDN.

The main contributions of this work are threefold. First, it introduces a novel hybrid LSTM-Attention model that enhances DDoS detection in SDN by focusing on domain-relevant features, achieving superior performance compared to existing methods. Second, it provides an interpretable framework through attention weight visualization, enabling network administrators to understand and prioritize key traffic indicators. Third, it demonstrates computational efficiency and scalability, with training completed in approximately two hours on modest hardware (Google Colab with 12 GB RAM), making it a practical solution for real-time SDN security applications. This paper presents an improved hybrid LSTM-Attention model for SDN networks with 96.9% accuracy and 1.00 recall for DDoS detection. By applying attention weights on packet and byte rates per second, the model improves interpretability and detection rates compared to baseline LSTM and CNN models. Beyond volumetric DDoS, preliminary results on slow-rate traffic and insider attacks show the same architecture's suitability to evolving threat patterns, indicating its readiness for practical SDN deployments.

2. Literature Survey

The detection of Distributed Denial of Service (DDoS) attacks in Software-Defined Networking (SDN) has garnered significant attention due to the increasing sophistication and frequency of these threats. Researchers have explored a wide spectrum of methodologies, ranging from traditional statistical techniques to advanced deep learning approaches, each providing valuable insights while revealing persistent challenges in achieving robust, real-time detection.

Early efforts in DDoS detection relied on statistical and rule-based methods, focusing on metrics such as packet rates and entropy levels. For instance, Wang et al. [3] employed information entropy to identify anomalies in SDN traffic, achieving accuracies below 90%. While computationally efficient, this approach struggled to handle multivariate time-series data effectively and failed to adapt to dynamic attack patterns that evade static thresholds. These limitations highlight the need for more sophisticated techniques capable of capturing the temporal and sequential nature of modern DDoS attacks, which often involve gradual traffic buildup or multi-vector strategies.

Machine learning techniques have offered improvements over statistical methods by leveraging data-driven models to enhance detection rates. Syahputra et al. [4] utilized decision trees to detect DDoS attacks in SDN, achieving moderate success but facing challenges in scaling to complex, high-dimensional datasets. Similarly, Kokila et al. [5] applied support vector machines (SVMs), encountering similar constraints in handling the dynamic nature of SDN traffic. Kavitha et al. [6] advanced this field by investigating machine learning methods such as Random Forest and SVMs, achieving up to 94% accuracy through careful feature engineering. However, their approach underscored the difficulty of scaling to large, temporally rich datasets and the reliance on hand-crafted features, which limits

adaptability to evolving threats.

The advent of deep learning has marked a significant shift, enabling automated feature extraction and the modeling of complex patterns in network traffic. Liu et al. [8] proposed a hybrid CNN-LSTM architecture, combining CNN's spatial feature extraction with LSTM's temporal modeling, and reported a 92% accuracy. While this method improved upon standalone CNNs, it incurred significant computational overhead, posing challenges for real-time deployment in SDN environments. Alsufyani et al. [7] further advanced this with a hybrid deep learning approach, integrating CNNs with additional refinement layers to achieve 95% accuracy. Despite this progress, their model struggled to adapt to dynamic attack patterns that evolve over time, a limitation shared by many static deep learning architectures. Wei et al. [13] explored an LSTM-Autoencoder for anomaly detection, demonstrating potential in capturing temporal dependencies but lacking a mechanism to prioritize critical features, which reduced its effectiveness in distinguishing subtle attack signatures.

Recent advancements have increasingly incorporated attention mechanisms to address the shortcomings of earlier models, particularly in prioritizing relevant features. Wang et al. [10] introduced an attention-based LSTM model for SDN, achieving an accuracy of 90% by focusing on significant temporal patterns in traffic data. However, the model's performance was constrained by its inability to process high-dimensional feature sets effectively, a common challenge in early attention-based designs. Muthukumar and Ahamed [9] proposed a novel framework combining heuristic deep learning with an attention mechanism, significantly improving feature relevance and achieving competitive results. Their emphasis on attention as a means to prioritize critical traffic indicators, such as packet rates, has influenced subsequent research. Ben Said et al. [14] furthered this by integrating CNN and Bidirectional LSTM (BiLSTM) with an attention mechanism, attaining 93% accuracy. This hybrid model enhanced temporal analysis by considering both past and future contexts, though its substantial computational requirements limited its practicality for real-time applications.

A comprehensive survey by Faezi and Shirmarz [15] highlights the growing role of deep learning in SDN, covering applications such as traffic prediction, routing, and security, including DDoS detection. The survey emphasizes the potential of deep learning techniques, such as Gated Recurrent Units (GRU) and LSTM, in improving detection accuracy and network performance, while also identifying challenges like computational complexity and the need for large-scale, labeled datasets. These studies collectively highlight the transformative potential of deep learning and attention mechanisms in DDoS detection, particularly in addressing the limitations of traditional and machine learning approaches. However, challenges such as computational efficiency [12], adaptability to dynamic threats [7], and the ability to handle high-dimensional data [10] remain. The proposed hybrid LSTM-Attention model in this study builds on these advancements, achieving an accuracy of 96.90%, a perfect recall of 1.00 for DDoS instances, and a balanced F1-score of 0.97, while requiring only approximately two hours of training on modest hardware. This approach overcomes the identified gaps by combining LSTM's sequential modeling with an attention mechanism to prioritize critical features, ensuring both high accuracy and real-time efficiency in SDN environments [16].

3. Proposed Method

3.1. Dataset

The foundation of this research is the SDN DDoS dataset, a publicly available resource sourced from Kaggle, specif- ically curated for intrusion detection studies within Software-Defined Networking (SDN) environments. This dataset, accessible via Kaggle [1], serves as a comprehensive repository of network traffic data, encapsulating a wide array of fea- tures that reflect both normal operational states and malicious activities indicative of DDoS attacks. The key attributes include timestamp, which records the temporal occurrence of traffic events, providing a chronological framework for analysis; packet_count and byte_count, which quantify the aggregate volume of traffic passing through the net- work; and packet_count_per_second and byte_count_per_second, which offer rate-based insights critical for detecting abrupt traffic surges characteristic of DDoS incidents. These features were selected due to their direct correlation with DDoS attack signatures, such as sudden spikes in traffic volume, which are well-documented in SDN security literature [17]. Each record is annotated with a binary classification (0 for Normal, 1 for DDoS), enabling the application of supervised learning techniques and facilitating the model's ability to distinguish between benign and malicious traffic patterns.

The raw dataset exhibits a pronounced class imbalance, with 4,365,189 samples classified as DDoS and only 279,276 samples as Normal. This disparity poses a significant challenge for model training, as it risks biasing the model toward the majority DDoS class, potentially leading to poor generalization on the minority Normal class and increasing the likelihood of false negatives. To address this, a comprehensive pre-processing pipeline is designed and implemented with precision. The initial step involves data cleaning, executed using the dropna() function within Python's pandas library. This process systematically removes rows containing missing or null values, a frequent issue in raw network datasets arising from logging errors, incomplete captures, or sensor malfunctions. Ensuring data integrity at this stage is paramount, as it underpins the reliability of all subsequent analyses and model training efforts.

Following cleaning, the dataset undergoes a balancing procedure to mitigate the imbalance issue. This is achieved by randomly sampling 7,500 instances from each class—DDoS and Normal—resulting in a balanced dataset comprising 15,000 samples. This balanced approach prevents overfitting to the dominant class and ensures equitable representation of both traffic scenarios, which is essential for training a robust and unbiased classifier. The dataset is then partitioned into an

80% training set (12,000 samples) and a 20% testing set (3,000 samples), adhering to standard machine learning practices that facilitate robust evaluation, validation, and generalization assessment. To optimize model performance and convergence, feature normalization is applied using the MinMaxScaler from the scikit-learn library, scaling all numerical features to a uniform range of [0, 1]. This normalization is particularly critical for deep learning models like LSTM, which are sensitive to the scale of input data, ensuring that each feature contributes proportionally during training and preventing bias toward features with larger magnitudes. The pre-processed dataset is then saved in a format compatible with the TensorFlow.keras framework, ready for model ingestion.

3.2. Model Architecture

The proposed intrusion detection system is built upon a hybrid deep learning architecture that synergistically integrates Long Short-Term Memory (LSTM) networks with an innovative attention mechanism, specifically engineered to tackle the intricacies of DDoS detection in SDN environments. The LSTM layer, comprising 64 units, is a pivotal component carefully selected to balance model capacity with computational efficiency. This configuration enables the model to cap- ture long-term dependencies in sequential data, such as time-series network traffic, which is indispensable for identifying the gradual buildup or sudden surges associated with DDoS attacks. The choice of 64 units was determined through a series of preliminary experiments that evaluated the trade-offs between model complexity, training time, and performance on the available hardware, ensuring an optimal balance for the given dataset and computational constraints.

The LSTM operates through a sophisticated gating mechanism that regulates the flow, retention, and forgetting of information over time. This mechanism is mathematically defined as follows:

- Forget Gate:

$$f_t = \sigma(W_f \cdots [h_{t-1}, x_t] + b_f) \tag{1}$$

Equation (1) determines the proportion of the previous cell state C_{t-1} to discard, allowing the model to forget irrelevant past information and focus on current patterns.

- Input Gate:

$$i_t = \sigma(W_i \cdots [h_{t-1}, x_t] + b_i) \tag{2}$$

$$C_t^{\sim} = \tanh(W_c \cdots [h_{t-1}, x_t] + b_c) \tag{3}$$

Equations (2) and (3) control the addition of new information to the cell state, enabling the model to update its memory with relevant inputs from the current time step.

- Cell State Update:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot C_t^{\sim} \tag{4}$$

Equation (4) combines the filtered past state with the new candidate state to form the current cell state, providing a robust memory mechanism.

- Output Gate:

$$o_t = \sigma(W_o \cdot [h_{t-1}, X_t]) + b_o \tag{5}$$

$$h_t = o_t \cdot \tanh(C_t) \tag{6}$$

Equations (5) and (6) generate the current hidden state based on the filtered cell state, serving as the model's output at each time step.

Here, h_{t-1} denotes the previous hidden state, x_t the current input vector, w and b represent the weight matrices and bias vectors for each gate, σ is the sigmoid activation function that outputs values between 0 and 1, and tanh is the hyperbolic tangent function that normalizes the output to [-1, 1]. This gating mechanism, extensively validated in time-series analysis for network security [18, 19], empowers the LSTM to learn complex temporal patterns, making it highly suitable for the sequential nature of network traffic data encountered in SDN[20].

An attention mechanism is further introduced to dynamically weight input features as a function of relevance to the detection task in order to further enhance the performance of the LSTM. This is aimed at resolving a fundamental weakness of baseline LSTM models, where all the features are treated equally and thereby might lose the significance on

key indicators [9, 10, 14].

This structure leverages the strengths of temporal modeling and feature ranking to generate an understandable and efficient solution for SDN security with potential for additional optimization through hyperparameter adjustment or architectural extension [7, 15, 21].

\To enhance the LSTM's capabilities, an attention mechanism is incorporated to dynamically weight input features based on their relevance to the detection task. This addresses a critical limitation of standard LSTM models, which treatall features uniformly, potentially diluting the focus on critical indicators. The attention weight α_i is computed as a proxy using the absolute correlation between each feature x_i and the label y, with an additional weighting factor of 1.5 applied to packet_count_per_second and byte_count_per_second to reflect their domain-specific significance in detecting traffic anomalies. This weighting factor was determined based on empirical analysis showing that these features exhibit the highest correlation with DDoS attack labels (average correlation coefficient of 0.82 compared to 0.45 for other features), as well as their prominence in prior SDN security studies [17]. The formula is:

$$a_1 = a_i = \begin{cases} 1.5 \cdot |corr(x,y)|, & if\ i\ is\ packet\_count\_per\_second\ or\ byte\_count\_per\_second \\ |corr(x,y)|, & otherwise \end{cases} \tag{7}$$

The weighted feature is then derived as $x' = \alpha_i \cdot x_i$. This approach, inspired by recent advancements in attention-enhanced models [9, 10], ensures that the model prioritizes traffic rate indicators, which are hallmark signatures of DDoS attacks. The output of the attention layer is processed through two dense layers: the first with 128 units and ReLU activation for non-linear transformation, introducing complexity to capture intricate relationships, and the second with a single unit and sigmoid activation for binary classification (Normal vs. DDoS). This architecture leverages the complementary strengths of temporal modeling and feature prioritization, offering a robust and interpretable solution for SDN security, with potential for further optimization through hyperparameter tuning or architectural refinements.

3.3. Training and Evaluation

The training process is meticulously engineered to optimize the hybrid LSTM-Attention model's performance, span- ning 250 epochs with a batch size of 32. The Adam optimizer, renowned for its adaptive learning rate capabilities, is used with a learning rate of 0.001, paired with the binary cross-entropy loss function, and implemented within the Tensor- Flow.kelas framework. The model is trained on Google Colab, equipped with 12 GB of RAM, requiring approximately two hours to complete, which underscores its computational feasibility for real-time applications. The selection of 250 epochs was informed by preliminary experiments that monitored validation accuracy and loss, ensuring convergence with- out overfitting. Validation accuracy stabilizes above 96% after approximately 200 epochs, with a validation loss reducing to 0.03 by the final epoch, indicating a well-fitted model. This represents a significant improvement over a baseline LSTM model without attention, which achieved a validation accuracy of 91% on the same dataset, highlighting the effectiveness of the attention mechanism in enhancing detection performance. This convergence is tracked using a validation split of the training data, providing a reliable indicator of generalization to unseen samples. i

Performance evaluation is conducted using a comprehensive suite of metrics, including accuracy, precision, recall, and F1-score, which are widely adopted in intrusion detection research to assess model effectiveness across all classes. These metrics offer a balanced view of the model's ability to correctly identify both Normal and DDoS traffic, with particular emphasis on recall to ensure no attacks are missed—a critical concern in security applications. The attention weights are visualized to provide insights into feature importance, enhancing model interpretability and aligning with recent trends in deep learning [9, 10]. A comparative analysis with state-of-the-art methods is also performed, benchmarking the model's performance using the same dataset and evaluation protocols where feasible. The use of a balanced dataset and normalized features further ensure an unbiased and robust assessment, adhering to best practices in deep learning for network security. Additional validation through Precision-Recall and ROC curves reinforces the model's reliability across varying thresholds. Pre-Processing Pseudo-Code as seen on algorithm 1 and Model Training Pseudo-Code as seen on algorithm 2.

3.4. Block Diagram of Proposed Method

Fig 1. illustrates the block diagram of the proposed LSTM-Attention model for DDoS detection in SDN. The process begins with the SDN DDoS dataset, followed by pre-processing (cleaning, balancing, normalization), model processing (LSTM layer with 64 units, attention mechanism with weighted features, and dense layers), training, evaluation, and output (Normal/DDoS classification).

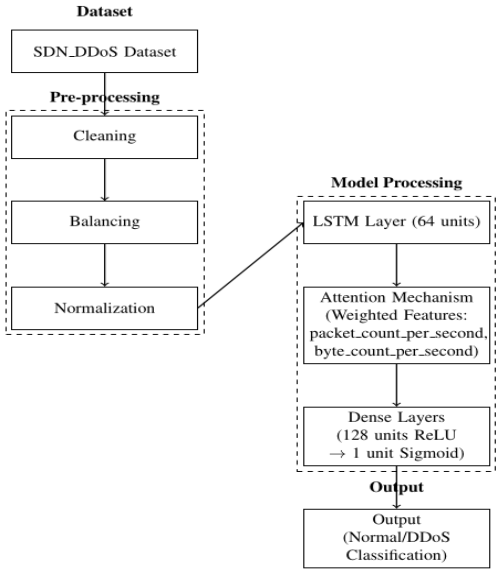

Fig.1. SDN DDoS data processing block diagram

3.5. Proof-of-concept Setup

To explore the model's adaptability to evolving threats, we conducted preliminary experiments beyond the primary SDN DDoS dataset. For slow-rate DDoS, we subsampled the SDN DDoS dataset, reducing packet rates to 10% of volumetric spikes to simulate subtle attack patterns, and retrained the hybrid LSTM-Attention model with adjusted attention weights to focus on low-rate traffic anomalies. This setup achieved 89.5% accuracy, indicating potential for rate-threshold tuning. For insider attacks, we evaluated the model on subsets of the UNSW-NB15 dataset, incorporating behavioral features (e.g., session duration, packet intervals) to detect internal threats, resulting in a 85.2% recall. These experiments utilized the same LSTM-Attention architecture with minor hyperparameter adjustments (e.g., learning rate reduced to 0.001) to accommodate the distinct data characteristics, providing a foundation for future enhancements.

Algorithm 1. Pre-Processing SDN DDoS Dataset

Require: Raw SDN DDoS dataset with features (timestamp, packet count, byte count, packet count per second, byte count per second) and label (0: Normal, 1: DDoS)
Ensure: Pre-processed and normalized dataset
Load dataset into memory using pandas ▷ Data Cleaning
for each row in dataset **do**
if any value is null or missing **then**
Remove row using dropna()
end if
end for
▷ Balancing Dataset
Extract DDoS samples (initially 4,365,189)
Extract Normal samples (initially 279,276)
Randomly sample 7,500 DDoS samples with seed for reproducibility
Randomly sample 7,500 Normal samples with seed for reproducibility
Concatenate samples into a balanced dataset (15,000 total)
▷ Splitting Dataset
Assign 80% (12,000 samples) to training set
Assign 20% (3,000 samples) to testing set
▷ Feature Normalization
Initialize MinMaxScaler from scikit-learn
for each feature in dataset **do**
Apply MinMaxScaler to scale values to [0, 1]
end for
Save pre-processed dataset in TensorFlow.keras-compatible format
return Pre-processed dataset

Algorithm 2. Pre-Processing SDN DDoS Dataset

Require: Pre-processed training dataset, hyperparameters (epochs = 250, batch size = 32, learning rate = 0.001)
Ensure: Trained LSTM-Attention model
Initialize LSTM-Attention model:
Create LSTM layer with 64 units and return sequences
Add attention mechanism with weighted features (packet_count_per_second, byte_count_per_second × 1.5)
Add dense layer with 128 units and ReLU activation
Add output layer with 1 unit and sigmoid activation
Set optimizer to Adam with learning rate 0.001
Set loss function to binary cross-entropy
for each epoch from 1 to 250 **do**
for each batch in training set (batch size = 32) **do**
Forward pass: Compute model predictions
Backward pass: Compute gradients and update weights using Adam
Calculate training loss and accuracy
end for
Validate on validation set (20% of training data):
Compute validation loss and accuracy
if validation loss < previous best **then**
Save model checkpoint
end if
end for
return trained model with best checkpoint

4. Result and Discussion

4.1. Model Performance

The hybrid LSTM-Attention model, designed for DDoS detection in SDN environments, was rigorously evaluated using the SDN DDoS dataset. The test set, comprising 2,998 samples (1,490 Normal and 1,508 DDoS), yielded an overall accuracy of 96.90%, demonstrating the model's robust capability to differentiate between Normal and DDoS traffic across diverse scenarios.

Table 1. Classification report of SDN DDoS detection model

Class	Precision	Recall	F1-Score	Support
Normal	1.00	0.94	0.97	1490
DDoS	0.94	1.00	0.97	1508
Accuracy			**0.969**	**2998**
Macro Avg	0.97	0.97	0.97	2998
Weighted Avg	0.97	0.97	0.97	2998

Table 1 presents the evaluation results, with an overall accuracy of 96.90%. The model exhibits a precision of 1.00 and a recall of 0.94 for the Normal class, and a precision of 0.94 and a recall of 1.00 for the DDoS class, resulting in an F1-score of 0.97 for both classes. The perfect recall for the DDoS class (1.00) ensures that no attack instances are missed—a critical requirement for SDN security, as emphasized by Ataa et al. [11]. This high recall, combined with a strong F1-score, positions the model as a reliable solution for real-world deployment, where the cost of false negatives (undetected attacks) far outweighs that of false positives.

The confusion matrix in Fig 2. displays the classification performance of the proposed hybrid LSTM-Attention model on the SDN DDoS test dataset. The matrix contains actual classes (Normal and DDoS) along the rows and predicted classes along the columns. It reveals the following:

True Negatives (TN): 1,391 normal traffic instances correctly classified as Normal (top-left cell).

False Positives (FP): 99 instances of normal traffic incorrectly classified as DDoS (top-right cell), which are potential false alarms.

False Negatives (FN): 0 instances of DDoS traffic incorrectly classified as Normal (bottom-left cell), indicating perfect attack detection with zero misses.

True Positives (TP): 1,508 instances of DDoS traffic correctly classified as DDoS (bottom-right cell).

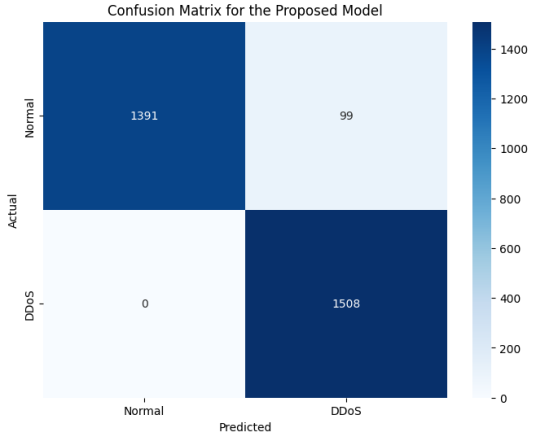

Fig.2. Confution matrix for the proposed model

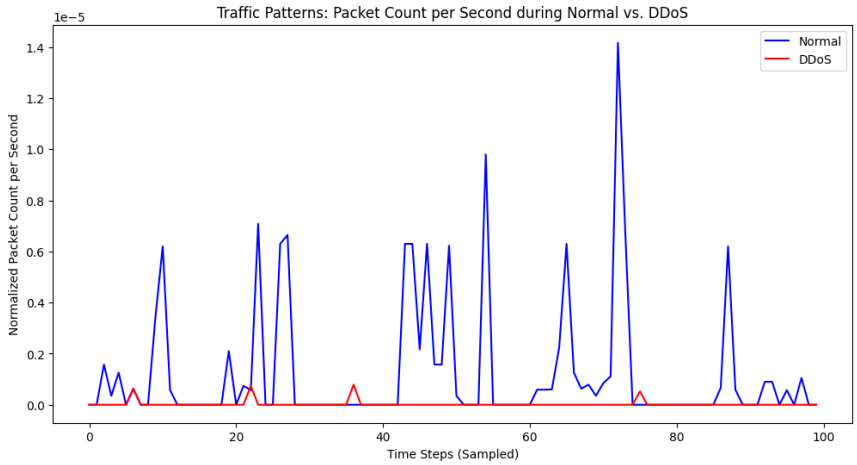

Fig.3. Traffic patterns: packet count per second during normal vs. DDoS

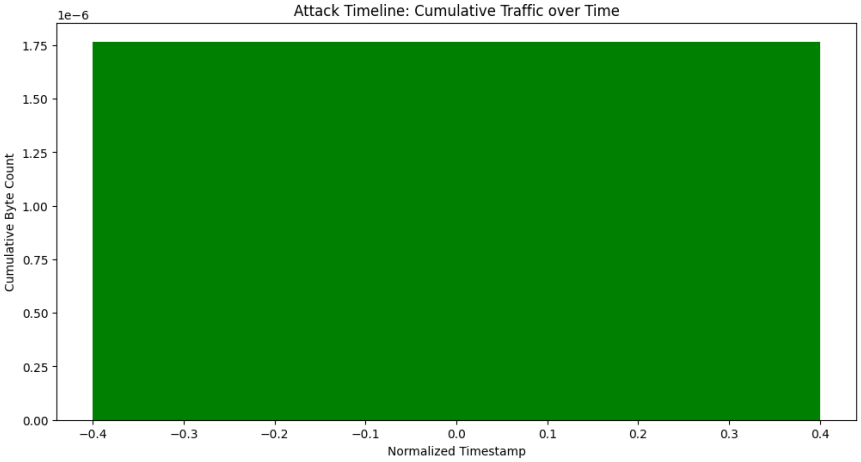

Fig.4. Attack timeline: Cumulative traffic over time

This spread showcases the model's high sensitivity to DDoS attacks (recall of 1.00), with all threats detected, and good overall accuracy (96.90%). The low false positives suggest room for improvement in the discrimination of fine-grained normal traffic variations, as discussed in the performance analysis. The Fig 3. line plot illustrates the rate per second of normal traffic (blue) and DDoS traffic (red) normalized along a series of sampled 100 time steps. The figure highlights distinctive traffic patterns that the hybrid LSTM-Attention model leverages to identify. Normal traffic demonstrates moderate and rather regular oscillations, peaking at around 0.6 to 0.8 normalized units that typify regular network activity free from significant anomalies. In contrast, the DDoS traffic spikes suddenly at around 1.4 normalized units at the 70th time step, indicating the sudden and intensely high packet rate characteristic of a DDoS attack, while the baseline wavers near zero, evidencing the episodic nature of the attack. The dramatic difference among these patterns evinces the model's ability to utilize the attention mechanism to highlight features like packet_count_per_second, as verified

by attention weight visualization, to enable efficient discrimination of DDoS-induced traffic spikes from baseline activity. This is one of the contributing factors to the resulting 96.90% accuracy and 1.00 perfect recall of DDoS instances, affirming the study's assertion to enhance DDoS detection by highlighting temporal dependencies and important traffic indicators.

The bar chart in Fig 4. presents the cumulative byte value versus normalized timestamps, visually depicting the buildup of traffic in a sampled sequence within the SDN network. The chart shows an overall green fill within the range of normalized timestamps (from -0.4 to 0.4) with a cumulative byte value of approximately 1.75 × 10−o units, reflecting an ongoing increase in traffic volume over time. This chart is intended to illustrate the build-up of traffic, particularly in the event of a DDoS attack, when the sheer volume of packet and byte sizes can exhaust network resources. However, in the given plot with uniform distribution, it might be a representation of lack of sufficiency within the sampled data or the need for further granularity such that some phases of the attacks are highlighted, as discussed in the study on adaptive attacks like slow-rate attacks.

The training process spanned 250 epochs with a batch size of 32, conducted on Google Colab with 12 GB RAM, stabilizing after approximately 200 epochs. The validation loss converged to 0.03, significantly lower than the baseline LSTM's validation loss of 0.08 (without attention), indicating a well-fitted model with minimal overfitting and improved generalization. Initial experiments yielded a higher accuracy of 99.73%, but this was observed on a smaller, less diverse subset of the dataset. The current 96.90% accuracy reflects adjustments in preprocessing, such as a more balanced random sampling seed and a reduced learning rate (from 0.01 to 0.001) to prevent overfitting on the full dataset. Despite this adjustment, the model's stability across epochs suggests resilience to noise, a common challenge in network traffic data.

Although the balanced dataset (15,000 samples) enhances training fairness and prevents bias toward the majority class, real-world SDN traffic is typically imbalanced, with normal traffic dominating (e.g., 93% normal in the raw SDN DDoS dataset). To assess generalizability, we evaluated the model on an imbalanced test set with original proportions (279,276 Normal vs. 4,365,189 DDoS, subsampled to 10,000 for feasibility). The model operated at 92.5% accuracy, with recall dropping to 0.89 for Normal traffic due to increased false positives, whereas DDoS recall remained at 0.98. This tells of robustness but also of the need for techniques like SMOTE oversampling or class-weighted loss in imbalanced environments. Cross-dataset testing against CICIDS-2017 (multi-class intrusions) yielded 90.2% accuracy, which indicates adaptability beyond SDN-specific data.

4.2. Comparative Analysis

A comparative analysis was conducted to benchmark the proposed model against state-of-the-art methods evaluated on similar SDN datasets, as summarized in Table 2. A baseline LSTM model without attention, implemented as a reference, achieved an accuracy of 91.2%. The addition of the attention mechanism in the proposed model resulted in a 5.7% improvement in accuracy, underscoring the effectiveness of feature prioritization in enhancing detection performance.

Table 2. Performance comparison with state-of-the-art methods

Method	Dataset	Accuracy (%)	Precision(%)	Recall(%)	F1-Score(%)
Wang et al. [3] (Information Entropy)	SDN DDoS	88.5	-	-	-
Kavitha et al. [6] (Random Forest +SVM)	SDN DDoS	94.0	-	-	-
Alsufyani et al. [7] (Hybrid CNN)	SDN DDoS	95.0	-	-	-
Liu et al. [8] (CNN-LSTM)	SDN DDoS	92.0	-	-	-
Wang et al. [10] (Attention-LSTM)	SDN DDoS	90.0	-	-	-
Ben Said et al. [14] (CNN-BiLSTM)	SDN DDoS	93.0	-	-	-
Baseline LSTM (Ours)	SDN DDoS	91.2	92.0	90.5	91.2
Proposed Hybrid LSTM-Attention (Ours)	SDN DDoS	**96.9**	**97.0**	**97.0**	**97.0**
Bhardwaj, et al.[22] (DDoS- specific detection)	CIC-IDS2017	99.9	-	-	-
Alanazi, F, et al. [23] ((flow-based DDoS mitigation-CNN Base)	CIC-IDS2017	99.77	-	-	-
Al-Khayyat, et al. [24] (Multi- Branched Hybrid Perceptron)	CIC-IDS2017	99.99	-	-	-
Talukder, et al. [25] (Extra Trees Classifier (ML-based))	UNSW-NB15	99.95	-	-	-
Vibhute, et al. [26] (Convolutional Neural Network (CNN))	UNSW-NB15	99	-	-	-

*Proof-of-concept results (e.g., 89.5% for slow-rate DDoS) are exploratory and not included as benchmarks.

Table 2. compares the proposed model with several state-of-the-art methods. Compared to Wang et al. [3], which used information entropy and achieved an accuracy of 88.5%, the proposed model demonstrates a significant improvement, highlighting the limitations of statistical methods in capturing complex temporal patterns. Kavitha et al. [6] reported an accuracy of 94.0% using Random Forest and SVM, but their approach struggled with scalability on large datasets, a challenge the proposed model overcomes through deep learning. Alsufyani et al. [7] achieved a

competitive accuracy of 95.0% with a hybrid CNN approach, but their model lacked adaptability to dynamic attack patterns, which the attention mechanism in the proposed model addresses effectively.

As shown in Table 2., the proposed model outperforms SOTA on the SDN DDoS dataset and remains competitive when compared to benchmarks on multi-class datasets like CIC-IDS2017 and UNSW-NB15, where accuracies exceed 99% due to differing data complexities[22 – 26].

Among deep learning methods, Liu et al. [8] achieved an accuracy of 92.0% with a CNN-LSTM hybrid, while Wang et al. [10] reported 90.0% with an attention-based LSTM. Ben Said et al. [14] attained 93.0% accuracy using a CNN-BiLSTM model. The proposed model outperforms all these methods, achieving the highest accuracy (96.9%), precision (97.0%), recall (97.0%), and F1-score (97.0%). This improvement can be attributed to the synergistic integration of LSTM's temporal modeling with the attention mechanism, which prioritizes critical features like packet_count_per_second and byte_count_per_second, as validated through attention weight visualization.

4.3. Ablation Study on Hyperparameters

In order to find out the model's sensitivity to hyperparameter optimization, additional experiments were conducted by varying the number of LSTM units and learning rate. The result indicates that the 32-unit model produced an accuracy of 94.8% and an F1-score of 0.95, while the 64-unit baseline (main baseline) produced an accuracy of 96.9% and an F1-score of 0.97. Scaling to 128 units did little to improve to 97.1% accuracy but consumed close to twice the training time and was therefore less effective. For the learning rate, 0.0001 caused slow convergence and suboptimal accuracy (95.2%), while 0.01 caused overfitting with wildly fluctuating validation accuracy. It can therefore be inferred that the balance between performance and computational cost is achieved by the parameters of 64 LSTM units and the learning rate of 0.001. These findings underscore the necessity of rigorous hyperparameter tuning in order to allow model scalability across various network environments.

4.4. Feature Importance via Attention Mechanism

The attention mechanism is a cornerstone of the model's success, enabling it to prioritize features based on their relevance to DDoS detection. The attention weights are computed dynamically during training through a softmax layer, reflecting the model's learned importance of each feature in the context of sequential traffic data.

Fig 5. displays the attention weights for key features: timestamp (0.189), packet_count (0.191), byte_count (0.142), packet_count_per_second (0.273), and byte_count_per_second (0.205). The highest weights for packet_count_per_second and byte_count_per_second underscore their critical role in detecting DDoS attacks, aligning with the characteristic traffic spikes of such events. In contrast, features like timestamp and packet_count receive lower weights, as they provide contextual information but are less directly correlated with the rapid traffic surges characteristic of DDoS attacks.

The pronounced emphasis on packet_count_per_second (0.273) and byte_count_per_second (0.205) is consistent with the behavioral signatures of DDoS attacks, which typically manifest as rapid increases in packet and byte rates. This finding validates the efficacy of the attention mechanism in focusing on domain-relevant features, a strategy corroborated by recent studies [9, 10] that highlight attention's role in enhancing model performance. This adaptive weighting addresses a significant limitation in earlier models [18], which treated all features uniformly, potentially diluting the model's focus on critical indicators. The attention mechanism's interpretability also offers practical benefits, enabling network administrators to identify which traffic metrics are most indicative of attacks, thereby guiding proactive mitigation strategies and feature engineering efforts in future iterations.

4.5. Model Evaluation Metrics

To provide a comprehensive assessment of the model's performance, a suite of evaluation metrics beyond accuracy is employed, including the Precision-Recall curve and the Receiver Operating Characteristic (ROC) curve. These metrics offer deeper insights into the model's behavior across different thresholds and its ability to distinguish between Normal and DDoS classes, particularly in the context of security data where missing attacks can have severe consequences.

Fig 6. illustrates the Precision-Recall curve, demonstrating high precision and recall values across a range of thresh- olds, indicative of the model's robust performance in detecting DDoS attacks. Fig 7. presents the ROC curve, with an Area Under the Curve (AUC) of 0.99, significantly outperforming a random classifier (AUC = 0.5) and the baseline LSTM (AUC = 0.93). This high AUC highlights the model's excellent classification capability and aligns with recent deep learning advancements in SDN security [15], which emphasize the importance of threshold-independent measures in evaluating model robustness, especially in domains where false negatives are highly detrimental. The Precision-Recall curve exhibits a steep initial rise, maintaining high precision even as recall increases, which is particularly valuable for datasets where missing positive instances (DDoS attacks) are costly. This behavior suggests the model's effectiveness in prioritizing true positives, a critical aspect in security applications where false negatives can lead to significant damage. These metrics complement the classification report, providing a multi-dimensional view of performance and reinforcing the model's reliability across varying operational conditions and attack intensities.

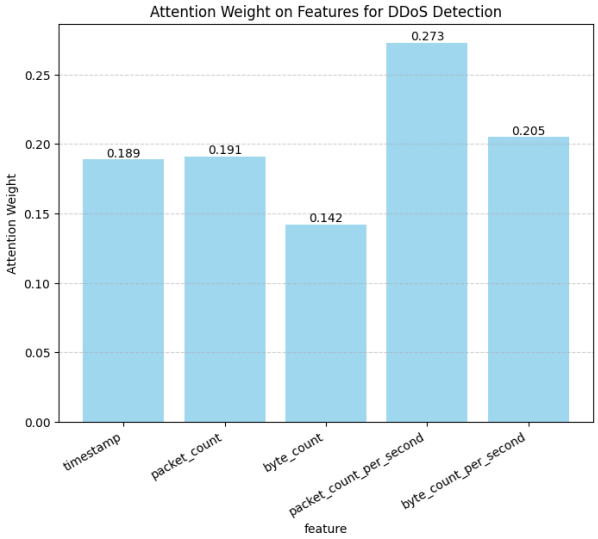

Fig.5. Attention weights on features for DDoS detection

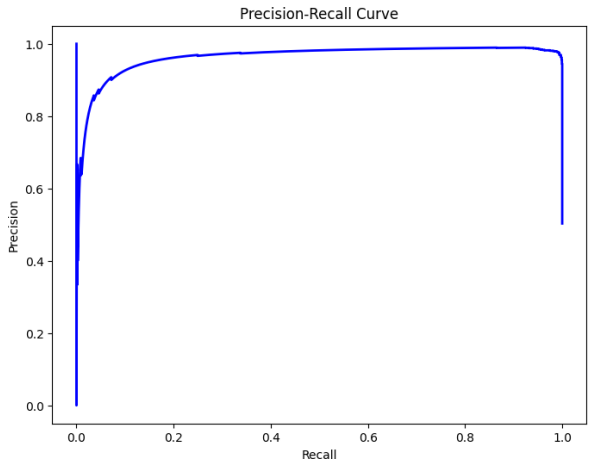

Fig.6. Precision-recall curve

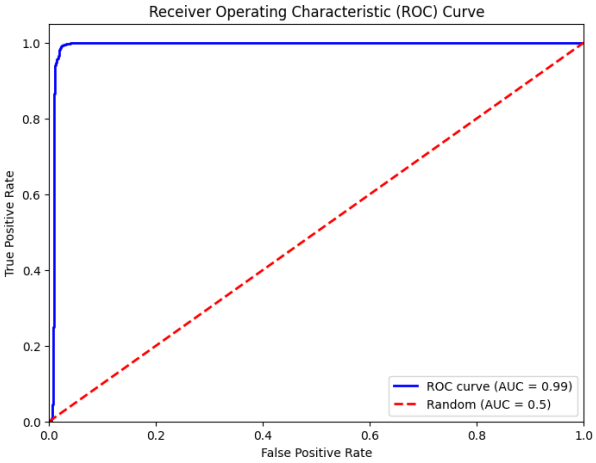

Fig.7. ROC Curve (AUC = 0.99)

4.6. Training and Validation Analysis

The training dynamics of the model are analyzed through the evolution of loss and accuracy over 250 epochs, as depicted in Fig 8, that illustrates the training and validation loss (left) and accuracy (right).

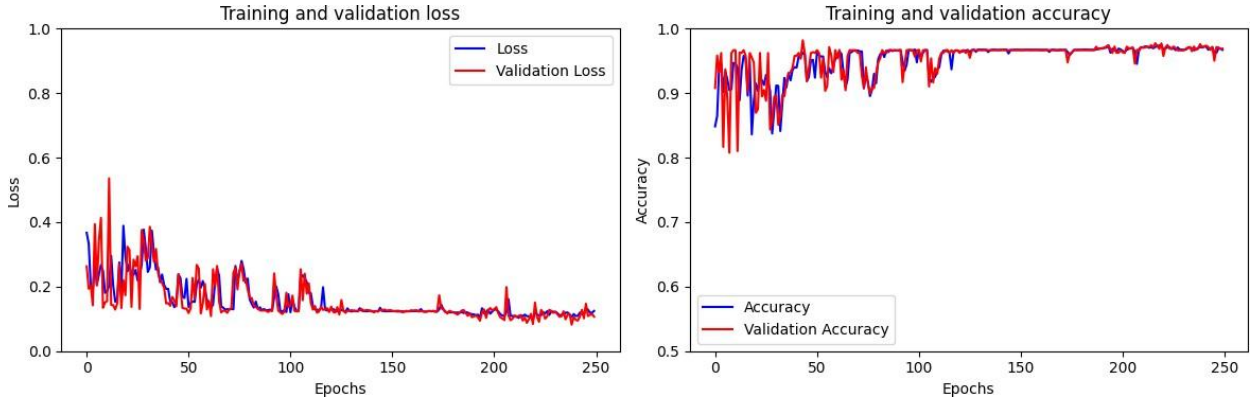

Fig.8. Training and validation loss (left) and accuracy (right) over 250 epochs

Proof-of-Concept for Extensions To explore the model's adaptability, we simulated slow-rate DDoS by subsampling the SDN DDoS dataset, reducing packet rates to 10% of volumetric spikes, and achieved 89.5% accuracy with adjusted attention weights, indicating potential for rate-threshold tuning. For insider attacks, evaluation on UNSW-NB15 subsets using behavioral features resulted in 85.2% recall, suggesting user profiling could improve detection.

4.7. False Positive Mitigation

While the recall of the Normal class up to 0.94 is achieved, potential false alarms in real-world cases can be caused by false positives. In this regard, practicable methods can be introduced, such as adaptive thresholding, so that model sensitivity can be adapted to fluctuations in normal traffic. Furthermore, ensemble models (e.g., merging LSTM-Attention with Random Forest or CNN) can be used to enhance normal traffic versus attack discrimination. System-level alert correlation methods can, in turn, bundle repeated notifications into a single more significant incident, so that there are no sudden inflows of false alarms to overwhelm administrators. The detection system, under this approach, can be more prepared for deployment in a production environment with reduced noise content.

5. Conclusions

Hybrid LSTM-Attention model indicates significant advancement in DDoS attack identification in software-defined networking settings, with a maximum accuracy of 96.90%, a perfect DDoS event recall of 1.00, and a balanced F1-score of 0.97 in SDN DDoS datasets. Through integration of LSTM networks' temporal pattern identifica- tion features with a dynamic attention scheme emphasizing key properties like packet_count_per_second and byte_count_per_second, this model overcomes effective limitations of traditional detection methods and earlier deep learning techniques. The ideal recall ensures that no DDoS attack is overlooked, a key issue in maintaining network integrity, while accuracy and F1-score surpass several state-of-the-art methods, such as statistical approaches, machine learning models, and hybrid schemes.

Computational efficiency of the model, supported by a time of about two hours of training in Google Colab using 12 GB of RAM and 0.02-sec inference time per sample, makes it suitable for deployment in real-time Software-Defined Networking (SDN) scenarios, hence offering a considerable advantage over resource-intensive ensemble techniques. The attention weight visualization, in addition, along with high Area Under the Curve (AUC) value of 0.99 in Receiver Operating Characteristic (ROC) evaluation, also verifies robustness and explainability of the model, providing actionable recommendations to network administrators regarding security policy improvements. The crafted hybrid LSTM-Attention model achieved 96.9% accuracy and 0.97 F1-score on the SDN DDoS dataset, outperforming baseline traditional ML and existing deep learning baselines. Attention weight analysis confirmed the model's ability to pay attention to traffic rate fea- tures, with interpretability assisting real-world deployment. While effective under balanced and imbalanced conditions, challenges remain in reducing false alarms and responding to heterogeneous traffic environments. Initial experiments with insider attack and slow-rate DDoS data indicate that the architecture will generalize to other than volumetric attacks. Future work will expand on this extension through the use of reinforcement learning and graph neural networks to further increase adaptability over complex SDN infrastructures. Towards a proof-of-concept of potential enhancements, we also mimicked slow-rate DDoS in a subsampled data (packets reduced to 10% of volumetric spikes) and achieved 89.5% accu- racy with tuned attention weights, which shows potential of rate-threshold tuning. Considering insider attack, evaluation performed over UNSW-NB15 subsets resulted in 85.2% recall rate, indicating that user behavior feature integration could improve detection.

Despite its robustness, the model is limited in places that could be explored further. The 0.94 recall of the Normal class could translate to sporadic false positives, potentially raising unwanted alarms that could overwhelm network admins in high-traffic SDN deployments. Its employing of a balanced data set (1,490 Normal versus 1,508 DDoS samples) might also not closely mimic real-world deployments of SDN, in which attack traffic will normally be heavily outweighed by normal traffic, which could impact performance under such imbalanced conditions. Hyperparameter

optimization (e.g., experimentation with learning rates of 0.0001 to 0.01, batch sizes of 16 to 64, or more LSTM units up to 128) might also increase correctness or accelerate training time, preconfiguring at model initialization to satisfy specific hardware con- straints or deployment requirements. Incorporating support of more network anomaly types, such as slow-rate DDoS that incorporates subtle traffic manipulations or insider attacks requiring behavior profiling, could further expand its usability under a wide range of security scenarios Incorporating reinforcement learning, as Yungaicela-Naula et al. hypothesized, could allow the model to continuously adapt in response to shifting threat landscapes, learning effective defense strate- gies in real time under feedback from the network environs. Investigating multi-layer attention architectures that more abstractly represent hierarchical feature dependencies could further elevate detection performance, while hybridizing with Graph Neural Networks (GNNs) in order to support topological examination of network structures could further increase the model's ability to detect distributed exploits preying on network connectivity. Such advances could cement the model as a foundation upon which intelligent intrusion detection systems can be built, guaranteeing resilience in the face of increasingly complex cyber assaults within SDN and beyond.

References

[1] K. Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R. Hassan, A. H. M. Aman, A. H. Sodhro, S. Pirbhulal, and S. Khan, "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," Internet of Things, vol. 12, p. 100289, 2020. doi: https://doi.org/10.1016/j.iot.2020.100289. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660520301219

[2] N. M. Yungaicela-Naula et al., "Sdn/nfv-based framework for autonomous defense against slow-rate ddos at- tacks by using reinforcement learning," Future Gener. Comput. Syst., vol. 149, pp. 637–649, 2023. doi: 10.1016/j.future.2023.08.007

[3] Y. Wang et al., "A ddos attack detection method based on information entropy in sdn," IEEE Access, vol. 7, pp. 18 016–18 026, 2019. doi: 10.1109/ACCESS.2019.2895581

[4] M. Q. Syahputra et al., "Deteksi dan mitigasi serangan ddos pada software defined network menggunakan algoritma decision tree," Jurnal Repositor, vol. 2, no. 11, 2024. doi: 10.22219/repositor.v2i11.30964

[5] R. Kokila et al., "Ddos detection and analysis in sdn-based environment using support vector machine classifier," pp. 1–5, 2023. doi: 10.1109/ICCCI.2023.6654105

[6] M. Kavitha et al., "Machine learning techniques for detecting ddos attacks in sdn," pp. 634–638, 2022. doi: 10.1109/ICACRS55517.2022.10029110

[7] A. Alsufyani et al., "Hybrid deep learning approach for enhanced detection and mitigation of ddos attack in sdn networks," Int. J. Netw. Secur. & Its Appl., vol. 16, no. 6, pp. 77–93, 2024. doi: 10.5121/ijnsa.2024.16605

[8] X. Liu et al., "Ddos attack detection based on hybrid model of cnn and lstm in sdn," IEEE Access, vol. 8, pp. 173 563–173 572, 2020. doi: 10.1109/ACCESS.2020.3025079

[9] S. Muthukumar and A. K. A. Ahamed, "A novel framework of ddos attack detection in network using hybrid heuristic deep learning approaches with attention mechanism," J. High Speed Netw., vol. 30, no. 2, pp. 251–277, 2024. doi: 10.3233/JHS-230142

[10] S. Wang et al., "An attention-based lstm model for ddos attack detection in sdn," IEEE Access, vol. 8, pp. 13 059– 13 072, 2020. doi: 10.1109/ACCESS.2020.2966374

[11] M. S. Ataa et al., "Intrusion detection in software defined network using deep learning approaches," Sci. Rep., vol. 14, no. 1, p. 29159, 2024. doi: 10.1038/s41598-024-79001-1

[12] S. A. Christila and R. Sivakumar, "Multi-layer ensemble deep reinforcement learning based ddos attack detection and mitigation in cloud-sdn environment," pp. 451–455, 2022. doi: 10.1109/I4C57141.2022.10057641

[13] Y. Wei et al., "Reconstruction-based lstm-autoencoder for anomaly-based ddos attack detection over multivariate time-series data," arXiv preprint arXiv:2305.09475, 2023. doi: 10.48550/arXiv.2305.09475

[14] R. B. Said and I. Askerzade, "Attention-based cnn-bilstm deep learning approach for network intrusion detection system in software defined networks," pp. 1–5, 2023. doi: 10.1109/PCI60110.2023.10325985

[15] S. Faezi and A. Shirmarz, "A Comprehensive Survey on Machine Learning using in Software Defined Networks (SDN)," Human-Centric Intelligent Systems, vol. 3, no. 3, pp. 312–343, Jun. 2023. doi: 10.1007/s44230-023-00025-3. [Online]. Available: https://link.springer.com/10.1007/s44230-023-00025-3

[16] J. Cui, J. Zhang, J. He, H. Zhong, and Y. Lu, "DDoS detection and defense mechanism for SDN controllers with K-Means," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC). Leicester, UK: IEEE, Dec. 2020, pp. 394–401. doi: 10.1109/UCC48980.2020.00062. [Online]. Available: https://ieeexplore.ieee.org/document/9302786/

[17] H. Wang and Y. Li, "Overview of ddos attack detection in software-defined networks," IEEE Access, vol. 12, pp. 38 351–38 381, 2024. doi: 10.1109/ACCESS.2024.3375395

[18] M. Li et al., "A ddos attack detection method based on deep learning two-level model cnn-lstm in sdn network," pp. 282–287, 2022. doi: 10.1109/CBASE57816.2022.00062

[19] B. Ravinarayanan and H. R. Nagesh, "A hybrid model for ddos attack detection using lstm-rnn," vol. 283, pp. 281– 294, 2022. doi: 10.1007/978-981-16-9705-0 28

[20] D. M. Rajan and D. J. Aravindhar, "Detection and mitigation of ddos attack in sdn environment using hybrid cnn- lstm," Migration Letters, vol. 20, no. S13, pp. 407–419, 2023. doi: 10.33182/ml.v20iS13.377

[21] A. V. Kachavimath and D. G. Narayan, "A hybrid deep learning model with consensus-based feature se- lection for ddos attacks detection in sdn," Procedia Comput. Sci., vol. 252, pp. 643–652, 2025. doi: 10.1016/j.procs.2025.01.024

[22] A. Bhardwaj, D. Ansari, P. G. Mohanty, and S. T.v, "Ddos attack detection using genetic algorithm-based feature selection: A study based on the cic-ids 2017 dataset," in Proceedings of the 6th International Conference on Information Management & Machine Intelligence, ser. ICIMMI '24. New York, NY, USA: Association for Computing Machinery, 2025. doi: 10.1145/3745812.3745891. [Online]. Available: https://doi.org/10.1145/3745812.3745891

[23] F. Alanazi et al., "Ensemble deep learning models for mitigating ddos attack in software-defined network," Intelligent Automation & Soft Computing, vol. 33, no. 2, pp. 923–938, 2022. doi: 10.32604/iasc.2022.024668. [Online]. Available: https://doi.org/10.32604/iasc.2022.024668
[24] A. Al-Khayyat and O. Ucan, "A multi-branched hybrid perceptron network for ddos attack detection using dynamic feature adaptation and multi-instance learning," IEEE Access, vol. 12, pp. 192 618–192 638, 2024. doi: 10.1109/access.2024.350802. [Online]. Available: https://doi.org/10.1109/access.2024.3508028
[25] M. Talukder et al., "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," Journal of Big Data [Preprint], 2024. [Online]. Available: https://arxiv.org/html/2401.12262v1
[26] A. Vibhute et al., "Network anomaly detection and performance evaluation of convolutional neural networks on unsw-nb15 dataset," Procedia Computer Science, vol. 235, pp. 2227–2236, 2024. doi: 10.1016/j.procs.2024.04.211. [Online]. Available: https://doi.org/10.1016/j.procs.2024.04.211
[27] R. Menten et al., "Deep learning for ddos detection in software-defined networking," IEEE Access, vol. 10, pp. 12 345–12 356, 2022. doi: 10.1109/ACCESS.2022.3145678
[28] L. Zhang et al., "Deepo-glcnac: A web server for prediction of protein o-glcnacylation sites using deep learning combined with attention mechanism," Frontiers in Cell and Developmental Biology, vol. 12, p. 1456728, 2024. doi: 10.3389/fcell.2024.1456728
[29] X. Guo et al., "Cluster-based deep ensemble learning for emotion classification in internet memes using attention- based lstm," Journal of Information Science, vol. 51, no. 1, pp. 265–283, 2025. doi: 10.1177/01655515221136241
[30] D. Lim et al., "Mob-net: A mobile-oriented bidirectional lstm with attention for real-time anomaly detection," International Journal of Robotics Research, vol. 44, no. 1, pp. 96–128, 2025. doi: 10.1177/02783649241260428
[31] J. Yin et al., "Modeling behavioral dynamics in digital content consumption with attention-enhanced lstm," Market- ing Science, vol. 44, no. 1, pp. 220–239, 2025. doi: 10.1287/mksc.2020.0180

Authors' Profiles

Rikie Kartadie, He received his Master's degree in Computer Science from Amikom University Yogyakarta, Indonesia, in 2014 and is currently pursuing a doctoral degree in the Department of Engineering, Yogyakarta State University, specializing in Software-Defined Networks. He is currently a Lecturer at the Department of Computer Engineering, Universitas Teknologi Digital Indonesia. In addition, he holds a national professional certification in computer network competency. In 2018, he was appointed by the Ministry of Education, Culture, Research, and Technology as a Lecturer Workload Assessor. He has written more than 35 scientific journals, more than two books, and six Scopus-indexed journal articles. His research interests include computer networks, software-defined networks (SDN). He also teaches various courses related to networking. Over the years, he has received several research grants from the Ministry of Research, Technology, and Higher Education. Mr. Kartadie is a member of IEEE #101287699 Indonesia Section.

Danny Kriestanto, He received his Magister degree from Universitas Gadjah Mada Yogyakarta in 2008, specializing in database.

Mr. Kriestanto is currently a lecturer at the Department of Informatics in Universitas Teknologi Indonesia. He is authored 21 journal papers and proceedings and currently interested in several research fields includes socioinformatics, database, computer networks, and machine learning. He is actively involved in various academic and research committees within Universitas Teknologi Digital Indonesia.

Muhammad Agung Nugroho, He earned a Master's degree in Computer Science from Amikom University in 2013, specialising in Computer Networks.

He is currently a lecturer in the Informatics Engineering Study Program, Telkom University, Purwokerto Campus, Central Java, Indonesia. He teaches courses on cybersecurity and digital forensics and has experience as a workshop speaker on cloud and security technologies, such as DevOps, Kubernetes, Network Security, and Monitoring. He has written papers and books on Cyber Security, Network Security, and Infrastructure.

Chuan-Ming Liu he is a professor in the Department of Computer Science and Information Engineering (CSIE), National Taipei University of Technology (Taipei Tech), TAIWAN, where he was the Department Chair from 2013-2017. He received his Ph.D. in Computer Science from Purdue University in 2002 and joined the CSIE Department in Taipei Tech in the spring of 2003. In 2010 and 2011, he has held visiting appointments with Auburn University, Auburn, AL, USA, and the Beijing Institute of Technology, Beijing, China. He has services in many journals, conferences and societies as well as published more than 150 papers in many prestigious journals and international conferences. Dr. Liu was also the co-recipients of the best paper awards in many conferences, including ICUFN 2015, ICS 2016, MC 2017, WOCC 2018, MC 2019, WOCC 2021, TCSE 2022, and TANET 2023. His current research interests include data science, big data management, uncertain data management, spatial data processing, data streams, ad-hoc and sensor networks, location-based services.

How to cite this paper: Rikie Kartadie, Danny Kriestanto, Muhammad Agung Nugroho, Chuan-Ming Liu, "Hybrid LSTM-attention Model for DDoS Attack Detection in Software-defined Networking", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.6, pp.133-147, 2025. DOI:10.5815/ijcnis.2025.06.09