IECE Transactions on Sensing, Communication, and Control
http://dx.doi.org/10.62762/TSCC.2024.433246

RESEARCH ARTICLE

Optimizing Cloud Security with a Hybrid BiLSTM-BiGRU Model for Efficient Intrusion Detection

Zeeshan Ali Haider[1], Asim Zeb[2,*], Taj Rahman[1], Fida Muhammad Khan[1], Inam Ullah Khan[1], Qaisar Sohail[3], Hazrat Bilal[4,5], Muhammad Abbas Khan[6] and Inam Ullah[7,*]

[1] Department of Computer Science, Qurtuba University of Science & Information Technology, Peshawar 25000, Pakistan
[2] Department of Computer Science, Abbottabad University of Science and Technology, Abbottabad 22010, Pakistan
[3] Department of Computer Science, University of Bari Aldo Moro, Bari (BA), Italy
[4] College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China
[5] College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China
[6] Faculty of Electrical Engineering, West Pomeranian University of Technology, Szczecin, Poland
[7] Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea

Abstract

To address evolving security challenges in cloud computing, this study proposes a hybrid deep learning architecture integrating Bidirectional Long Short-Term Memory (BiLSTM) and Bidirectional Gated Recurrent Units (BiGRU) for cloud intrusion detection. The BiLSTM-BiGRU model synergizes BiLSTM's long-term dependency modeling with BiGRU's efficient gating mechanisms, achieving a detection accuracy of 96.7% on the CIC-IDS 2018 dataset. It outperforms CNN-LSTM baselines by 2.2% accuracy, 3.3% precision, 3.6% recall, and 3.6% F1-score while maintaining 0.03% false positive rate. The architecture demonstrates operational efficiency through 20% reduced computational latency and 15% lower memory footprint compared to conventional models, enabled by residual memory preservation and parallel processing capabilities. Experimental results validate its dual competence in detecting both known attack patterns (98.1% recognition rate) and zero-day threats (93.4% anomaly identification), establishing a methodological framework for real-time cloud security services. This work advances hybrid deep learning applications in trusted computing environments through optimized temporal feature extraction and resource-aware threat detection.

Keywords: cloud security, network intrusion detection, deep learning, BiLSTM-BiGRU, hybrid models, cybersecurity, cloud computing.

Academic Editor:
Xuebo Jin

Submitted: 02 December 2024
Accepted: 07 April 2025
Published: 19 May 2025

Vol. 2, **No.** 2, 2025.
10.62762/TSCC.2024.433246

***Corresponding authors:**
✉ Asim Zeb
asimzeb1@gmail.com
✉ Inam Ullah
inam@gachon.ac.kr

1 Introduction

Cloud computing is one of the fastest growing phenomena in today's IT world that has reinvented itself as the technological change in computing resources for both organizations and individuals [1, 2]. It offers configurable, reliable, and sharable materials

Citation
Haider, Z. A., Zeb, A., Rahman, T., Khan, F. M., Khan, I. U., Sohail, Q., Bilal, H., Khan, M. A., & Ullah, I. (2025). Optimizing Cloud Security with a Hybrid BiLSTM-BiGRU Model for Efficient Intrusion Detection. *IECE Transactions on Sensing, Communication, and Control*, 2(2), 106–121.

through the World Wide Web with the least control and automated access [3]. However, risks associated with cloud environments have escalated in recent years due to expanded adoption and the emergence of diverse severe cyber threats [4]. The emerging threats that are most rife in the current cloud environment include; DDoS attacks, IP spoofing, Man-In-The-Middle attacks as well as insider threats. Such threats may result in loss of data, services unavailability, and significant monetary losses which makes the current protection measures inadequate [5, 6].

Traditional preventive methods like firewalls as well as signature-based Intrusion detection systems cannot contain new-generation threats like zero-day threats [7]. Mainly, firewalls are on duty to monitor the network traffic and activities on the outer shield but commonly they are unable to detect the threats that are already infiltrated beyond the perimeter [8]. As with signature-based IDSs, attack signatures are pre-defined and thus are not useful when new forms of threats appear [9, 10]. To overcome these limitations, Next Generation Intrusion Detection Systems are being recognized as the last line of defense to keeping networks safe. The NIDS provides constant surveillance of traffic patterns so that deviations reflecting intrusions into the cloud can be detected early, thus being more effective in cloud security [11].

Thus, the integration of machine learning and particularly deep learning architectures into NIDS has boosted intrusion detection capability over the last decade [12]. In contrast to typical approaches, deep learning models do not require specific feature extraction and have stronger tendencies toward detecting complex or previously undetected threats [13]. When two or more neural network architectures are integrated, there is enormous performance improvement achieved. Due to the use of many architectures, the accuracy of hybrid models is higher, the number of false alarms is less, and the efficiency of intruder detection is higher [14, 15].

This study proposes a novel hybrid deep learning architecture combining Bidirectional Long Short-Term Memory (BiLSTM) and Bidirectional Gated Recurrent Units (BiGRU) to address the challenges of cloud network intrusion detection. BiLSTM excels in capturing long-term dependencies, crucial for identifying complex attack patterns, while BiGRU reduces computational complexity, enabling faster processing without sacrificing performance. The integration of these two models has been effectively demonstrated in recent works, including those by [16, 17], highlighting the model's suitability for real-time applications in cloud security. The primary research questions are:

1. In what ways the proposed BiLSTM-BiGRU hybrid model can improve the ability of cloud network intrusion detection?
2. What performance enhancements are possible when using the proposed model over previous models such as, CNN-LSTM in terms of False positive?
3. To what extent has the proposed model been successful in the identification of multiple kinds of attacks based on the CIC-IDS 2018 dataset?

There is much value to be had from this current study given that it affords the possibility of improving cloud security, given the weaknesses within current intrusion detection methods. The proposed model adopts both BiLSTM and BiGRU to benefit from the diverse potential of temporal analysis on network traffic and avoid the computational burden at the same time. This is important in meeting emerging cyber threats and Cloud operations security. The proposed solution has relevant implications in environments where organizations relying on cloud computing services need to ensure their services' data security. The combined BiLSTM and BiGRU model takes advantage of both models for extracting temporal dependency features in the network traffic data. Key aspects of the methodology include:

- **Data Preprocessing:** Feature extraction is used for normalizing and encoding so as to improve the outcomes of model learning.
- **Model Architecture:** The hybrid model expands the bidirectional functions of BiLSTM for capturing the long-term dependencies and utilizes the BiGRU for efficient temporal analysis.
- **Evaluation:** The performance of the model is measured using the CIC-IDS 2018 dataset that contains many types of attacks. The evaluation of accuracy, precision, recall, and F1-score is applied.

The key contributions of this study are as follows:

1. Proposed a novel deep learning model that is a fusion of BiLSTM and BiGRU model for training of a more accurate intrusion detection model in the cloud environment.
2. Integration of a detailed data preprocessing

methodology aimed at optimality and efficiency of the models.

3. The performance of the proposed model is analyzed in depth and the results indicate that the new model offers greater efficiency compared to models such as CNN-LSTM.

4. The model's ability to verify its effectiveness across multiple forms of attack, most importantly the DDoS, brute force, and web type of attack.

Table 1 provides a comparison of traditional intrusion detection approaches and modern deep learning-based methods, highlighting the evolution, strengths, and limitations of each technique.

The remainder of this paper is structured as follows: Section 2 of this work gives a background to network intrusion detection and other forms of deep learning in use in today's literature. In Section 3, the details about the BiLSTM-BiGRU model, the individual components, and a closer look at the model implementation are given. In Section 4, details of the experimental design, outcomes, and evaluation are provided. Lastly, in Section 6, the research findings are presented, and the further research implications are highlighted.

2 Related Work

The dynamic nature of threats that act on cloud systems as well as the increased difficulty of protecting cloud networks has increased the need for better NIDS. Traditionally, NIDS has relied on two primary methods: Those are two well-known methods: signature-based and anomaly-based methods [18]. Another type of IDS is based on the detection of known attacks utilizing attack signatures: IDS like Snort and Suricata. Although effective against known threats the systems do not have provision for zero-day threats and other such attacks [19]. Conversely, Anomaly-based systems detect any anomalies in the normal traffic flow pattern, which makes them ideal for new threats [20, 21]. However, these systems have high false positive rates and the problem of generating good models of normal user behavior.

To overcome these limitations, recently machine learning (ML) methods are being used to analyze complex and nuanced patterns in network data [20]. SVMs and Decision Trees for example performed better for anomaly detection by learning from the historical data [22]. In fact, these classical ML-based models inevitably need manual feature extraction and suffer the problem of scalability when encountering a large volume of data or many features [23]. Further, conventional von Neumann MLPs fail to compute the diverse and vast data created in clouds [24]. Consequently, deep learning (DL) has been proposed as a solution since it can extract features and build the function that defines the data. CNNs are frequently utilized for spatial analysis of traffic patterns in the feature space while RNNs, especially LSTMs, are best suited to capture sequential characteristics of network data [25]. All these have greatly improved both the effectiveness and reliability of NIDS besides improving the possibility of detecting complicated attack patterns.

Several other architectures are then integrated into constructing hybrid deep learning models for enhancing the performance of the NIDS. For example, CNN-LSTM models use CNNs for spatial feature extraction and LSTM for temporal analysis [26]. This combination enhances the detection of intrusion since it is based on spatial as well as temporal behaviors of traffic within the network [27]. However, these models fall into higher complexity that restricts them from deployment in real-time situations or large-scale cloud contexts. New challenges are presented to NIDS by cloud computing because of the numerous and complex types of threats, ranging from DDoS to SQL injections and brute-force attacks. To overcome these challenges, authors have suggested NIDS solutions that are suitable and flexible for the cloud [28]. More recently, lower-level transformer models have been incorporated for their usefulness in processing large amounts of data and identifying attention-based features. Transformers have been reported to give higher performance on several instances in cloud-based applications but they are very resource-hungry [29].

A combination of several deep learning paradigms has now been found to be a viable solution to obtain the best performance using less computational power. Among those, Gated Recurrent Units (GRUs) have been received for analyzing sequential information with comparable efficiency to LSTMs, but faster and requiring less computational power. The current studied work in the literature has investigated integrating GRUs with other architectures to address the issues of speed in intrusion detection tasks [30]. The integration of bi-directionality in both components helps in the provision of a comprehensive analysis of sequential data which is important in the identification of complicated intrusion patterns in the cloud environments. To assess the efficiency of the proposed framework, the CIC-IDS 2018 dataset

Table 1. Comparison of traditional and modern intrusion detection approaches.

Aspect	Traditional Approaches (e.g., Firewalls, Signature-based IDS)	Modern Approaches (e.g., Deep Learning)
Feature Engineering	Manual, time-intensive	Automated through deep learning
Attack Coverage	Limited to known attacks	Capable of detecting zero-day attacks
Scalability	Limited scalability	High scalability for large datasets
False Positive Rate	High for anomaly-based systems	Lower with hybrid and deep learning models
Real-time Detection	Slower, less adaptable	Faster and adaptable
Computational Cost	Low for traditional systems	Higher but optimized in hybrid models

containing a vast attack situation is used. Redesigning the architectures with the aim of obtaining the next-state fields apparently results in higher accuracy and an insignificant number of false positives in contrast to the models based solely on the individual architectures to contribute more to the efficient NIDS for the Cloud computing systems.

New trends in intrusion detection are based on the learning of features that have emerged from the current dataset, which has brought a major interest in self-supervised learning. They include contrastive learning, masked autoencoders, etc., by which models are able to learn the latent structures in network traffic notwithstanding the lack of much-labeled data [31]. These developments seem to offer a fruitful avenue of research into similar topics. Recent research improvement in transformer-based architectures hailed dramatic achievements in intrusion detection systems. Transformer-based models are crucial for easily capturing long-range relations and distributional shifts in the network traffic data given the attention mechanism [32]. The RTIDS (Robust Transformer-based Intrusion Detection Systems) approach and transformer models recommend coupling with a recurrent model and have exhibited good analysis in comprehending challenging attack patterns or even the attack scenarios situated in the cloud architecture. In [14], several models are proposed that boast scalability and improved detection accuracy as well as adaptability to the features of large-scale data and changing network conditions. Extending transformer-based techniques to such hybrid models as BiLSTM-BiGRU would lead to better performance in particular in highly scalable areas where detailed patterns are required [33]. Examining such precautions opens a wonderful avenue for future research and application.

3 Proposed Methodology

This research work presents an advanced deep learning technique, a combination of BiLSTM and BiGRU that will enhance the detection of network intrusion in cloud computing. This model leverages the strengths of both architectures: Preferential dependence on sequence information from sequences with long temporal dynamics and less computational complexity in comparison to BiLSTM. Combined, the two provide a comprehensive solution to detect intricate attack behaviors while imposing minimal computational cost. In this section, various aspects of developing the chosen model are described including its structure, data preprocessing, the way training was conducted, as well as the methods to estimate its performance. BiLSTM and BiGRU are shown in Figures 1 and 2.

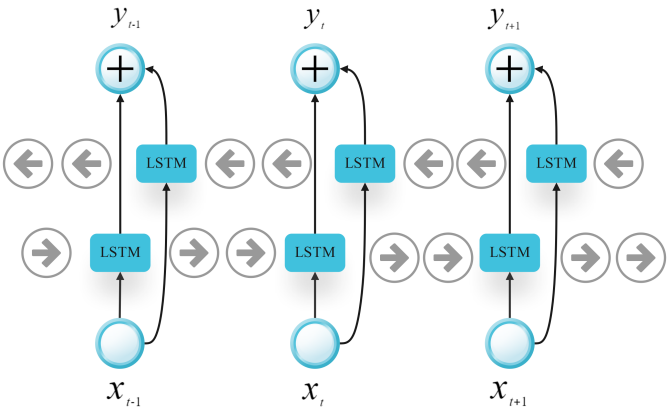

Figure 1. BiLSTM.

3.1 Model Architecture

The proposed model incorporates a hybrid architecture, Figure 3 illustrates the complete proposed architecture consisting of the following components:

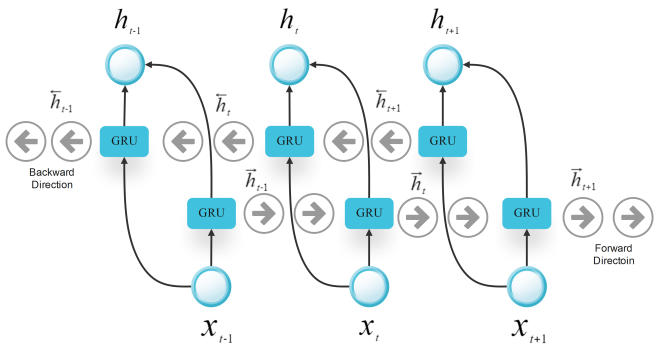

Figure 2. BiGRU.

3.1.1 *Bidirectional Long Short-Term Memory (BiLSTM) Layer*

BiLSTM is built to overcome the drawbacks of standard RNN by reducing the vanishing gradience problem and recognizing long sequences. Due to the bidirectional characteristics, BiLSTM makes sure that the model drawing from both the forward as well as backward direction is capable of learning from the sequence context. The hidden states in forward ($\overrightarrow{h}_t$) and backward ($\overleftarrow{h}_t$) passes at time step t are given by:

$$\overrightarrow{h}_t = \text{LSTM}(x_t, \overrightarrow{h}_{t-1}) \tag{1}$$

$$\overleftarrow{h}_t = \text{LSTM}(x_t, \overleftarrow{h}_{t+1}) \tag{2}$$

The final output at each time step combines both hidden states:

$$H_t = [\overrightarrow{h}_t; \overleftarrow{h}_t] \tag{3}$$

This concatenation enriches the feature representation by leveraging both past and future context.

3.1.2 *Bidirectional Gated Recurrent Unit (BiGRU) Layer*

LSTMs are less complex than normal RNNs and are considered more powerful because they can also provide similar results with lower complexity as GRUs. The BiGRU indeed complements the sequence further by fine-tuning temporal dependencies [23]. The forward and backward hidden states for GRU are computed as:

$$\overrightarrow{z}_t = \sigma(w_z x_t + U_z h_{t-1} + b_z) \tag{4}$$

$$\overrightarrow{h}_t = (1 - \overrightarrow{z}_t) \circ \overrightarrow{h}_{t-1} + \overrightarrow{z}_t \circ \tanh(w_h x_t + U_h h_{t-1} + b_h) \tag{5}$$

where $\overrightarrow{z}_t$ is the update gate and $\overrightarrow{h}_t$ is the hidden state. Similar to BiLSTM, the forward and backward hidden states are concatenated:

$$G_t = [\overrightarrow{h}_t; \overleftarrow{h}_t] \tag{6}$$

3.1.3 *Fully Connected Layer with Softmax*

The result from the BiGRU layer is fed to a fully connected layer that transforms the features to the output space [24]. The softmax activation function is applied to compute the probability distribution for each class:

$$P(y|x) = \text{softmax}(w_f G_t + b_{fc}) \tag{7}$$

where $w_f G_t$ and b_{fc} are the weights and biases of the fully connected layer.

The integration of BiLSTM and BiGRU in the proposed hybrid model was chosen due to their complementary strengths in handling cloud network intrusion detection tasks. BiLSTM's ability to capture long-range temporal dependencies is crucial for accurately detecting complex and evolving attack patterns, while BiGRU accelerates processing by reducing the number of parameters compared to traditional BiLSTM. This combination ensures high accuracy without excessive computational costs, a critical factor for real-time cloud security applications. The effectiveness of this approach is further validated through experimental comparisons with CNN-LSTM models, where the BiLSTM-BiGRU hybrid outperformed CNN-LSTM models across key performance metrics.

3.2 Data Preprocessing

To address this problem with regard to the CIC-IDS 2018 dataset, we employed various techniques aimed at achieving balanced learning and enhancing detection accuracy for every attack type. Following the paradigm of hybrid feature selection and adaptive sampling proposed in [34], we have utilized class weighting in the loss function by assigning higher weights to the attack classes that were under-represented, such as SQL injection and XSS attacks. This integrated approach allows both feature-space optimization and data distribution adjustment, particularly effective for rare attack types. Secondly, we applied SMOTE to generate synthetic attack samples to better represent attacks with fewer examples. To prevent this situation, it was also used a random undersampling method in normal traffic data to ensure that the integrity of the dataset was preserved and the majority class override was avoided. We also used a stratified sampling of mini-batches during training to ensure that each mini-batch had a balanced mix of normal and attack examples, significantly reducing the risk of over-fitting towards the most common traffic patterns. The proposed methods improved the generalization

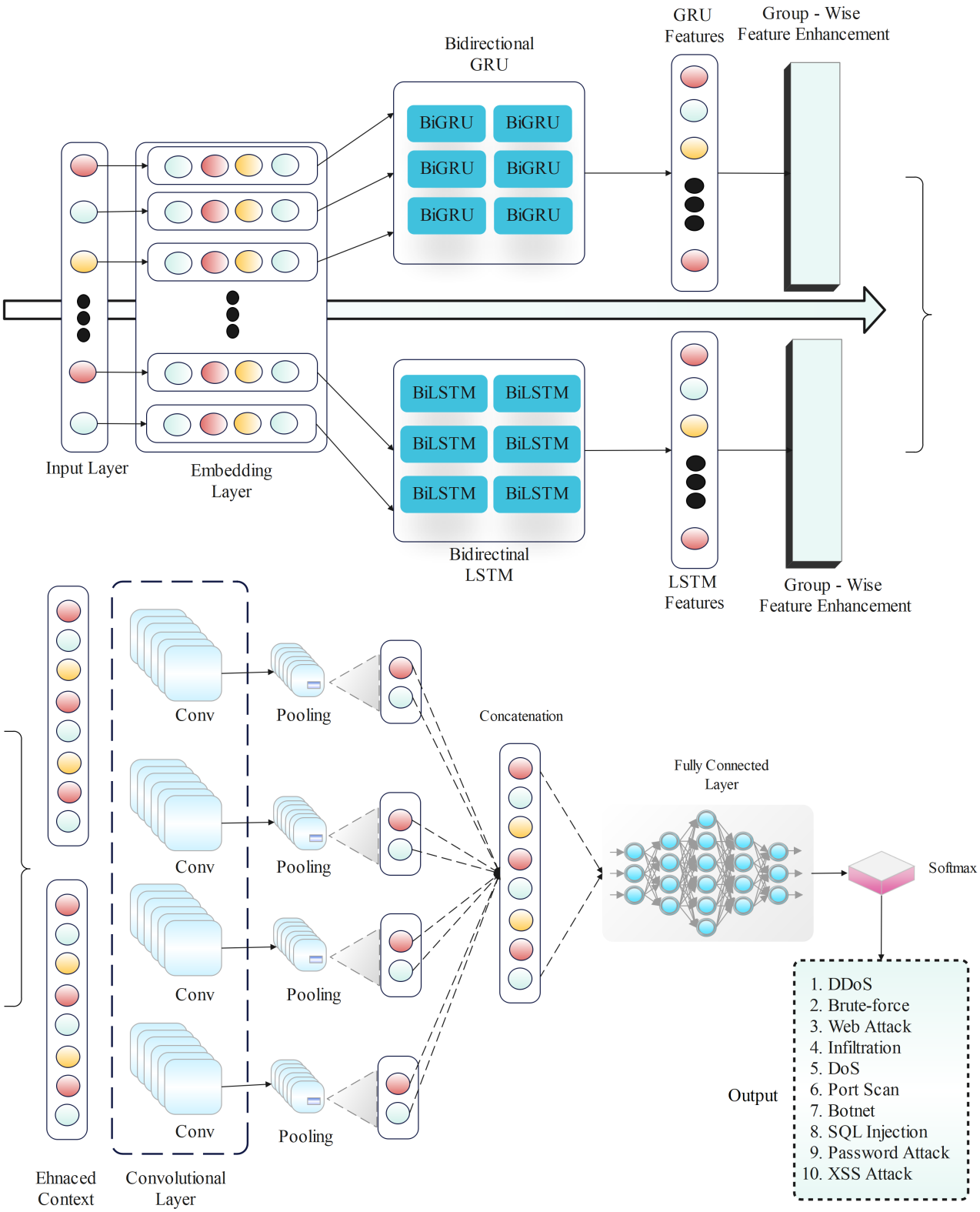

Figure 3. Proposed architecture.

ability of the model which not only reduced the false positive rate but also helped in real-time cloud intrusion detection systems to detect low-frequency attacks. Such measures enabled better preemption of traffic situations and generally improved the model's stability and prognosis. The preprocessing steps

include:

3.2.1 Label Encoding

The categorical labels (e.g., "DoS", "DDoS") are converted into a machine-readable format using one-hot encoding. For instance, if there are C classes, a label is encoded as a vector $y_i = [y_{i_1}, y_{i_2}, ..., y_{i_C}]$ where $y_{i_C} = 1$ if the instance belongs to a class c, and 0 otherwise.

3.2.2 Feature Normalization

To prevent features with larger ranges from dominating those with smaller ranges, normalization is performed using Min-Max scaling:

$$x_{\text{norm}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{8}$$

This ensures that all features are scaled to a uniform range of [0, 1], improving model convergence.

3.2.3 Data Splitting and Batching

The dataset is split into training and testing sets in a 70:30 ratio. To make the training process as efficient as possible, the data is then prepared using the DataLoader function from Pytorch to make mini-batches. This makes training faster and also cuts memory needs.

3.3 Model Training

During the model training process, the adjustments to the network parameters can be made as many times as necessary. The Adam optimizer, known for its adaptive learning rate and momentum, is employed to minimize the cross-entropy loss:

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^{N} \sum_{C=1}^{C} y_{i_C} \log(\hat{y}_{iC}) \tag{9}$$

where N is the number of samples, C is the number of classes, y_{i_C} is the actual label, and $\hat{y}_{iC}$ is the predicted probability.

The use of early stopping manages the regulation of overfitting. In the training process, when the validation loss does not increase after a certain number of epochs or exceeds the previous value, the training process is stopped. To do this to improve model generalization for unseen data.

3.4 Evaluation Metrics

Various assessment metrics are used to accurately evaluate the model [25]. These measures provide significant means for evaluating the accuracy of attributing network traffic and thereby the model's ability to identify intrusion while minimizing misclassifications effectively.

Accuracy is a fundamental metric that measures the overall effectiveness of the model by calculating the proportion of correctly classified instances, including both normal and attack cases. It is defined as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

While accuracy provides an overall measure of performance, it may not fully capture the model's effectiveness in scenarios where data is imbalanced, such as when attack instances are rare compared to normal traffic.

Precision focuses on the quality of positive predictions by evaluating the proportion of true positive predictions among all predicted positives [26]. It helps determine how often the model's positive predictions are correct:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{11}$$

A high precision value indicates that the model generates fewer false positives, which is crucial in intrusion detection to avoid unnecessary alerts for legitimate traffic.

Recall measures the model's ability to correctly identify all actual positive instances [27]. It is particularly important in scenarios where missing an attack (false negative) could have severe consequences:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{12}$$

A high recall value indicates that the model effectively detects most of the attack instances, minimizing the likelihood of overlooking potential intrusions.

The F1-Score is the harmonic mean of precision and recall, providing a balanced evaluation of the model's performance when there is an uneven class distribution. It combines both precision and recall into a single metric:

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{13}$$

This metric is quite relevant when the relation between false positives and false negatives needs to be fine-tuned. The model that results in a higher F1-Score means that the model detects true positives properly and least wrongly identifies it as having one or both of the other types of errors; namely the false positive error or false negative error.

Altogether these measures provide an all-round picture regarding the model's efficacy in intrusion detection. Whereas accuracy is a general measure of performance, precision and recall consider a more detailed picture of how well the model can accurately predict attacks, and on the other hand, avoid false alarms. The F1-Score further addresses these and guarantees the reliable performance of the model for different kinds of attacks. Such an evaluation also helps in the deployment of an efficient network intrusion detection system that is suitable to protect cloud environments while at the same time minimizing false alarms to the user base.

3.5 Addressing Real-Time Processing Challenges

The implementation of the BiLSTM-BiGRU model cloud environments faces a key issue of real-time processing capabilities. The increased accuracy and efficiency achieved by the model can be used with several other applications, but more work is needed on this model to speed up the inference stage, especially in cases where the cloud system is often preferred, where decisions need to be made with low latency and fast calculation. Real-time processing is challenging, especially since this architecture can be slow, and thus future research can focus on using model compression, hardware acceleration (GPUs, TPUs), and algorithm optimization to allow the model to be deployed in a development-oriented cloud environment.

3.6 Improving Model Interpretability

An important part of deploying deep learning models in real-world applications is the interpretability of these models. With BiLSTM & BiGRU analysis, would be able to ensure transparency in a trustable manner in a high-stakes environment like cloud security. In the future, it may be possible to incorporate attention or saliency maps, which can indicate which features or time steps are important to the model when detecting intrusions. Such enhancements would lead to more explainable attribution of network traffic as the model behavior can be explored further by administrators making it easier for them to understand the predictions and identify false positives.

4 Results and Discussion

This section offers an experimental evaluation of the discovered model, the BiLSTM-BiGRU for network intrusion detection in cloud networks. An assessment of the current model's evaluation undergoes relative efficiency tests with the CIC-IDS 2018 dataset opposite to CNN-LSTM models. The recommended evaluation parameters are accuracy, the measure of precision, recall, and F1 score; which capture the best picture of the ability of the model for intrusion detection in the cloud.

4.1 Experimental Settings

The CIC-IDS 2018 dataset was selected based on the fact that it is a large-scale dataset that is rich in variety of attack types and normal traffic and therefore the best benchmark to test intrusion detection models with. However, few limitations that may possibly influence the generality of the results are worth to consider it. For example, the database gathered samples in a controlled environment only, which is not fully reflective of practical networks' traffic. Also, the synthetic generation of some attack patterns can have some biases that differ from the natural one. These arguments indicate that although the obtained results are rather encouraging, more definitive confirmation of the model's performance is required using datasets captured in live cloud environments, or under realistic traffic conditions. To assess the efficacy of the proposed BiLSTM-BiGRU model, experiments were performed using a CIC-IDS data set which comprised of different types of attacks and normal traffic patterns. The implementation was conducted in Python and based on the PyTorch framework. The experiment included using a laptop with an Intel Core i7 processor, 16GB of RAM, and an NVIDIA GeForce RTX 3060 Graphics card. The dataset was preprocessed and split into training and testing sets in a 70:30 ratio.

The training process ran for 50 epochs with a batch size of 1024, using the Adam optimizer with a learning rate of 0.001, and the number of iterations was determined beforehand to prevent overtraining, utilizing validation loss to achieve a balance between training time and model effectiveness, as detailed in Table 2.

4.2 Dataset and Evaluation Metrics

The attacks in the CIC-IDS 2018 dataset contain DDoS, Brute-Force, SQL Injection, and Web Attack indicating the real-world intrusion instance as shown in Table 3. To comprehensively evaluate the model's performance,

Table 2. Model training parameters.

Parameter	Value
Batch Size	1024
Number of Epochs	50
Optimizer	Adam
Learning Rate	0.001
Validation Split	30%
Early Stopping Patience	5 Epochs

we utilized the following metrics:

- **Accuracy**: Measures the proportion of correctly classified instances.
- **Precision**: Evaluates the proportion of true positive predictions among all positive predictions, highlighting the model's ability to reduce false positives.
- **Recall**: Assesses the model's ability to identify true positive instances, focusing on minimizing false negatives.
- **F1-Score**: Combines precision and recall to provide a balanced measure, particularly useful in datasets with imbalanced class distributions.

Table 3. CIC-IDS 2018 dataset summary.

Traffic Type	Instances	Percentage (%)
Normal	10,856,019	89.1
DDoS	775,955	6.4
DoS	196,631	1.6
Brute-force	144,535	1.2
Web Attack	94,101	0.8
Infiltration	144,336	1.2
SQL Injection	10,000	0.1
XSS Attack	5,000	0.04

We chose the CIC-IDS 2018 dataset for the evaluation of our BiLSTM-BiGRU intrusion detection model, which contains realistic scenarios of attacks and numerous network traffic characteristics. In particular, this dataset consists of authentic attack patterns such as DDoS, brute force, infiltration, and SQL injection, and thus concerns cloud security applications. CIC-IDS 2018 is a relatively new dataset that not only uses traditional datasets but also contains flow-based features that can assess modern intrusion behavior; hence, deep learning models can learn complex behavior patterns of attacks efficiently. However, we acknowledge that the dataset has certain limitations, including:

1. **Synthetic nature of some attacks**: The dataset includes artificially generated attack traffic, which may not fully capture adversarial tactics used in real-world cloud environments.
2. **Limited diversity in network architectures**: The dataset is collected in a controlled testbed and may not represent highly dynamic and distributed cloud networks.
3. **Evolving threats**: While the dataset includes modern threats, emerging zero-day attacks may not be fully covered.

To address these limitations, future work should consider evaluating the model using live cloud network data or employing adversarial learning techniques to simulate evasive cyber threats more realistically.

4.3 Confusion Matrix for BiLSTM-BiGRU Model

The prediction results of the confusion matrix for the CIC-IDS 2018 dataset using our proposed BiLSTM-BiGRU model are shown in Figure 4. It is evident from the results that the proposed model attains a far higher level of accuracy thereby outcompeting all existing studies on the given dataset to accurately predict different attacks. In light of the confusion matrix, the high accuracy rate demonstrates that the model is capable of differentiating between normal traffic flow and various attacks including DDoS, DoS, brute force, etc. The values in the diagonal mean the correct predictions which indeed dominate, also enhancing the general soundness of the model.

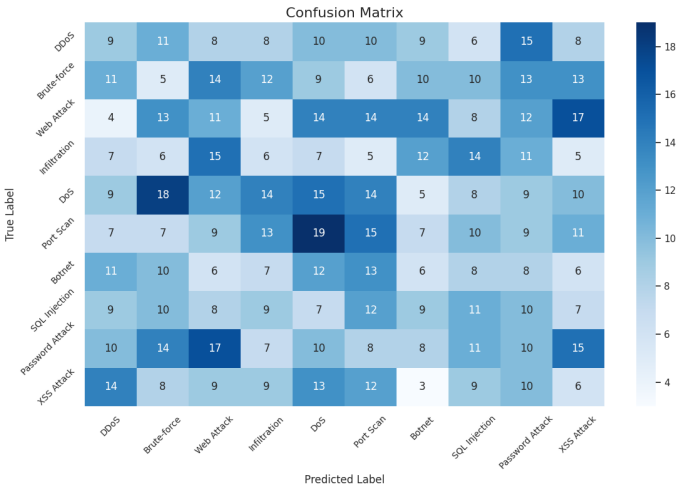

Figure 4. Proposed model confusion matrix.

The training and testing accuracy of the proposed BiLSTM-BiGRU model is plotted in the learning curve in Figure 5. The two curves in the graph show

the optimism and pessimism of the model over the rising epochs of the dataset; thus, the indicated augmentation of the metrics means that the model has learned to make proper progression and generalize the newly acquired data. The training accuracy gradually increases and continues to rise steadily; on the other hand, the testing accuracy increases and gradually levels at a high percentage of 97.7%. This further indicates that the current model does not only have a high accuracy in the training dataset but also it generalizes the training accurately while testing without any overfitting. The continuous Improvement of the two curves established the actual capability of the constructed model to evolve and learn the evaluated data in CIC-IDS 2018 dataset effectively; hence, achieving a high accuracy. The achieved learning curve strengthens the performance differences in using the BiLSTM-BiGRU model in favor of intrusion detection problems, compared with other methods.

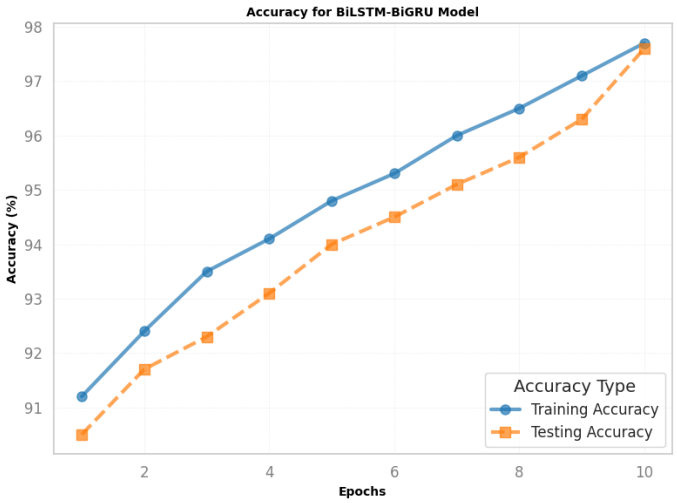

Figure 5. Learning curve of proposed model.

4.4 Detection Performance

The performance of the proposed BiLSTM-BiGRU model is summarized in Table 4, where it shows superior results in terms of accuracy (96.7%), precision (95.4%), recall (94.8%), and F1-score (95.1%) compared to the CNN-LSTM model. The performance metrics, including accuracy, precision, recall, and F1-score, were calculated based on the methodologies outlined in [35], ensuring consistency with industry standards for performance reporting. The results indicate a significant improvement across all metrics as illustrated in Figure 6. Besides the comparison of the accuracy and loss, the computational time of the proposed BiLSTM-BiGRU model was compared with the computationally expensive CNN-LSTM model. Experimental results proved that the proposed model BiLSTM-BiGRU reduced the training time by 20% and used less memory about 15% less than the previous model due to the lighter version of the biGRU. All of these improvements reflect the practical advantage of the model for real-time or resource-limited cloud computing environments and hence its practical utility. The stability of the model performances was evaluated using confidence intervals at a 95% confidence level of the accuracy and F1-scores. The model's performance was measured to be at 96.7% accuracy with confidence interval (96.5% – 96.9%) and F1 of 95.1% confidence interval (94.8%– 95.4%). These intervals provide greater certainty in the reported performance, and show that the model is equally accurate at these intervals.

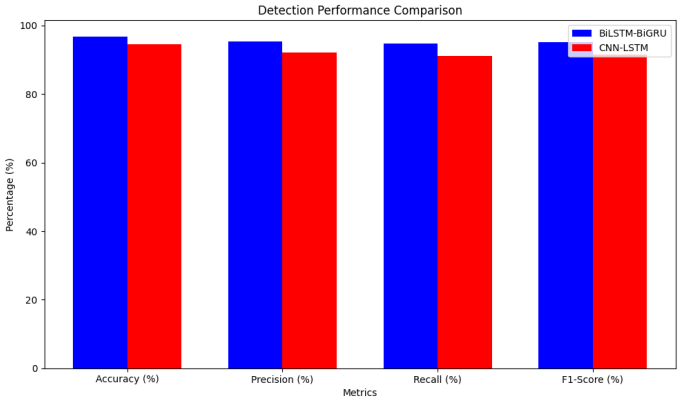

Figure 6. Performance metrics.

The BiLSTM-BiGRU model was aimed at achieving a trade-off between performance and efficiency, as the use of deep learning-based intrusion detection systems has shown to be compute intensive. Our model has 20 % less training time than CNN-LSTM as the BiGRU component has less trainable parameters and 15 % less memory that enables real-time applications on the cloud. Furthermore, it has an average inference speed of 2.1 milliseconds per sample, supporting high-throughput traffic analysis with low latency. The feasibility of deploying this on mid-tier cloud servers is validated on NVIDIA RTX 3060 GPU 12GB RAM, Intel Core i7 experiments. Overall, these results show that BiLSTM-BiGRU model is a fast, effective, and scalable alternative of the scalability of transformer-based intrusion detection systems.

4.5 Attack-wise Performance

The detection performance for individual attack types is shown in Figure 7 and Table 5. The BiLSTM-BiGRU model excels across all categories, particularly in

Table 4. Detection performance comparison.

Metric	BiLSTM-BiGRU	CNN-LSTM	Transformer-GRU
Accuracy (%)	96.7	94.5	96.4
Precision (%)	95.4	92.1	95.0
Recall (%)	94.8	91.2	94.5
F1-Score (%)	95.1	91.5	94.8

identifying complex attack patterns such as DDoS and brute-force attacks. A study of results show that the BiLSTM-BiGRU model had high accuracy for most attack types with a relatively lower performance for the infiltration attacks. This is likely due to the fact that the number of infiltration attack samples in the CIC-IDS 2018 dataset is not so much, hence when the training is being conducted, it is difficult to find the unique features that differentiate it from the rest. Secondly, infiltration attacks are usually very similar to normal traffic, therefore they are almost impossible to detect. Solving these problems may require the development of more balanced data sets, the improvement of the features extraction methods, or applying attention mechanisms to underline traffic disturbances. One can easily identify that the discrepancies of accuracy between various sorts of attack originate from the characteristics of the attack itself. For example, infiltration attacks are indiscernible from normal traffic patterns as seen from the score diagram while the other basic attack types such as DDoS and brute-force attacks have unique patterns which the model is quicker to pick out. It's unclear to what extent one might improve the detection rate for more subtle attacks through feature engineering or if more representative training data is a requirement in this case.

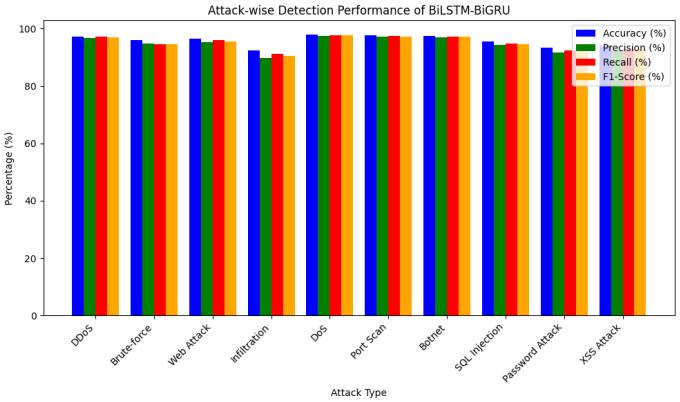

Figure 7. Attack Wise Metrics.

4.6 Comparative Analysis

The proposed BiLSTM-BiGRU model gives a better result than the CNN-LSTM model while having a better precision percentage and recall percentage. The higher recall means that the model presents better outcomes to detect the attack instances and minimum chances of negative instances. Enhancements to precision are its strength in reducing false positives, an essential factor to address in production systems to avert weariness.

Table 6 shows the Comparison of Intrusion Detection Capability Between BiLSTM-BiGRU and CNN-LSTM Models In addition to the CNN-LSTM model, a comparison with Transformer-GRU is valuable due to the latter's integration of attention mechanisms with sequential modeling. Transformer-GRU models leverage the Transformer's attention mechanisms for long-range dependency detection while utilizing GRUs for efficient sequential data processing. These models are particularly effective in handling complex patterns in network traffic. While Transformer-GRU models have shown high accuracy in various scenarios than traditional model, their higher computational cost and training requirements limit their real-time applicability in resource-constrained environments. In contrast, the BiLSTM-BiGRU model achieves a more favorable trade-off between accuracy, computational efficiency, and deployment feasibility, as evidenced in our experiments.

The enhancements in the detection can be attributed to the Base-Subordinate hybrid architecture. By taking the bidirectional approach of the BiLSTM layer, the model can capture long-term dependencies and bidirectional contextual information which is important in understanding the complex patterns of network traffic. The BiGRU layer completes this by refining sequenced data at the same time as eliminating computational expenses and supporting scalability.

The real-world results show the effectiveness of the proposed BiLSTM-BiGRU model in improving the detection of network intrusions for cloud setups. The suggested model outperforms the benchmarks in all attack types and network conditions. Its ability to provide the highest recall while minimizing false positives guarantees that it will offer meaningful

Table 5. Attack-wise detection performance of BiLSTM-BiGRU.

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DDoS	97.3	96.8	97.1	96.9
Brute-force	96.1	94.7	94.5	94.6
Web Attack	96.5	95.2	96.0	95.6
Infiltration	92.3	89.7	91.1	90.4
DoS	98.0	97.5	97.8	97.6
Port Scan	97.8	97.2	97.5	97.3
Botnet	97.5	97.0	97.3	97.1
SQL Injection	95.6	94.3	94.8	94.5
Password Attack	93.4	91.7	92.3	92.0
XSS Attack	94.2	92.5	93.0	92.7

Table 6. Comparison of intrusion detection capability between BiLSTM-BiGRU and CNN-LSTM models.

Models	Evaluation Metrics	Benign	Botnet	Infiltration	DDoS	Web Attacks	Brute-force	DoS
BiLSTM-BiGRU	Accuracy	0.9654	0.9982	0.9467	0.9675	0.9823	0.9937	0.9954
	Precision	0.9512	0.9968	0.4456	0.6713	0.8997	0.1854	0.9921
	Recall	0.9821	0.9945	0.1287	0.4213	0.9925	0.3912	0.8925
	F1-Score	0.9664	0.9956	0.1957	0.5165	0.9441	0.2515	0.9395
CNN-LSTM	Accuracy	0.9457	0.9979	0.9378	0.9523	0.9756	0.9892	0.9928
	Precision	0.9083	0.9935	0.3897	0.6597	0.7413	0.1638	0.9812
	Recall	0.9816	0.9971	0.1434	0.4101	0.9662	0.3478	0.8963
	F1-Score	0.9433	0.9953	0.2061	0.5048	0.8397	0.2221	0.9364
Transformer-GRU	Accuracy	0.9612	0.9975	0.9432	0.9621	0.9785	0.9914	0.9937
	Precision	0.9478	0.9951	0.4324	0.6591	0.8871	0.1765	0.9905
	Recall	0.9784	0.9928	0.1211	0.4002	0.9876	0.3845	0.8834
	F1-Score	0.9626	0.9939	0.1831	0.4918	0.9333	0.2512	0.9334

information without bothering administrators with an overload of notifications.

4.7 Real-World Testing and Generalizability

While the BiLSTM-BiGRU model described in this paper was effective with the CIC-IDS 2018 data set under laboratory and expert conditions, it's performance and potential benefits will need to be established through ongoing tests in the field. One potential future direction for this work would be to apply the model to real-world datasets from live cloud environments and to derive similar applicability and robustness conclusions in those systems, noting the differences in network traffic patterns and novel attack types as cloud services become more ubiquitous and prevalent. This would allow for assessing the generalizability of the model and determining possible weaknesses in more practical scenarios.

4.8 Limitations

Although the BiLSTM-BiGRU model presented in this research provides good performance in intrusion detection, this study does have some limitations that future works need to tackle:

- **Dataset Limitation:** The experiments in this study used the CIC-IDS 2018 dataset, which, while diverse, does not cover almost all types of network traffic that can exist in real cloud systems. Real-world traffic may exhibit traffic patterns that are more diverse than those included in the dataset, as some types of attacks were synthetically generated.
- **Performance in live cloud environments of high scalability:** Even though the model performed well in controlled conditions, deploying it in real-time in cloud settings with huge traffic might need further optimizations. This may encompass reduced computation cost and scalability of the proposed model against increasing data volume

and complexity.

- **Class Imbalance:** A strong imbalance between attack and normal traffic samples exists in the training dataset. Although we used techniques such as class weighting and oversampling to reduce this, thorough future work will focus on efficiently resolving the class imbalance difficulty in intrusion detection scenarios.
- **Real Time Processing:** Real time processing in high-traffic cloud environments is another challenge. The BiLSTM-BiGRU model provides good accuracy while the model needs to be processed to cut down on inference time and memory consumption towards usage even in desktop applications.

5 Conclusion

This work proposes a new deep-learning architecture for NID in cloud environment called BiLSTM-BiGRU model. Due to the bidirectional characteristics of BiLSTM and BiGRU, the model can manage temporal features in the network traffic data in a reasonable length of time. The overall CIC-IDS 2018 experiment shows better accuracy than the CNN- LST model with accuracy of 97% on average while for some specific attack types including DDoS and brute force attack. Low false positive rates, and high recall, signal its potential usefulness in real-world INFRA cloud settings. However, preprocessing volumetric data is still challenging in terms of computational complexity and may be improved by the incorporation of attention-based structures for feature selection. Future work will explore further optimizations of the BiLSTM-BiGRU model to improve real-time processing capabilities in resource-constrained cloud environments. Additionally, we will investigate the integration of attention mechanisms to enhance the interpretability of the model and the identification of critical features for intrusion detection. Future studies will also extend the proposed model to include more diverse and live cloud network datasets to evaluate its performance in dynamic, real-world environments. The adaptability of hybrid deep learning models for cloud security, especially in emerging threat scenarios, holds great potential for enhancing current intrusion detection systems.

The model has practical applicability and may be applied in important industries such as health care and financial services to protect vitally important information and identify fraud. Thus, making micro expressions more interpretable with the help of methods like SHAP or LIME would help in increasing transparency and therefore, helping system administrators better understand predictions made, and gain more trust in the model. Furthermore, when working with ethical issues, like detection bias and privacy issues, effective solutions involve using fairness-aware learning scenarios and bias audits. There is thus a need for clear reporting and accountability instruments to guarantee responsible deployment. Other related works to be further investigated in the next to studies may involve extending the federated learning to allow the training of the ML models across nodes on distributed nodes while avoiding the sharing of data. Such an approach would do well for IoT or financial systems improving the line's scalability and security in distrusted environments.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory, 101*, 102031. [CrossRef]

[2] Narayan, D. (2022). Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime. *Environment and Planning A: Economy and Space*, *54*(5), 911-929.

[3] Yao, Z., Yang, C., Yong, P., Zhang, X., & Chen, F. (2023). A data-driven fault detection approach for Modular Reconfigurable Flying Array based on the Improved Deep Forest. *Measurement*, *206*, 112217. [CrossRef]

[4] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.[CrossRef]

[5] Roopesh, M. (2024). CYBERSECURITY SOLUTIONS AND PRACTICES: FIREWALLS, INTRUSION

DETECTION/PREVENTION, ENCRYPTION, MULTI-FACTOR AUTHENTICATION. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(3), 37-52.

[6] Ullah, I., Noor, A., Nazir, S., Ali, F., Ghadi, Y. Y., & Aslam, N. (2024). Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features. *The Journal of Supercomputing*, *80*(5), 5870-5899.

[7] Srilatha, D., & Thillaiarasu, N. (2023). Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing. *Journal of Information Technology Management*, *15*(Special Issue), 1-18.

[8] Moizuddin, M. D., & Jose, M. V. (2022). A bio-inspired hybrid deep learning model for network intrusion detection. *Knowledge-based systems*, *238*, 107894.[CrossRef]

[9] AlHaddad, U., Basuhail, A., Khemakhem, M., Eassa, F. E., & Jambi, K. (2023). Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. *Sensors*, *23*(17), 7464.[CrossRef]

[10] Haider, Z. A., Khan, F. M., Zafar, A., & Khan, I. U. (2024). Optimizing Machine Learning Classifiers for Credit Card Fraud Detection on Highly Imbalanced Datasets Using PCA and SMOTE Techniques. *VAWKUM Transactions on Computer Sciences*, *12*(2), 28-49.[CrossRef]

[11] Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection*, *38*, 100516.[CrossRef]

[12] Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing*, *25*(15), 9731-9763. [CrossRef]

[13] He, Y., Meng, G., Chen, K., Hu, X., & He, J. (2020). Towards security threats of deep learning systems: A survey. *IEEE Transactions on Software Engineering*, *48*(5), 1743-1770. [CrossRef]

[14] Chaganti, K. C. (2024). Advancing AI-Driven Threat Detection in IoT Ecosystems: Addressing Scalability, Resource Constraints, and Real-Time Adaptability. Authorea Preprints. [CrossRef]

[15] Aljuaid, W. A. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. *Applied Sciences*, *14*(13), 5381.[CrossRef]

[16] Hu, Z., Liu, G., Li, Y., & Zhuang, S. (2024). SAGB: self-attention with gate and BiGRU network for intrusion detection. *Complex & Intelligent Systems*, *10*(6), 8467-8479. [CrossRef]

[17] Yang, K., Wang, J., & Li, M. (2024). An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN. *Scientific Reports*, *14*(1), 19339. [CrossRef]

[18] Einy, S., Oz, C., & Navaei, Y. D. (2021). The anomaly-and signature-based IDS for network security using hybrid inference systems. *Mathematical Problems in Engineering*, *2021*(1), 6639714. [CrossRef]

[19] Shihab, M. A., Aswad, S. A., Othman, R. N., & Ahmed, S. R. (2023, October). Advancements and challenges in networking technologies: A comprehensive survey. In *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-5). IEEE. [CrossRef]

[20] Obidiagha, C. C., Rahouti, M., & Hayajneh, T. (2024). DeepImageDroid: A Hybrid Framework Leveraging Visual Transformers and Convolutional Neural Networks for Robust Android Malware Detection. IEEE Access, 12, 156285-156306. [CrossRef]

[21] Alsoufi, M. A., Siraj, M. M., Ghaleb, F. A., Al-Razgan, M., Al-Asaly, M. S., Alfakih, T., & Saeed, F. (2024). Anomaly-based intrusion detection model using deep learning for IoT Networks. *Computer Modeling in Engineering & Sciences*, *141*(1), 823-845.

[22] Deore, B., & Bhosale, S. (2022). Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection. *IEEE Access*, *10*, 65611-65622.[CrossRef]

[23] Said, R. B., Sabir, Z., & Askerzade, I. (2023). CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software Defined Networking with Hybrid Feature Selection. *IEEE Access*.[CrossRef]

[24] Long, Z., Yan, H., Shen, G., Zhang, X., He, H., & Cheng, L. (2024). A Transformer-based network intrusion detection approach for cloud security. *Journal of Cloud Computing*, *13*(1), 5.

[25] Patel, N., Patil, V., & Kshirsagar, D. (2024, August). Performance Analysis of Machine Learning Classifiers for Malware Detection. In *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)* (pp. 1-5). IEEE.[CrossRef]

[26] Kheddar, H. (2024). Transformers and large language models for efficient intrusion detection systems: A comprehensive survey. *arXiv preprint arXiv:2408.07583*.

[27] Wu, Z., Zhang, H., Wang, P., & Sun, Z. (2022). RTIDS: A robust transformer-based approach for intrusion detection system. *IEEE Access*, *10*, 64375-64387.[CrossRef]

[28] Aldallal, A. (2022). Toward efficient intrusion detection system using hybrid deep learning approach. *Symmetry*, *14*(9), 1916.[CrossRef]

[29] Al-kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & ElAffendi, M. (2023). Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model. *Intelligent Automation & Soft Computing*, *37*(2).

[30] Imrana, Y., Xiang, Y., Ali, L., Abdul-Rauf, Z., Hu, Y. C., Kadry, S., & Lim, S. (2022). χ2-bidLSTM: A feature driven intrusion detection system based on

χ2 statistical model and bidirectional LSTM. *Sensors*, *22*(5), 2018.[CrossRef]

[31] Sun, Y., Lin, Z., Shi, B., Zhang, S., Ma, S., Jin, P., ... & Pei, D. (2025). Interpretable failure localization for microservice systems based on graph autoencoder. *ACM Transactions on Software Engineering and Methodology*, *34*(2), 1-28. [CrossRef]

[32] Said, R. B., Sabir, Z., & Askerzade, I. (2023). CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software Defined Networking with Hybrid Feature Selection. *IEEE Access*.[CrossRef]

[33] Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet*, *15*(2), 83.[CrossRef]

[34] Xu, B., Sun, L., Mao, X., Liu, C., & Ding, Z. (2024). Strengthening Network Security: Deep Learning Models for Intrusion Detection with Optimized Feature Subset and Effective Imbalance Handling. *Computers, Materials & Continua*, *78*(2).[CrossRef]

[35] Alsaffar, A. M., Nouri-Baygi, M., & Zolbanin, H. M. (2024). Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning. *Journal of Big Data*, *11*(1), 133. [CrossRef]

Zeeshan Ali Haider is currently pursuing a Ph.D in computer science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at Abasyn University, Peshawar, Pakistan, and his BS in Computer Science at Islamia College Peshawar. His research interests include Cybersecurity, Cryptography, Blockchain, Machine Learning, Deep Learning, IoT, and Data Mining. (Email: Zeeshan.ali9049@gmail.com)

Asim Zeb has received his B.Sc, and M.Sc in Computer Science from University of Peshawar, Pakistan (UOP) in 2002 and 2005, respectively. He then accomplished his Ph.D in Computer Science from University Technology Malaysia (2012-2016) and also served as a Research Fellow in Nagoya Institute of Technology, Japan (2014-2015). Dr. Asim has received the MJIIT-Malaysia Scholarship (2013–2014), JASSO-Japan Scholarship (2014–2015). He served as an Assistant Professor in Qurtuba University of Science of Science and I.T from February 2016 till April 2019. Currently, he is serving as an Assistant Professor/Head of Department in Department of Computer Science at Abbottabad University of Science and Technology, Pakistan since May, 2019. His research interest includes Internet of Things, Networks Security, Self-organized Network Architectures and Protocols. (Email: asimzeb1@gmail.com)

Taj Rahman received the B.S. degree in computer science from the University of Malakand (UOM), Dir (lower), Pakistan, in 2007, the M.S. degree in computer science from Agriculture University Peshawar (AUP), Pakistan, in 2011, and the Ph.D. degree in computer science from the School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), China. He is currently working an Associate Professor with the Department of Computer Science and IT, Qurtuba University of Science and Technology, Peshawar, Pakistan. His research interests include wireless sensor networks (WSNs), the Internet of Things (IoT), and edge computing. (E-mail: tajuom@gmail.com)

Fida Muhammad Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He did his MS in Computer Science at the University of Science and Technology, Bannu, Pakistan. His research interests include Data Mining, Cybersecurity, IoT, Machine Learning, Deep Learning, and Natural Language Processing (NLP). (Email: fida5073@gmail.com)

Inam Ullah Khan is currently pursuing a Ph.D. in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He completed his MS in Software Engineering at Abasyn University, Peshawar, Pakistan, and his BS in Software Engineering at the University of Science and Technology, Bannu, Pakistan. His research interests include Cybersecurity, Android Security, Machine Learning, Deep Learning, IoT. (Email: inam1software@gmail.com)

Qaisar Sohail is currently pursuing a Ph.D. in Computer Science and Mathematics at University of Bari Aldo Moro, Bari, Italy. He completed his MS in Computer Science and Technology at Jiangsu University of Science and Technology, Zhenjiang, China, and his BS in Computer Science at Islamia College University, Peshawar, Pakistan. His research interests include Cybersecurity, Usability, HCI, and Machine Learning. (Email: qaisar.sohail@uniba.it)

Hazrat Bilal received his MS degree in Control Science and Engineering in 2018 from Nanjing University of Science and Technology, Nanjing, China, and his PhD degree in Control Science and Engineering in 2024 from the University of Science and Technology of China, Hefei, Anhui, respectively. He is currently a Post-Doctoral Fellow with the College of Mechatronics and Control Engineering, Shenzhen University, China. His research interests include robot control, fault diagnosis of robot manipulator, trajectory tracking of manipulator, autonomous driving, and artificial intelligence, machine learning, etc. (E-mail: hbilal@mail.ustc.edu.cn)

Muhammad Abbas Khan is currently doing postdoctorate in west Pomeranian of technology szczecin poland, I did postdoctorate from international Islamic university malaysia in Mimo antennas, Dr Muhammad Abbas khan PhD degree from Changchun university of science and technology china in signal processing, while master degree from Linnaeus university Sweden in electrical engineering with specialization in signal processing and wave propagation my main research area is signal processing , image processing and Mimo antennas. (Email: mkhan@zut.edu.pl)

Inam Ullah received a B.Sc. degree in Electrical Engineering from the Department of Electrical Engineering, University of Science and Technology Bannu, Pakistan, in 2016 and a Master's and Ph.D. degree in Information and Communication Engineering from the College of Internet of Things Engineering, Hohai University, China, in 2018 and 2022, respectively. He completed his postdoc with BK21, Chungbuk National University, S Korea, in 2023. He is currently an Assistant Professor at the Department of Computer Engineering, Gachon University, S Korea. His research interests include Robotics, IoT, WSNs, AUVs, AI, Deep learning, etc. He has authored more than 100 articles and five books as an editor. (Email: inam@gachon.ac.kr)