2024 International Wireless Communications and Mobile Computing (IWCMC) | 979-8-3503-6126-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/IWCMC61514.2024.10592352

Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices

Mohammed Jouhari*, Mohsen Guizani†
*LSIA Laboratory, Moroccan School of Engineering Sciences (EMSI), Tanger, Morocco
†Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE
m.jouhari@emsi.ma, mohsen.guizani@mbzuai.ac.ae

Abstract—**Intrusion Detection Systems (IDSs) have played a significant role in detecting and preventing cyber-attacks within traditional computing systems. It is not surprising that the same technology is being applied to secure Internet of Things (IoT) networks from cyber threats. The limited computational resources available on IoT devices make it challenging to deploy conventional computing-based IDSs. The IDSs designed for IoT environments must also demonstrate high classification performance, utilize low-complexity models, and be of a small size. Despite significant progress in IoT-based intrusion detection, developing models that both achieve high classification performance and maintain reduced complexity remains challenging. In this study, we propose a hybrid CNN architecture composed of a lightweight CNN and bidirectional LSTM (BiLSTM) to enhance the performance of IDS on the UNSW-NB15 dataset. The proposed model is specifically designed to run onboard resource-constrained IoT devices and meet their computation capability requirements. Despite the complexity of designing a model that fits the requirements of IoT devices and achieves higher accuracy, our proposed model outperforms the existing research efforts in the literature by achieving an accuracy of 97.28% for binary classification and 96.91% for multiclassification.**

Index Terms—**Intrusion Detection Systems, Deep Learning, Convolutional Neural Networks, Long-Short-Term-Memory, UNSW-NB15.**

I. INTRODUCTION

The infrastructure of smart cities is increasingly vulnerable to cyberattacks as they expand and integrate ubiquitous IoT networks [1]. These attacks can pose a threat to public safety by disrupting critical services and compromising sensitive data. In interconnected networks like these, intrusion detection systems (IDS) play a crucial role in real-time monitoring and identification of malicious activity before it causes significant damage [2]. Although existing IDS solutions have shown promising results, they often face challenges in smart city environments. Traditional rule-based systems struggle to adapt to constantly evolving attack patterns, while complex deep learning models can be computationally expensive and resource-intensive for resource-constrained smart city devices [3]. These IoT devices, which include temperature sensors and smart devices for monitoring light bulbs or thermostats, are characterized by their small size and limited functionality. The data collected by these devices is transmitted via the internet for storage and analysis, making security measures necessary to protect personal, private, or sensitive information [4].

IoT has enhanced individuals' lifestyles by introducing automated services. As a result of this unchecked growth, privacy and security concerns have become increasingly important. Addressing these concerns is a challenging task due to the inherent complexity of dynamic and diverse IoT ecosystems. Consider protecting such a dynamic environment as a smart city or smart home which are characterized by their constrained visibility of the network, and the lack of professional support for the devices after their first use. This makes the traditional network security methods ineffective due to the dynamic nature of this environment. The risk to user privacy and the environment's general security is further increased by the fact that many interconnected IoT devices are poorly designed and do not receive regular security updates. Thus, to fully realize the potential of IoT-based smart environments, creative solutions that prioritize security and privacy while also being able to adapt to this ever-changing environment are required [5].

Previous research on smart city IDS has predominantly utilized traditional machine learning (ML) techniques like decision trees and Support Vector Machines (SVMs) to enhance IDS performance. While these methods deliver respectable accuracy, they require extensive manual feature engineering and often suffer from high rates of false positives. In contrast, deep learning methods, especially convolutional neural networks (CNNs), have emerged as promising alternatives due to their ability to autonomously extract features from network traffic data. However, their substantial computational demands render them impractical for smart city devices with limited resources. In this study, we introduce several key contributions:

1) We propose a novel hybrid approach that integrates lightweight CNNs with bidirectional Long Short-Term Memory (LSTM) networks to achieve efficient and accurate intrusion detection in IoT networks.
2) We develop a customized CNN architecture optimized for IoT devices, featuring fewer layers and parameters to facilitate efficient data processing. This architecture efficiently extracts critical features from network traffic, which are subsequently processed by a bidirectional LSTM for accurate classification of normal and

979-8-3503-6126-1/24/$31.00 ©2024 IEEE

malicious activities.

3) Our hybrid model combines the strengths of both CNNs and LSTMs, addressing the limitations inherent in each method.
4) To tackle the challenge of imbalanced datasets, we implement a weighted loss function in our multiclassification model. The weights are assigned based on the relative frequency of each attack type within the UNSW-NB15 dataset, enhancing model fairness and accuracy.

The remainder of this paper is structured as follows: Section 2 reviews relevant literature related to our study. Section 3 offers a detailed description of our proposed hybrid intrusion detection approach, including the lightweight CNN-BiLSTM architecture, and outlines the dataset and evaluation metrics used in our analysis. Section 4 presents the experimental results and discusses our findings. Finally, Section 5 concludes the paper by summarizing our contributions and outlining future directions for this research.

II. Related work

The authors in [6] tackle anomaly detection in IoT networks by proposing a 1D CNN-LSTM model. This model leverages CNNs for spatial feature extraction and LSTMs for temporal analysis, achieving 99.20% accuracy and 0.80% false alarm rate on the Bot-IoT dataset. It offers both binary and multiclass detection, surpassing other methods and demonstrating potential for real-world applications. Our previous paper [7] investigated a novel approach to improve anomaly detection in IoT networks using conditional Generative Adversarial Networks (cGANs). We addressed the issue of unbalanced data and lack of specific attack samples by generating realistic adversarial malware examples. This training process enhanced our CNNLSTM-based IDS model, increasing its accuracy in detecting theft attacks by 40%.

Many researchers have explored how to improve IDS performance using the UNSW-NB15 dataset, which is popular for its realistic and diverse network traffic data, including both normal and attack activities. A Feed-Forward Neural Network and the UNSW-NB15 dataset are used in the paper [8] to investigate the use of Deep Learning for Network IDS. In the article, it is argued that traditional machine learning fails to detect intrusions accurately because of the complexity of modern network threats. As a result of their experiments, the authors were able to achieve high accuracy and lower false alarm rates compared to existing machine learning models by finding the optimal activation functions and features. In this paper [9], the authors proposed IGRF-RFE, a hybrid feature selection method for network intrusion detection that combined filter and wrapper techniques. IGRF-RFE successfully identified and eliminated irrelevant features, reducing the feature count from 42 to 23 while simultaneously improving anomaly detection accuracy from 82.25% to 84.24% on the UNSW-NB15 dataset. These results suggest that IGRF-RFE could have been a valuable tool for building more efficient and accurate IDSs.

TABLE I
Categories of the UNSW-NB15 Dataset

No.	Type	Description
1	Normal	Routine, legitimate network traffic
2	Analysis	Attempts to uncover vulnerabilities through web application attacks
3	Backdoor	Covertly bypasses authentication for unauthorized remote access
4	DoS	Disrupts system resources through memory-based attacks
5	Exploits	Leverages network errors or bugs for malicious purposes
6	Fuzzers	Crashes systems by overwhelming them with random data
7	Generic	Exploits block-cipher vulnerabilities using hash functions
8	Reconnaissance	Gathers information to evade security controls
9	Shellcode	Executes code to exploit software vulnerabilities
10	Worms	Self-replicating malware that spreads across systems

In [10], the authors explored the use of Support Vector Machines (SVMs) with a new scaling method to detect network intrusions in the modern UNSW-NB15 dataset. They compared their method to previous approaches on both binary and multi-class classification tasks. The paper highlights the effectiveness of SVMs with a new scaling method for intrusion detection on the more realistic UNSW-NB15 dataset, especially compared to older methods and datasets. The authors in [11] proposed a new Network Intrusion Detection System (NIDS) for protecting Internet of Things (IoT) devices from cyberattacks. The system used LSTM layer, which could learn from past data to identify both known and unknown attacks. This showed an improvement over older methods that struggled to detect new attacks. The researchers tested their system on two large datasets of network traffic and found it to be more accurate than previous methods, while also reducing false alarms.

III. Hybrid CNN model for the UNSW-NB15 dataset

A. Description of the UNSW-NB15 dataset

The UNSW-NB15 dataset provides a realistic snapshot of modern network traffic, encompassing both routine activity and a diverse range of nine contemporary attack types, including DoS, backdoors, and reconnaissance. Its clear organization with ten distinct data types and balanced representation of normal and malicious traffic makes it a valuable resource for developing and evaluating IDS. Refer to Table I for detailed information on each data type.

This work utilizes the UNSW-NB15 dataset, which comprises 257,673 data instances (175,341 training and 82,332 testing), carefully split without redundancy to ensure reliable

TABLE II
FEATURES OF UNSW-NB 15 DATASET

No.	Name of Feature	No.	Name of Feature
1	proto	23	response_body_len
2	rate	24	sinpkt
3	dur	25	dinpkt
4	service	26	sjit
5	state	27	djit
6	spkts	28	tcprtt
7	dpkts	29	synack
8	sbytes	30	ackdat
9	dbytes	31	ct_srv_src
10	sttl	32	ct_srv_dst
11	dttl	33	ct_src_ltm
12	sload	34	ct_dst_ltm
13	dload	35	ct_dst_src_ltm
14	sloss	36	ct_src_dport_ltm
15	dloss	37	ct_dst_sport_ltm
16	swin	38	ct_state_ttl
17	dwin	39	is_ftp_login
18	stcpb	40	ct_ftp_cmd
19	dtcpb	41	ct_flw_http_mthd
20	smeansz	42	is_sm_ips_ports
21	dmeansz	43	attack_cat
22	trans_depth	44	label

NIDS evaluations. Both sets share identical attack types, further detailed in Table I. Each data point boasts 44 features categorized into six groups: flow, basic, content, time, additional generated (divided into general-purpose and connection features), and labeled attack classes. Features #1-#30 represent core network packet information, while additional and connection features (#31-#42) provide deeper insights. Labeled features (#43-#44) serve for supervised learning tasks (refer to Table II). This comprehensive dataset offers a robust platform for exploring intrusion detection in modern networks such as the IoT network in smart cities.

B. Lightweight CNN-BiLSTM

Traditional IDS often rely on rule-based systems or shallow machine learning models, which can struggle with the evolving nature of cyberattacks and the resource constraints of resource-constrained IoT devices. To address these challenges, we propose a novel hybrid model that combines the strengths of lightweight convolutional neural networks (CNNs) with bidirectional Long Short-Term Memory (BiLSTM) layers [12] for effective intrusion detection in IoT networks. The first stage of our model utilizes a lightweight CNN architecture specifically designed for efficient processing on edge devices. This CNN employs fewer layers and parameters compared to standard CNNs, reducing computational complexity and memory footprint while maintaining acceptable accuracy. The convolutional layers extract spatial features from the network traffic data, identifying patterns and relationships between different data points.

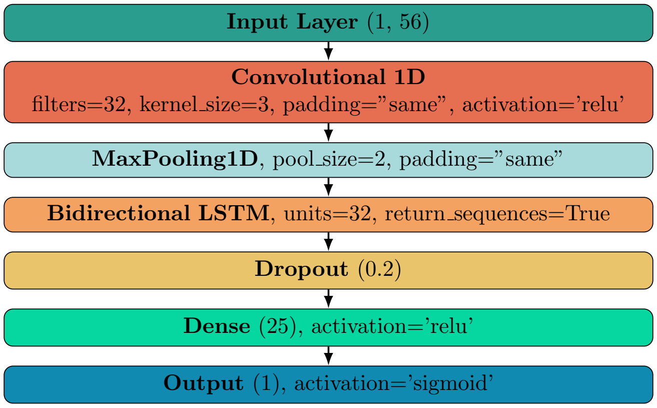
Input Layer (1, 56)
Convolutional 1D
filters=32, kernel_size=3, padding="same", activation='relu'
MaxPooling1D, pool_size=2, padding="same"
Bidirectional LSTM, units=32, return_sequences=True
Dropout (0.2)
Dense (25), activation='relu'
Output (1), activation='sigmoid'

Fig. 1. The architecture of our Lightweight CNN-BiLSTM Model with 7841 Trainable Parameters for UNSW-NB15 Dataset Classification

The extracted features are then fed into a BiLSTM layer, which excels at capturing temporal dependencies within sequential data. Figure 1 present the architecture of our proposed CNN-BiLSTM model. This is particularly valuable for network traffic analysis, as cyberattacks often exhibit specific patterns over time. The BiLSTM analyzes the sequence of features, learning the underlying dynamics and identifying anomalies that deviate from normal network behavior. The outputs from the CNN and BiLSTM layers are combined, leveraging the strengths of both approaches. The combined features are then fed into a final decision-making layer, such as a sigmoid classifier, which determines the class of the network traffic (normal or malicious). The BiLSTM model is comprised of a pair of LSTM units. One LSTM unit processes the input sequence in the forward direction, while the other LSTM unit processes it in the reverse direction. In Figure 2, we can see that the forward LSTM analyzes the input sequence from the start to the end, while the backward LSTM operates in the opposite direction. At each time step, the hidden states of the two LSTMs are combined or concatenated to create the final hidden state sequence. This combined sequence is then forwarded to the subsequent layer. The mathematical representation of this process is provided by Equations:

$$\mathbf{h}_t^{(f)} = \text{LSTM}^{(f)}\left(\mathbf{x}_t, \mathbf{h}_{t-1}^{(f)}, \mathbf{c}_{t-1}^{(f)}\right) \quad (1)$$

$$\mathbf{h}_t^{(b)} = \text{LSTM}^{(b)}\left(\mathbf{x}_t, \mathbf{h}_{t+1}^{(b)}, \mathbf{c}_{t+1}^{(b)}\right) \quad (2)$$

$$\mathbf{h}_t = [\mathbf{h}_t^{(f)}; \mathbf{h}_t^{(b)}] \quad (3)$$

where $\mathbf{h}_t^{(f)}$ and $\mathbf{h}_t^{(b)}$ represent the forward and backward hidden states at time step t, respectively. $\mathbf{c}_{t-1}^{(f)}$ and $\mathbf{c}_{t-1}^{(b)}$ represent the forward and backward cell states at time step t,

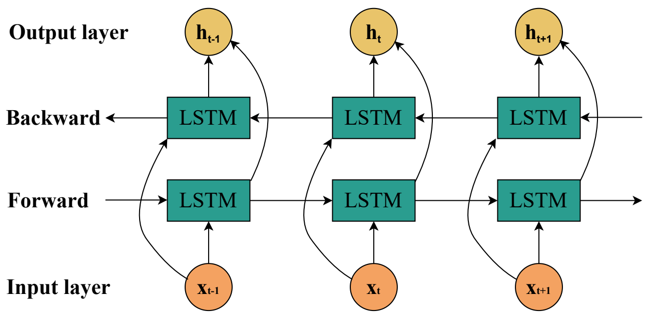

Fig. 2. BiLSTM architecture.

respectively. $\mathbf{x}_t$ represents the input vector at time step t. $\mathbf{h}_t$ represented the concatenation of the forward and backward hidden states into a single vector.

C. Measuring NIDS Performance: Key Metrics

To assess the effectiveness of NIDS, we analyze key metrics derived from the confusion matrix, which maps the system's accuracy in classifying network traffic. We consider in the work the following parameters:

1) **Accuracy:** Measures the overall correctness of the NIDS, reflecting the proportion of correct predictions (both attacks and normal traffic) out of all predictions.

$$\text{Accuracy} = \frac{(\text{ TP + TN })}{(\text{ TP + TN + FP + FN })}$$

2) **Recall (also known as Detection Rate or Sensitivity):** Measures the NIDS's ability to correctly identify actual attacks. It focuses on how many of the actual attacks were correctly detected.

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

3) **Precision:** Measures the proportion of predicted attacks that were actually correct. It focuses on how many of the predicted attacks were true positives.

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

4) **F1-Score:** Combines precision and recall into a single metric, providing a balanced view of the NIDS's performance.

$$\text{F1-Score} = \frac{2 * (\text{Precision} * \text{Recall})}{\text{Precision + Recall}}$$

While overall accuracy, encompassing both attack and normal traffic classification, plays a crucial role in assessing NIDS performance, its limitations within imbalanced datasets become readily apparent. In such scenarios, we prioritize recall, ensuring minimal missed attacks, as even a single undetected threat can have significant consequences. Conversely, high precision, minimizing false alarms, becomes vital to avoid resource drain and maintain operational efficiency. Ultimately, the F1-score, harmonizing these dual perspectives, offers a more nuanced understanding of the NIDS's efficacy, balancing attack detection with false alarm mitigation for robust network security.

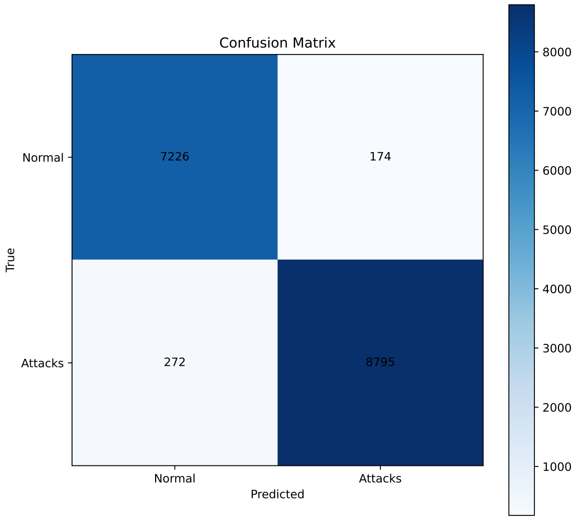

Fig. 3. CNN-BiLSTM confusion matrix for binary classification of attacks.

IV. Experimental Results and Analysis

Our experiments, powered by Python and TensorFlow on a standard PC, investigated the feasibility of Lightweight CNNs for intrusion detection compared to traditional ML methods. Leveraging the versatile UNSW-NB15 dataset for multi-class classification, we built a custom CNN architecture within TensorFlow to assess its performance against established methods. This setup enabled a clear comparison of their effectiveness and resource demands, providing valuable insights for deploying CNNs in real-world network security scenarios.

The confusion matrix in Figure 3 presents the performance of our proposed model in classifying attacks on the UNSW-NB15 dataset. The horizontal axis (X-axis) represents the model's predicted attack categories for the testing data, while the vertical axis (Y-axis) shows the actual attack categories based on the ground truth labels. Our model achieved 7,226 true positives and 8,795 true negatives, correctly identifying both normal and attack instances. However, it also generated 272 false negatives (missed attacks) and 174 false positives (incorrectly identified attacks). While this translates to an overall accuracy of 97%, as mentioned in the previous figure, we are committed to exploring methods to address the remaining false positives and negatives.

Table III presents a performance evaluation of our CNN-BiLSTM model compared to traditional ML models from the literature. We assessed accuracy, recall, precision, and F1-score. While precision and recall are typically used for imbalanced data, we primarily use precision here to gauge our model's overfitting prevention capabilities. Combining these parameters through the F1-score provides a comprehensive understanding of our model's performance. Furthermore, we considered training and inference times to demonstrate the proposed model's suitability for resource-constrained IoT devices. As shown in the table, our model outperforms existing

TABLE III
PERFORMANCE COMPARISON OF CNN-BILSTM AND TRADITIONAL ML MODELS FOR BINARY CLASSIFICATION IN UNSW-NB15

	Accuracy	Recall	Precision	F1-Score	time to train (s)	time to predict (s)	total time (s)
Logistic Regression	92.80%	92.80%	92.83%	92.80%	1.2	0.0	1.2
KNN	95.04%	95.04%	95.09%	95.05%	0.0	15.3	15.3
Decision Tree	96.56%	96.56%	96.56%	96.56%	1.0	0.0	1.0
Gradient Boosting Classifier	95.85%	95.85%	95.86%	95.85%	27.4	0.0	27.4
MLP	96.34%	99.99%	55.05%	70.60%	21.3	21.9	43.2
LSTM	96.49%	96.49%	96.49%	96.49%	70.9	22.4	93.3
Proposed model	97.28%	96.44%	98.59%	97.43%	122.5	3.8	126.3

TABLE IV
COMPARING ACCURACY: PROPOSED CNN-BILSTM MODEL AND RECENT WORKS WITH HYBRID CNN AND LSTM ARCHITECTURE FOR BINARY CLASSIFICATION IN THE UNSW-NB15 DATASET

Ref	Year	Dataset	Algorithm	Accuracy
[13]	2021	CIC-IDS2017	BiLSTM	97.72%
[14]	2023	NSL-KDD	CNN-BiLSTM	99.9%
[15]	2023	NSL-KDD	CNN-BiLSTM	99.4%
		UNSW-NB15		82.3%
		CIC-IDS2017		99.53%
[16]	2023	UNSW-NB15	CNN-LSTM	93.21%
Proposed model	2024	UNSW-NB15	CNN-BiLSTM	97.28%

models in terms of accuracy, achieving 97.28% compared to the best LSTMs using Keras (96.49%). This suggests that our model can more effectively detect attacks on the UNSW-NB15 dataset. Our model also achieves the highest precision (98.59%), ensuring highly accurate attack classification. Since our focus is on resource-constrained IoT devices in smart cities, we evaluated the model's training and inference times. While the training time of 122.5 seconds might seem long for on-device processing, training usually happens offline in real-world applications, so this factor doesn't affect our model's performance. More importantly, the inference time of 4 seconds is significantly faster than other deep learning models, even though we're not aiming for real-time processing.

In Table IV, we summarize and compare the accuracy of our proposed CNN-BiLSTM model with recent works that adopt the same CNN-LSTM architecture. We observe that this architecture has already been used to improve the accuracy of IDS, not only on the UNSW-NB15 dataset but also on other traditional datasets in the field. In contrast, this work focuses on designing a lightweight hybrid model for resource-constrained devices using the BiLSTM. Regarding performance, we achieved a higher accuracy compared to works based on the UNSW-NB15 dataset. However, some works using the same architecture have achieved higher accuracy on the NSL-KDD dataset. This might be attributed to the larger number of features in UNSW-NB15 compared to NSL-KDD, potentially requiring more sophisticated feature selection for optimal performance.

Table V shows the results of the multiclassification of our CNN-BiLSTM model compared to the traditional model. To obtain these results, we made some adjustments to our model compared to the binary classification while keeping the same architecture. The adjustments involved the hyperparameters of the model, including the number of epochs, batch size, and learning rate. These changes affected the training and prediction times. The results of the multiclassification were lower than those obtained in the binary classification due to the complexity of the task, which involves classifying 10 attacks using the proposed model. However, the obtained results demonstrate that our model outperforms other models in terms of accuracy, precision, recall, and F1-score, which are respectively 96.91%, 97.54%, 97.13%, and 97.33%. Although the proposed model requires more time in the training phase due to adjustments in the number of epochs and batch size, it is always performed offline before deploying the model on resource-constrained IoT devices. Once deployed, these devices will act as IDS, and even with the increased training time and resource consumption, our model still meets the requirements of these devices in terms of resource usage due to the relatively lower time and resource needed for prediction.

Figure 4 presents the confusion matrix for our CNN-BiLSTM multiclassification model on the UNSW-NB15 dataset, allowing us to evaluate each attack class individually. The dataset contains 10 attack classes, as shown in the x and y labels. The x-axis represents the ground truth (true labels), while the y-axis shows the predicted classes by our model. The diagonal, running from top-left to bottom-right, reflects the model's effectiveness in classifying each attack type. Darker squares indicate higher accuracy for that specific class. However, for minority classes like ”Analysis,” ”Shellcode,” and ”Worms,” the square colors might be less reliable due to the limited number of samples in the test data. By using a weighted loss function, our model prioritizes achieving better accuracy on these minority classes. This is evident in the correct detection of all 9 worms and the classification of 75 out of 76 Shellcode attacks with only one false negative. Conversely, the normal traffic class has the darkest square due to its high accuracy and abundance of samples. Overall, the confusion matrix serves as a visual representation of the model's accuracy. Generally, a darker diagonal signifies

TABLE V
PERFORMANCE COMPARISON OF CNN-BILSTM AND TRADITIONAL ML MODELS FOR MULTICLASSIFICATION IN UNSW-NB15

	Accuracy	Precision	Recall	F1-Score	Time to Train (s)	Time to Predict (s)
Logistic	91.83%	94.31%	92.74%	93.53%	2.20	0.10
KNN	93.06%	95.06%	93.80%	94.43%	0.30	10.10
Decision Tree	84.10%	89.89%	86.28%	88.09%	0.20	0.10
GBC	75.47%	85.16%	79.11%	82.09%	55.90	0.10
MLP	96.74%	97.45%	97.00%	97.22%	122.80	0.10
LSTM	96.11%	97.02%	96.43%	96.72%	90.80	15.10
Proposed Model	96.91%	97.54%	97.13%	97.33%	1220.20	3.20

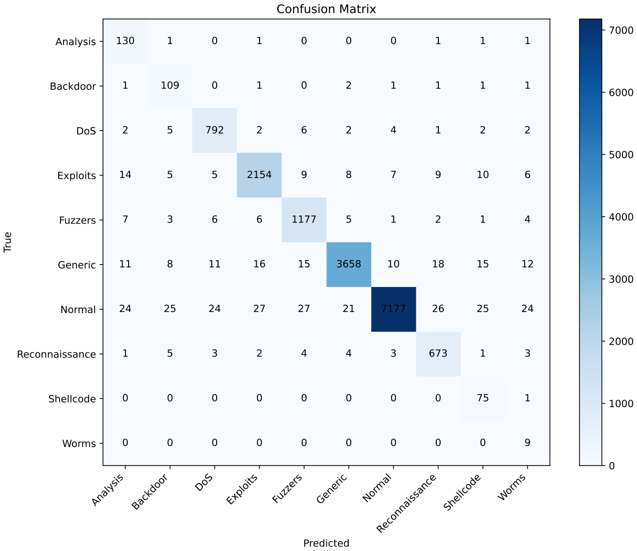

Fig. 4. CNN-BiLSTM confusion matrix for multiclassification of attacks.

higher overall performance.

V. CONCLUSION

In this study, we developed a lightweight CNN-BiLSTM model tailored for resource-constrained IoT devices, addressing a critical gap in the application of complex machine learning models for IDS. Traditional models, while effective, are often unsuitable for such devices due to their computational demands. Our model not only considers model complexity but also achieves high accuracy, with binary and multiclass classification accuracies of 97.28% and 96.91%, respectively, on the UNSW-NB15 dataset. When compared to recent hybrid CNN-LSTM architectures, our model demonstrates superior performance on the UNSW-NB15 dataset, despite some models achieving up to 99% accuracy on the NSL-KDD dataset. Moving forward, we aim to refine our approach by exploring Bayesian Optimization for hyperparameter tuning to enhance the performance of simpler models, thereby advancing research in IDS for IoT environments.

REFERENCES

[1] M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud, "A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023.

[2] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. U. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," *IEEE Access*, vol. 12, pp. 4745–4761, 2024.

[3] M. Jouhari, K. Ibrahimi, J. B. Othman, and E. M. Amhoud, "Deep Reinforcement Learning-Based Energy Efficiency Optimization for Flying LoRa Gateways," in *ICC 2023 - IEEE International Conference on Communications*, pp. 6157–6162, 2023.

[4] S. Li, H. Song, and M. Iqbal, "Privacy and Security for Resource-Constrained IoT Devices and Networks: Research Challenges and Opportunities," *Sensors*, vol. 19, no. 8, 2019.

[5] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021.

[6] H. Benaddi, M. Jouhari, K. Ibrahimi, A. Benslimane, and E. M. Amhoud, "Improvement of Anomaly Detection System in the IoT Networks Using CNN-LSTM Approach," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023.

[7] H. Benaddi, M. Jouhari, K. Ibrahimi, A. Benslimane, and E. M. Amhoud, "Adversarial Attacks Against IoT Networks Using Conditional GAN Based Learning," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, pp. 2788–2793, 2022.

[8] L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye, and L. Zhijun, "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 299–303, 2019.

[9] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, "IGRF-RFE: A Hybrid Feature Selection Method for MLP-Based Network Intrusion Detection on UNSW-NB15 Dataset," *Journal of Big Data*, vol. 10, no. 1, 2023.

[10] D. Jing and H.-B. Chen, "SVM Based Network Intrusion Detection for the UNSW-NB15 Dataset," in *2019 IEEE 13th International Conference on ASIC (ASICON)*, pp. 1–4, 2019.

[11] K. Saurabh, S. Sood, P. A. Kumar, U. Singh, R. Vyas, O. P. Vyas, and R. Khondoker, "LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks," 2022.

[12] Y. Tatsunami and M. Taki, "Sequencer: Deep LSTM for Image Classification," in *Advances in Neural Information Processing Systems* (A. H. Oh, A. Agarwal, D. Belgrave, and K. Cho, eds.), 2022.

[13] O. M. A. Alsyaibani, E. Utami, and A. D. Hartanto, "An Intrusion Detection System Model Based on Bidirectional LSTM," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, pp. 1–6, 2021.

[14] A. Abdelkhalek and M. Mashaly, "Addressing the Class Imbalance Problem in Network Intrusion Detection Systems Using Data Resampling and Deep Learning," *The Journal of Supercomputing*, pp. 1–34, 2023.

[15] H. Peng, C. Wu, and Y. Xiao, "CBF-IDS: Addressing Class Imbalance Using CNN-BiLSTM with Focal Loss in Network Intrusion Detection System," *Applied Sciences*, vol. 13, no. 21, 2023.

[16] H. C. Altunay and Z. Albayrak, "A Hybrid CNN+LSTM-Based Intrusion Detection System for Industrial IoT Networks," *Engineering Science and Technology, an International Journal*, vol. 38, p. 101322, 2023.