Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems

Hao Xue
1023041134
Nanjing University of Posts and Telecommunications
Jiangsu, Nanjing China

***Abstract*—Protecting Internet of things (IoT) devices against cyber attacks is imperative owing to inherent security vulnerabilities. These vulnerabilities can include a spectrum of sophisticated attacks that pose significant damage to both individuals and organizations. Employing robust security measures like intrusion detection systems (IDSs) is essential to solve these problems and protect IoT systems from such attacks. In this context, our proposed IDS model consists on a combination of convolutional neural network (CNN) and long short-term memory (LSTM) deep learning (DL) models. This fusion facilitates the detection and classification of IoT traffic into binary categories, benign and malicious activities by leveraging the spatial feature extraction capabilities of CNN for pattern recognition and the sequential memory retention of LSTM for discerning complex temporal dependencies in achieving enhanced accuracy and efficiency. In assessing the performance of our proposed model, the authors employed the *new* CICIoT2023 dataset for both training and final testing, while further validating the model's performance through a conclusive testing phase utilizing the CICIDS2017 dataset. Our proposed model achieves an accuracy rate of 98.42%, accompanied by a minimal loss of 0.0275. False positive rate (FPR) is equally important, reaching 9.17% with an F1-score of 98.57%. These results demonstrate the effectiveness of our proposed CNN-LSTM IDS model in fortifying IoT environments against potential cyber threats.**

***Index Terms*—Intrusion detection system, deep learning, internet of things, CNN, LSTM, cyber security, CICIoT2023.**

I. Introduction

IoTs have grown notably to sweep the whole world, it involves billions of devices connected to each other without any human interactions (interplay). The IoT generates large data analytics through using sensors, actuators, and control devices. These data are leveraged for diverse tasks and objectives across different fields including healthcare, industry, agriculture, military, and other sectors. The expansive realm of the IoT is proportionate to its exposure to a myriad of threats and cyber attacks that have the potential to compromise the integrity and security of connected devices and networks. Hence, it is imperative to address optimal solutions for countering such behaviors. Moreover, IDSs assume a pivotal role in identifying and mitigating cyber attacks in any network [1–3].

An IDS functions as a monitoring tool, it serves to identify any form of potentially malicious network traffic such as intrusion attempts, viral attacks, and suspicious traffic that pose threats to the security of information systems based on standards when activities deviate from these standards or baseline, the IDS alerts us at an early stage. In the realm of security components, IDSs provide two distinct forms : (1) host-based (HIDS) which focuses on monitoring and analyzing activities transpiring on a server, and (2) network-based (NIDS), tasked with the observation of network activities and communications [4]. Numerous organizations opt for a hybrid approach, incorporating both HIDS and NIDS [5].

Based on the nature of the analysis performed, IDSs are categorized as either signature-based or anomaly-based [6]. Signature-based schemes, alternatively referred to as misuse-based, aim to identify predefined patterns, or signatures, within the analyzed data, these systems serve to identify specified and well-known attacks but may fail to detect novel and unfamiliar intrusions [4, 6–8]. Whereas, the anomaly-based IDSs are employed to observe the behavior of a standard network and establish a threshold for detecting deviations from the norm [4]. Their main benefit is the ability to detect previously unseen and unknown intrusion activities [9].

In addressing security threats, IDS software is frequently developed employing artificial intelligence (AI) algorithms, including techniques such as machine learning (ML) and data mining (DM). These methods have proven to be highly effective, in identifying intrusions [7]. DL is a broader subfield of ML, its architectural configuration comprises an initial input layer succeeded by a series of hidden layers, which subsequently propagate inputs to the output layer [1]. The CNN represents a DL model extensively applied in different domains, like in [10] for image classifications, in [11–14] for speech processing and security, and in [15] for cyber attacks. LSTM is a special class of recurrent neural network (RNN), which lies in its capability to be directly applied to raw data without necessitating the usage of any feature selection methods [1]. Nevertheless, LSTM entails a lengthier training duration and demands more computational resources compared to CNN [9]. Hence, this study introduces an advanced unified model, CNN-LSTM, which combines the strength of CNN and LSTM models. The below steps constitute the procedural flow and the contribution of this paper.

979-8-3503-5026-5/24/$31.00 ©2024 IEEE

- Propose a new IDS using CNN-LSTM hybrid model for enhancing the security of IoT infrastructures,
- The assessment of the suggested model entails employing a subset of the new CICIoT2023 dataset. The effectiveness and generalizability of the proposed approach are validated through its application to other segments of the same dataset, as well as a distinct CICIDS2017 dataset,
- Compare our proposed methodology with the existing state-of-the-art work using diverse datasets.

The remaining sections of the paper are structured as follows: Section II gives preliminaries that contain a literature review. Section III provides the proposed methodology. This is followed by section IV which delves into the aspects of experimentation, results, and discussion. Section V covered our conclusion and future directions.

II. Literature review

DL models have successfully demonstrated considerable efficacy across various fields such as cyber security, image processing, speech recognition, healthcare, and many more. These methods are notably pronounced in their effectiveness compared to traditional ML techniques.

The focus area of [16] is the combination of the strengths of convolutional auto-encoders (CAE) and one-class support vector machine learning (SVM), aiming to enhance the performance of network intrusion detection. The proposed work uses the CAE to extract meaningful features from network traffic and detect anomalies, then the authors apply one-class SVM to classify network traffic into normal and abnormal categories. They have used two benchmark datasets to validate their proposed scheme. The results obtained outperform the existing traditional ML and DL.

However in [17], the paper investigates adversarial attacks on DL-based IDS for IoT network security, they have employed two DL models including feed-forward neural networks (FNN) and self-normalizing neural networks (SNN) in order to classify intrusion attacks in IoT networks. The results demonstrate that the FNN is well at multi-classification metrics such as Cohen Cappa's score. Upon assessment of adversarial robustness, the SNN demonstrates better resilience when confronted with adversarial samples derived from the IoT dataset. Chouhan et al. [18] introduced an architectural framework termed channel boosted and residual learning-based deep convolutional neural network (CBR-CNN) to address the task of NIDS. The proposed methodology integrates stacked auto-encoders (SAE) and leverages unsupervised training techniques. R. Vinayakumar et al. [5] presents a DNN model that serves to detect and classify unforeseen and unpredictable cyber-attacks in IoT networks in a timely and automatic manner. The performance was tested using many datasets. Table I presents a collection of various aforementioned studies that have employed IDS based on DL within the framework of IoT environments to detect and mitigate cyber-attacks.

III. Proposed methodology

This section is reserved for the explanation of our proposed model, which is a combination of CNN-LSTM. This architecture is designed to detect and classify both benign and malicious traffic in a new environment dataset. The proposed scheme has the following steps:

- ***Data preprocessing:*** Our initial dataset comprised a table encompassing 45 distinct features, consisting of 33 different attack instances along with benign traffic. The features were then extracted and organized into a matrix of vectors to facilitate model training. The subsequent phase involved the conversion of the dataset to two dimensions to align with the input of our model. Additionally, the numerical transformation of the labels into binary form was performed.
- ***Data splitting:*** The pre-processed selected sets of the dataset are divided into two segments: The first one is further subdivided into two subsets training and validation, for the second segment, is reserved for the final testing of the model.

  The initial segment comprises 80% for training the model and 20% for validating its performance. Significantly, the second segment pertains to the conclusive testing phase of our model, representing a distinct subset from the initial division. This partition is instrumental in reinforcing the performance evaluation of our model (Figure 1).
- ***Model architecture:*** Our proposed model was formulated employing multiple layers, including an input layer, CNN-1D layers, average pooling layers, a flattened layer, and a dense layer as shown in Figure 2, with a combination of two separate DL models, a CNN-1D model and an LSTM model.

  First, the model receives a sequence of 45 features, it's the first input layer that takes in raw network traffic data. Then, a series of convolutional layers, batch normalization, and average pooling layers are applied to the input sequence. This is done to extract features and patterns from the sequence. Afterward, dense layers with ReLU activation are used to transform the features into a higher-level representation. The outputs of the last two dense layers are passed through a dense layer with 2 units and a softmax activation function. This is the first task, which is to predict the class of the input sequence. The results of the final two dense layers are also reshaped into a 2D array comprising 16 units, subsequently traversing through multiple LSTM layers, an LSTM layer with a kernel size of 1x256 and a recurrent kernel size of 64x256. This is followed by another LSTM layer with the same configuration. Following this, the outputs of the LSTM layers traverse through a dense layer featuring 2 units and a sigmoid activation function, constituting the second task of predicting the authenticity of malicious traffic. The outcomes of both the classification and prediction tasks are concatenated along the last axis. The concatenated outputs then traverse through a concluding dense layer with 2 units and a softmax activation function, representing the

TABLE I: Summary of related works on intrusion detection. The results presented in this table were derived by opting for the most favorable outcome when authors employed various datasets or models.

Year	Authors	Focus area	Models	Datasets	Performance (%)
2021	A. Binbusayyis et al. [16]	Unsupervised DL approaches, for network intrusion detection	CAE-OCSVM	NSL-KDD, UNSW-NB-15	Acc= 94.28
2019	O. Ibitoye [17]	Analyzing adversarial attacks against DL for intrusion detection in IoT networks	FNN, SNN	BoT-IoT	Acc= 95.1
2019	Chouhan et al [18]	Improving network anomaly detection in IoT networks using a deep learning	CNN	NSL-KDD	Acc= 89.41
2019	R. Vinayakumar et al. [5]	Intrusion detection on DL/ML approaches in IoT networks	DNN	KDD Cup 1999, NSL-KDD, UNSW-NB-15, WSN-DS	Acc= 99

comprehensive output of the model. The output layer has two nodes labeled malicious and benign, indicating that the model is used for binary classification.

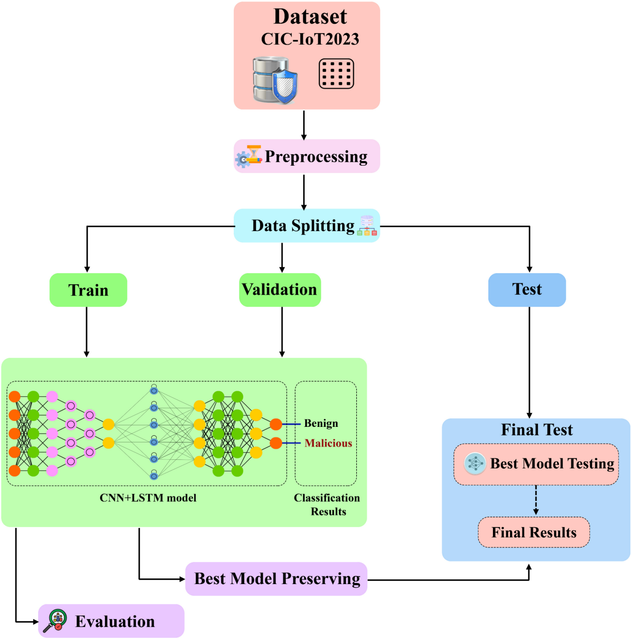

Fig. 1: The classification framework for CNN-LSTM-based IDS.

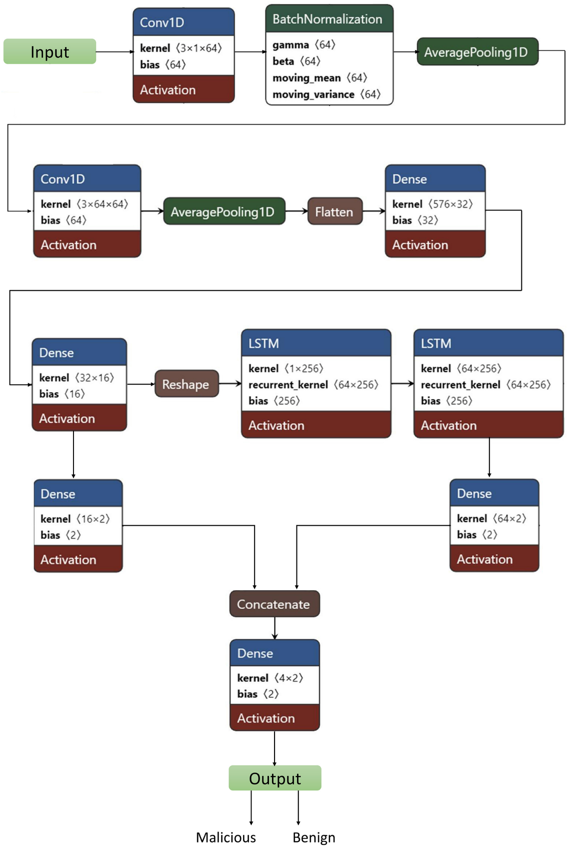

Fig. 2: CNN-LSTM proposed IDS model.

IV. Experimentation, Results and Discussion

A. Dataset exploration

In order to evaluate the performance of our DL-IDS, we have utilized the *most recent* and *extensive* Canadian institut for cybersecurity 2023 (CIC-IoT2023) dataset[1] to carry out the suggested workflow. This dataset boosts the creation of security analytics applications for actual IoTs operations, it contains seven classes with 33 attacks, namely: DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai as shown in Table II. The Mirai attack system involves a massive DDoS attack targeting IoT devices, both of these categories represent typical and emerging attack classifications within IoT network traffic. Lastly, all attacks are carried out by malicious IoT devices that are directed at other IoT devices. A total of 105 devices were intricately involved in the incident, comprising 67 IoT devices that actively participated in the attacks, while 38 Zigbee and Z-Wave devices were connected to five distinct hubs. This devices includes various categories such as smart home components, cameras, sensors, and microcontrollers. Notably, within this ensemble, certain devices assumed the role of victims, while others assumed an active role as attackers. This dataset encompasses a total of 169 files available in two distinct file formats, namely PCAP and CSV. The CSV files represent processed versions of the PCAP files. It contains almost 47 million instances with both attack and normal data with 45 different features that indicate the different types of attacks. For the hardware computation limit, we have extracted a subset of the dataset for the purpose of our study, comprising approximately 1,191,264 rows representing both

[1] https://www.unb.ca/cic/datasets/iotdataset-2023.html

TABLE II: The types of attacks in CIC-IoT2023 dataset

Classes	Attacks
DDoS	ACK fragmentation, UDP flood, SlowLoris, ICMP flood, RSTFIN flood, PSHACK flood, HTTP flood, UDP fragmentation, TCP flood, SYN flood, SynonymousIP flood
Brute force	Dictionary brute force
Spoofing	ARP spoofing, DNS spoofing
DoS	TCP flood, HTTP flood, SYN flood, UDP flood
Recon	Ping sweep, OS scan, Vulnerability scan, Port scan, Host discovery
Web-based	SQL injection, Command injection, Backdoor malware, Uploading attack, XSS, Browser hijacking
Mirai	GREIP flood, Greeth flood, UDPPlain

attack and normal traffic. For the conclusive evaluation of the optimal preservation model, the final test dataset comprises 1,175,692 rows.

B. Performance metrics

The performance of our proposed model for the detection of diverse types of attacks is quantified using standard metrics, including accuracy, precision, recall, F1-score and FPR, which are defined in [13, 19, 20]. The corresponding equations are presented below:

$$\mathrm{Acc} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} \tag{1}$$

$$\mathrm{Rc} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}, \qquad \mathrm{Pr} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{2}$$

$$\mathrm{F1-Score} = 2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}} \tag{3}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{4}$$

Where, the term ”true positive” (TP) denotes instances where the IDS accurately identifies an intrusion, while ”true negative” (TN) signifies the correct identification of normal traffic. Conversely, ”false positives” (FP) denote instances where benign traffic is mistakenly flagged as malicious, and ”false negatives” (FN) represent failures of the IDS to detect actual intrusions. A robust F1 score, which integrates precision and recall, is indicative of effective IDS performance, particularly when it reflects low rates of FP and FN [19].

C. Results

This subsection introduces the results of our proposed model. This method used a combination of CNN-LSTM for network security, the results were obtained by splitting the dataset into 80% for training and 20% for the validation. In the conducted experiment, the model underwent training using the CIC-IoT2023 dataset, encompassing both benign and malicious network traffic and the training procedure was executed on Google Colab, employing 25 epochs and the Adam optimizer.

- ***Accuracy and loss graph:*** Figure 3 shows the accuracy and loss performance of both training and validation established based on the numbers of epochs equal to 25. In Figure 3 (b), the model increases as the number of training epochs progresses. This indicates that the model is learning and enhancing its efficiency across successive epochs. The accuracy starts with a value of 98% and reaches 98.42% proving the accuracy of the model. On the other hand. In Figure 3 (a), the model decreases significantly through the number of epochs, starting approximately from 0.03 to reaching 0.0275 at the last epoch. Evidently, the CNN–LSTM model for the validation demonstrates stability and convergence compared to the training, it indicates that the model is learning effectively and not overfitting the training data.

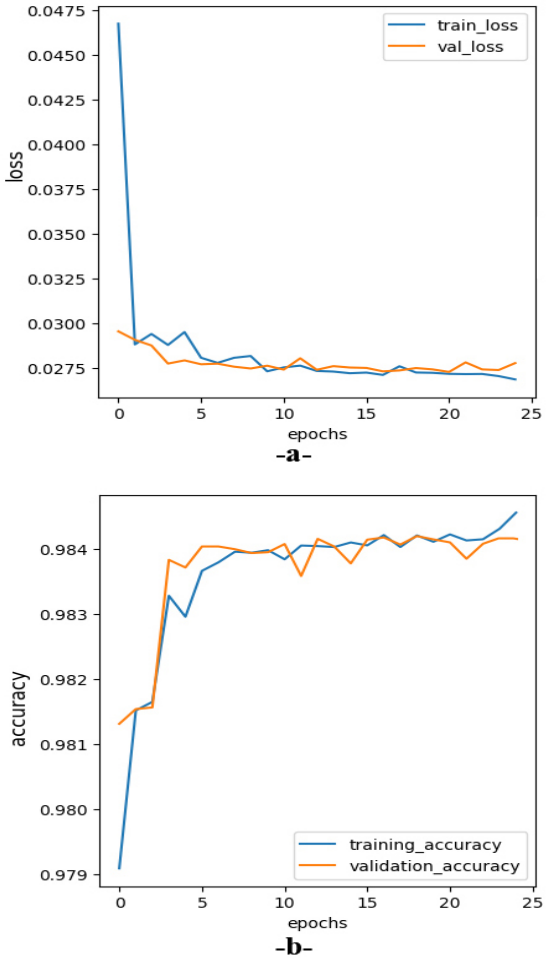

Fig. 3: Accuracy and loss model during the training phases. (a): train and validation losses. (b) training and validation accuracies.

- ***Classification Report:*** Table III presents a detailed evaluation of the binary classification of our system using a set of metrics like precision, recall, F1-score, and support. It is obvious that the model's performance changes through different classes, especially for the first and second classes (normal traffic and attacks). Concerning the first class, the precision obtained is 90% compared to other classes, this implies that the model could face difficulties in precisely classifying instances associated with the normal situation

TABLE III: Classification report.

	Precision	Recall	F1-score	Support
Normal traffic	90%	61%	73%	8321
Attacks	99%	100%	99%	229932
Accuracy			98%	238253
Macro avg	95%	80%	86%	238253
Weighted avg	98%	98%	98%	238253

category. For the same class, the recall is documented at 61%, indicating that the model might encounter difficulties in identifying all positive instances (a higher recall indicates fewer false negative results). For this particular class, the F1-score stands at 73%, which is determined by both precision and recall. The challenges encountered may stem from the inherent resemblance between certain features of benign network traffic and malicious attacks. For the other class (attacks), the F1-score reaches a value of 99%.

It is evident that the model exhibits commendable performance in accuracy, precision, recall, and F1-score. Nevertheless, it is imperative to note that while accuracy provides valuable insights, it alone may not suffice for making the final decision regarding the system's performance.

- ***FPR:*** An FPR of 9.17% is generally considered an acceptable result, signifying that only 9.17% of instances representing normal traffic were erroneously categorized as attacks. This denotes the classifier's proficiency in accurately discerning the majority of normal traffic instances, a critical factor in mitigating false alarms and enhancing the overall efficacy of the system (Determined using the confusion matrix).
- ***Confusion matrix:*** Referring to Figure 4, it is discerned that the classification performance is notably robust, with an accuracy rate of 90% for the first class (representing normal traffic), and an even higher accuracy of 99% for the second class, designated for cyberthreats. Regarding mis-classifications, a marginal 10% pertains to instances where the first class is erroneously classified as the second, whereas a mere 1% of attacks are misclassified as normal traffic which substantiates our proposition as delineated in the classification report.
- ***Receiver operating characteristics (ROC):*** ROC presented in Figure 5 indicates the commendable performance of our CNN-LSTM model in the classification of attacks, with high TPR values and low FPR values. The model has an elevated capability to discriminate between normal network traffic and instances of attacks. This is likely because the ROC curve is positioned near the left corner suggesting that the models' predictions are both accurate and precise.
- ***Generalization verification:*** Additional subsets of CICIoT2023 dataset is conducted in our study. The ensuing accuracy from this evaluation attains 98.43%, accompanied by the precision, recall, and F1-score values of 98.85%, 98.43%, and 98.57%, respectively. Remarkably, the loss metric maintains an analogous value to that observed during the training phase, registering at 0.02%, while the FPR manifested a numerical value of 9.17%. It is noteworthy that all obtained results closely align with those of the training model. Besides, we have conducted experiments utilizing an alternative dataset, namely the CICIDS2017. The primary objective is to assess the model's performance across diverse datasets and ascertain its generalization capabilities. The targeted metric for performance evaluation in this context is the same as previous tests, achieving an accuracy rate of 97.45%, loss of 0.06, precision of 97.17%, recall 97.15%, F1-score 97.07% and FPR 2.08%. This meticulous examination of the model's proficiency on a distinct dataset serves to reinforce the robustness and reliability of its predictive capabilities, contributing to a more nuanced understanding of its potential applications in real-world scenarios. The confusion matrix of the final test described related to CIC-IoT2023 and CICIDS2017 datasets are in Figure 6 (a) and (b) respectively. The results showed similar results to previous tests. However, regarding the confusion matrics of the CICIDS2017, the classifier correctly identified 98% instances and misclassified 0.02% instances as ”attacks”. Out of instances that are true ”attacks”, the classifier correctly identified 94% and misclassified 0.06% instances as ”normal traffic” which shows that the classifier performs well in identifying ”normal traffic” but has some error rate in detecting ”attacks”.

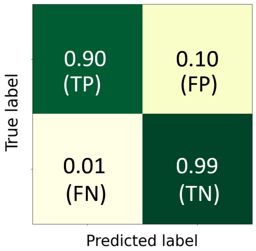

Fig. 4: Confusion matrix during the training phase.

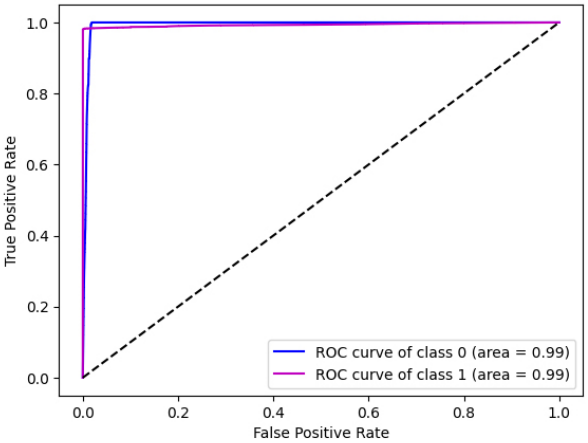

Fig. 5: ROC curve.

TABLE IV: Performance metrics of the proposed model CNN-LSTM compared to state-of-the-art for binary classification.

Work	year	Model	datasets	Accuracy (%)	Loss	Precision (%)	Recall (%)	F1-score (%)	FPR (%)
A. Kim et al. [21]	2020	CNN-LSTM	CICIDS2017 CSIC-2010	91, 93	✗	86.47 98.54	94.40 81.36	86.47 80.65	✗
S. S. S. Sugi et al. [22]	2020	LSTM	BoT-IoT	97.28	✗	✗	✗	✗	✗
M. M. Hassan et al. [23]	2020	CNN-WDLSTM	UNSW-NB15	97.17	✗	N: 98, A: 94	N: 99, A: 82	N: 98, A: 88	✗
W. Yao et al.[24]	2023	LSTM-XGboost	CICIoT2023	97.7	✗	97.4	97.4	97.4	✗
S. Abba et al. [25]	2024	RNN	CICIoT2023	96.52	✗	96.25	96.52	96.73	✗
Our	2024	CNN-LSTM	CICIoT2023 (first subset)	**98.42**	**0.0275**	**98.85**	**98.42**	**98.57**	**9.17**
			CICIoT2023 (second subset)	**98.43**	**0.0275**	**98.85**	**98.43**	**98.57**	**9.17**
			CICIDS2017	**97.46**	**0.0627**	**97.17**	**97.15**	**97.09**	**2.08**

Abbreviations: Normal (N), Abnormal (A)

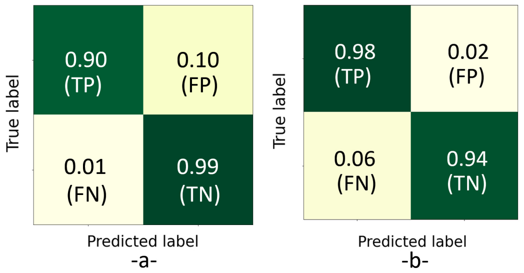

Fig. 6: Confusion matrix of the generalization verification. (a): the remaining CICIoT2023 subsets. (b): when using the CICIDS2017 dataset.

- ***Comparison with state-of-the-art:*** Table IV illustrates the outcomes of our system, encompassing a myriad of metrics for comparison with extant works employing different models (CNN-LSTM, LSTM, CNN-WDLSTM, LSTM-XGboost, and RNN) and alternative datasets. It is noteworthy that our study introduces a pioneering dataset. The tabulated data unequivocally demonstrates the superior performance of our proposed model compared to state-of-the-art models across various binary classification datasets, as evidenced by elevated accuracy, lower loss, and heightened recall and precision values.

V. Conclusion

This paper introduces a new IDS that leverages the combined strength of two robust DL models, CNN-LSTM. These models are adept at the detection and binary classification of diverse attacks as well as benign traffic. The training and validation processes of the proposed model are conducted using a specific partition of the recently introduced CICIoT2023 dataset. Subsequently, a distinct subset from this dataset is designated for the conclusive testing phase. In addition to this, to further elucidate the performance of our proposed method, a separate dataset, namely CICIDS2017, is introduced for the final testing evaluation. This methodical approach ensures a comprehensive assessment of the model's generalization across different datasets, thereby enhancing the credibility of its observed performance outcomes. The results obtained demonstrate the efficacy of the CNN-LSTM model in effectively detecting and classifying traffic into binary classification. For future works, we consider using all the CICIoT2023 datasets to achieve more results. Furthermore, integrating a Transformer, such as an attention layer, could significantly enhance the results [26–28]. This layer is adept at capturing intricate features within lengthy dependencies and sequences, thereby refining the overall performance. Given our engagement in binary classification, another next task involves the development of the model to facilitate multi-class classification, encompassing a diverse range of attacks, another prospective avenue to consider in our future work is to study the effectiveness of our proposed approach in a real-time scenario, where the proposed model will be implemented on Raspberry, FPGA, and more.

Acknowledgment

The authors acknowledge that the study was partially funded by the PRFU-A25N01UN260120230001 grant from the Algerian Ministry of Higher Education and Scientific Research.

References

[1] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in iot networks," in *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. IEEE, 2019, pp. 0452–0457.

[2] ——, "An intrusion detection system against ddos attacks in iot networks," in *2020 10th annual computing and communication workshop and conference (CCWC)*. IEEE, 2020, pp. 0562–0567.

[3] M. Haggag, M. M. Tantawy, and M. M. El-Soudani, "Implementing a deep learning model for intrusion detection on apache spark platform," *IEEE Access*, vol. 8, pp. 163 660–163 672, 2020.

[4] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT intrusion detection taxonomy, reference architecture, and analyses," *Sensors*, vol. 21, no. 19, p. 6432, 2021.

[5] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *Ieee Access*, vol. 7, pp. 41 525–41 550, 2019.

[6] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[7] H. Kheddar, Y. Himeur, and A. I. Awad, "Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 220, p. 103760, 2023.

[8] M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for iot-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, pp. 1–20, 2018.

[9] P. R. Kanna and P. Santhi, "Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features," *Knowledge-Based Systems*, vol. 226, p. 107132, 2021.

[10] Y. Habchi, Y. Himeur, H. Kheddar, A. Boukabou, S. Atalla, A. Chouchane, A. Ouamane, and W. Mansoor, "AI in thyroid cancer diagnosis: Techniques, trends, and future directions," *Systems*, vol. 11, no. 10, p. 519, 2023.

[11] H. Kheddar, D. Megias, and M. Bouzid, "Fourier magnitude-based steganography for hiding 2.4 kbps MELP secret speech," in *2018 International Conference on Applied Smart Systems (ICASS)*. IEEE, 2018, pp. 1–5.

[12] N. Djeffal, D. Addou, H. Kheddar, and S. A. Selouani, "Noise-robust speech recognition: A comparative analysis of LSTM and CNN approaches," in *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, vol. 1. IEEE, 2023, pp. 1–6.

[13] H. Kheddar, M. Hemis, Y. Himeur, D. Megías, and A. Amira, "Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions," *Neurocomputing*, p. 127528, 2024.

[14] H. Kheddar and D. Megías, "High capacity speech steganography for the G723.1 coder based on quantised line spectral pairs interpolation and CNN auto-encoding," *Applied Intelligence*, vol. 52, no. 8, pp. 9441–9459, 2022.

[15] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[16] A. Binbusayyis and T. Vaiyapuri, "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM," *Applied Intelligence*, vol. 51, no. 10, pp. 7094–7108, 2021.

[17] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *2019 IEEE global communications conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[18] N. Chouhan, A. Khan *et al.*, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Applied Soft Computing*, vol. 83, p. 105612, 2019.

[19] A. Gueriani, H. Kheddar, and A. C. Mazari, "Deep reinforcement learning for intrusion detection in IoT: A survey," in *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, vol. 1. IEEE, 2023, pp. 1–7.

[20] H. Kheddar, Y. Himeur, S. Al-Maadeed, A. Amira, and F. Bensaali, "Deep transfer learning for automatic speech recognition: Towards better generalization," *Knowledge-Based Systems*, vol. 277, p. 110851, 2023.

[21] A. Kim, M. Park, and D. H. Lee, "Ai-ids: Application of deep learning to real-time web intrusion detection," *IEEE Access*, vol. 8, pp. 70 245–70 261, 2020.

[22] S. S. S. Sugi and S. R. Ratna, "Investigation of machine learning techniques in intrusion detection system for iot network," in *2020 3rd international conference on intelligent sustainable systems (ICISS)*. IEEE, 2020, pp. 1164–1167.

[23] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," *Information Sciences*, vol. 513, pp. 386–396, 2020.

[24] W. Yao, H. Zhao, and H. Shi, "Privacy-preserving collaborative intrusion detection in edge of internet of things: A robust and efficient deep generative learning approach," *IEEE Internet of Things Journal*, 2023.

[25] S. Abbas, I. Bouazzi, S. Ojo, A. Al Hejaili, G. A. Sampedro, A. Almadhor, and M. Gregus, "Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks," *PeerJ Computer Science*, vol. 10, p. e1793, 2024.

[26] H. Kheddar, M. Hemis, and Y. Himeur, "Automatic speech recognition using advanced deep learning approaches: A survey," *Information Fusion*, p. 102422, 2024.

[27] Y. Habchi, H. Kheddar, Y. Himeur, A. Boukabou, A. Chouchane, A. Ouamane, S. Atalla, and W. Mansoor, "Machine learning and vision transformers for thyroid carcinoma diagnosis: A review," *arXiv preprint arXiv:2403.13843*, 2024.

[28] N. Djeffal, H. Kheddar, D. Addou, A. C. Mazari, and Y. Himeur, "Automatic speech recognition with BERT and CTC transformers: A review," in *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, vol. 1. IEEE, 2023, pp. 1–8.