Bidirectional LSTM Approach based Intrusion Detection for IoT Network

Yee Mon Thant
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
yeemonthant@ucsy.edu.mm

Zin Thu Thu Myint
Faculty of Information Science
University of Computer Studies,Yangon
Yangon, Myanmar
zinthuthumyint@ucsy.edu.mm

Chaw Su Htwe
Faculty of Computer Science
University of Computer Studies,Yangon
Yangon, Myanmar
chawsuhtwe@ucsy.edu.mm

***Abstract*— The Interconnected Network of Devices has gotten to be a crucial portion of our everyday lives. These networks utilize effectively to operate in various setters such as healthcare, education, transportation, industrial and financial etc. However, the connecting things networks are prone to numerous cyber-attacks in the large numbers of user and various network types environment. So, attackers have chance to attempt the malicious attacks such as unauthorized access. The solution for internet of things cyber-attacks detection is becomes Intrusion detection system (IDS). A proficient Intrusion Detection System (IDS) model is presented by comparing the evaluation results of four algorithms, namely Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and Bidirectional Long Short-Term Memory (BLSTM). Evaluation of IDS models for binary class classification used UNSW-NB15 benchmark dataset in the IoT cyber-attacks detection. The evaluation of the models' performance reveals their accuracy, precision, recall, and F1 score. The comparison result of the proposed BLSTM detection model's performance is superior that the other models.**

Keywords*— *intrusion detection system, cyber-attacks, the internet of things, deep learning

I. INTRODUCTION

Over a few years, the technology behind the Internet of Things (IoT) has advanced quickly because it has been extensively utilized in numerous application domains such as smart transportation, smart education, smart vehicles, smart farming, smart healthcare, smart industrial and city etc. In real time IoT devices, there are so many chances of attack on the IoT network [1]. Therefore, in the deployment of IoT networks, IoT security is playing a crucial part. However, IoT devices are due to constrained resources and limited computational capabilities. Thus, safeguarding the IoT network form cyber-attacks is an important case and can be realized through planning and deployment of effective security controls, one of the security control mechanism is intrusion detection system. Intrusion detection idea was introduced in [2]. An Intrusion Detection System (IDS) serves as a framework for security by monitoring network activities to differentiate between attacks and normal behavior. Three type of Intrusion Detection Systems (IDS).They are signature-based [3], anomaly based detection [4] and hybrid method [5].In this study, primary contributions summarized as follows.(i)To show BLSTM better than the other families of Recurrent Neural Networks models are applied in Intrusion Detection System on the IoT Networks.(ii)To assess the performance for families of Recurrent Neural Networks (RNNs) models on UNSW-NB15 intrusion dataset with repeated experiment.(iii)To introduce a proficient IDS model for detecting cyber-attacks with high accuracy by using deep learning approach based on Bidirectional LSTM.

This paper is structured as the following way. Part of Section II, it will discuss relevant other research to this study in both Internet of Things networks and traditional networks, focusing on deep learning methodologies. In Section III, a methodology introduced for IoT networks especially in detecting the intrusion using Deep Learning models. Section IV describes the experimental setup encompasses the intrusion dataset, preprocessing procedures, evaluation parameters, assessment metrics and the analysis of obtained experimental results. Subsequently, paper concludes in Section V.

II. RELEATED WORK

This section offers a compilation of prior research studies focusing on intrusion detection work for various machine learning and deep learning techniques. In [6] authors has presented an intrusion detection mechanism for binary classification that employs LSTM and RNN with UNDW-NB15 benchmark dataset. In the performance evaluation phase, LSTM's accuracy 99% outperformed than RNN. Authors [7], introduced an anomaly-based intrusion detection approach employing LSTM and GRU, along with Convolutional Neural Networks (CNN) applied to the NSL-KDD dataset. Their findings indicate that CNN is better than RNN with an accuracy surpassing 97%. However, their work acknowledges limitations related to computational resources and long training times for the proposed model. According [8] The authors introduced a method to detect DoS attacks utilizing Multilayer Perceptron(MLP), Random Forests(RF), Support Vector Machine(SVM), and Convolutional Neural Networks(CNN). Random forests and CNN yielded the highest accuracy results, and they employed the BoT-IoT dataset for model evaluation. In [9] authors employed the CIDDS dataset for implementing a network intrusion detection system using LSTM. They compared their proposed method with MLP, Naïve Bayes, and SVM. Their approach achieved a detection accuracy exceeding 85%, outperforming other machine learning methods.

III. METHODOLOGY

A. Intrusion Detection in Deep Learning

In this research, various intrusion detection systems are discussed grounded in Deep Learning methodologies. Fig. 1 illustrates the ten deep learning techniques employed in detecting cyber-attacks, they are, Convolutional Neural Network, Deep Migration Learning, Deep Auto-encoder, Deep Belief Network and Restricted Boltzmann Machine, Recurrent Neural Network, Feed Forward Deep Neural Network.

B. Bidirectional Long Short Term Memory

The Bidirectional LSTM (BLSTM) extends the concept of Bidirectional RNN (BRNN) [10] operating on input sequences in both the forward and reverse directions, utilizing two separate hidden layers. Bidirectional LSTM can learn faster and more propagate the information that it adds additional information the network. The Bidirectional LSTM comprises two parallel LSTM layers: one for the forward pass and another for the backward pass. The forward pass progresses along a positive time dimension, whereas the backward pass moves along a negative time dimension. The outputs from both LSTM layers are combined using concatenation [11].

Fig. 1. Deep learning based Intrusion Detection Techniques

IV. EXPERIMENT

A. Experiment Enviroment

The experiments were conducted using a Windows 10 Pro 64-bit operating system, Core(TM) i7-7500U CPU, 8.00 GB of memory, and without the utilization of a Graphics Processing Unit (GPU). The research work effectively employed with Keras libraries and TensorFlow framework to successfully implement RNN models on Python programming language. For tasks such as data manipulation, cleansing, and feature engineering, the Pandas and NumPy frameworks were utilized. Data visualization was achieved using the Matplotlib and Seaborn frameworks, while the Scikit-learn framework facilitated data analysis.

B. UNSW-NB15 Intrusion Dataset

Australian Centre's Cyber Security Lab created it in 2015. Comprising 49 features, this dataset encompasses a wide range of both attack and normal activities, featuring labeled data across over 2,000,000 records [12]. The selection of the UNSW-NB15 dataset for our research was motivated by its encompassment of contemporary attack patterns, including IoT attacks, and its binary classification of attack and normal classes.

C. Data Preprocessing

In this research, applied UNSW-NB15 dataset, which originally features consists of 49 [13]. Building upon prior work [14], where the author to get the better performance for IDS models introduced the five attributes. To prepare the data for analysis, we needed to change categorical data into a numerical format by using LabelEncoder. Subsequently, we applied normalizing techniques to standardize the input data into a consistent format. Final step in data preprocessing involved data reshaping, where we adjusted features to fit that the data representation was well-suited for deep learning models.

D. Evalution Parameter

BLSTM model is developed with an input layer comprising 5 neurons, a hidden layer housing 4 BLSTM memory units, and an output layer containing a single neuron responsible for generating a binary output indicating attack or normal traffic. To facilitate the malicious vs. benign classification task, binary cross entropy is employed as the loss function. Each experiment is conducted by turning the parameters, four types of epochs (5, 10, 20, and 30), different optimizers (adam), and batch sizes (32). The experimental outcomes revealed that a batch size of 32 consistently yielded superior performance results.

TABLE I. DATA DISTRIBUTION IN UNSW-NB15 DATASET

Attacks Type	Train	Test
Backdoor	1746	583
Analysis	2000	677
Exploits	33393	11132
Dos	12264	4089
Fuzzers	18184	6062
Generic	40000	18871
Reconnaissance	10491	3496
Shellcode	1133	378
Worms	130	44
Normal	56000	37000
Total	175341	82332

E. Evaluation Metrics

In this section, the assessment of classification model performance in deep learning research employs metrics. Table II description are TP=True positives, TN =True negatives, FP=False positives, FN =False negatives.

TABLE II. DEFINITION OF EVALUATION METRICS

Accuracy(A)	$\frac{TP + TN}{TP + TN + FP + FN}$
Precision(P)	$\frac{TP}{TP + FP}$
Recall(R)	$\frac{TP}{TP + FN}$
F1 measure	$\frac{2 * (P * R)}{(P + R)}$

F. Experiment Result

After implementing the deep learning models including Simple RNN, LSTM, GRU, and BLSTM, we conducted multiple iterations of experiments on these models to achieve a satisfactory outcome, as illustrated in Table III.

TABLE III. EVALUATION RESULT

Models	Accuracy	Precision	Recall	F1score	Epoch
RNN	81.18%	75.90%	96.42%	84.94%	30
LSTM	85.95%	80.97%	97.37%	88.41%	30
GRU	95.91%	93.36%	99.65%	96.40%	30
BLSTM	98.12%	97.43%	99.20%	98.31%	30

In experimentation, proposed model is explored different learning rates, utilized a batch size of 32, and various epochs to assess the performance of detection models for binary classification. Fig.2 illustrates the BLSTM model accuracy for set of train and test across different epochs.

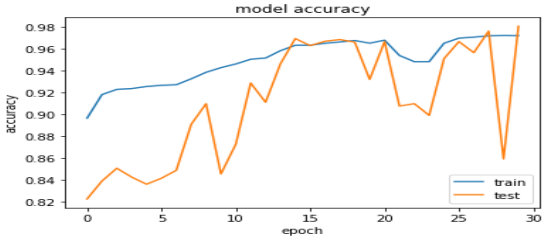


Fig. 2. Accuracy of BLSTM Model over Epochs

In Fig. 3 shown for BLSTM model's loss is depicted with plot figure. In Fig.4 and Fig.5 display the confusion matrix for binary classification of deep learning models, respectively.

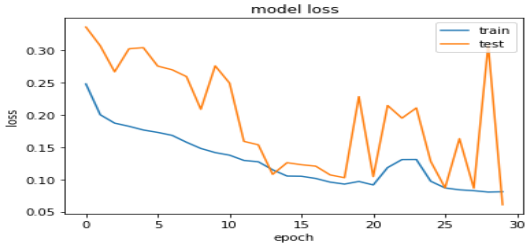
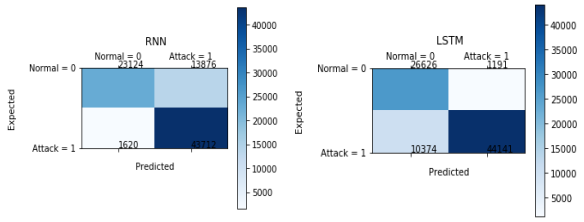


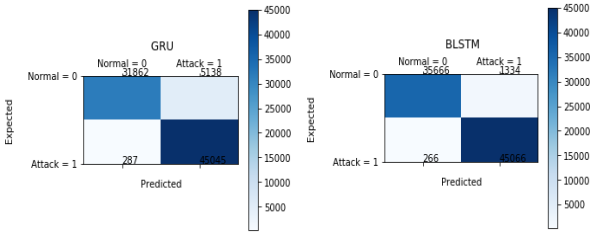
Fig. 3. Loss of BLSTM Model over Epochs



(a) (b)

Fig. 4. Confusion matrix for (a) RNN and (b) LSTM

In Fig. 6 demonstrates the performance for families of RNN models in epochs 30 with batch size 32.



(c) (d)

Fig. 5. Confusion matrix for (c) GRU and (d) BLSTM

According to the evaluation results of these four models, BLSTM achieves the highest average value of accuracy 98.12% and precision 97.43%metric. GRU performs best in terms of recall by achieving 99.20% performance measure . BLSM is highest and lowest is RNN for f1 score of model performance. So, BLSTM model is outperformed GRU, LSTM and RNN in IoT cyber-attack detection.

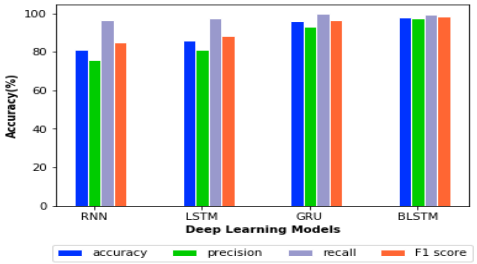


Fig. 6. Performance Evaluation for Deep Learning Models

V. Conclusion

In this investigation, a comparative analysis of intrusion detection is studied by using four distinct methodologies, including Simple RNN, LSTM, GRU and BLSTM. Accordingly to the comparative studies of these models for IoT cyber-attacks detection, BLSTM is superior to the other models in term of accuracy over 98% with lowest training and testing time(seven minutes, twelve seconds for training and one seconds for testing). The study is explored a comparison for performance evaluations in conventional machine learning and deep learning algorithms with IoT realistic traffic based dataset . As a potential avenue for future research, employing a robust feature selection method could be explored to enhance the detection performance for IoT cyber-attacks. Moreover, proposed BLSTM RNN-IDS model will support to improve for the IoT technologies in future research studies.

References

[1] A. Parashar and S. Rishishwar, "Security challanges In IoT," in 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India: IEEE, Feb. 2017, pp. 446–449. doi: 10.1109/AEEICB.2017.7972351.

[2] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," p. 56.

[3] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France: IEEE, Oct. 2013, pp. 600–607. doi: 10.1109/WiMOB.2013.6673419.

[4] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, and M.-C. Hsieh, "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN," in Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Y.-M. Huang, H.-C. Chao, D.-J. Deng, and J. J. Park, Eds., in Lecture Notes in Electrical Engineering, vol. 260. Dordrecht: Springer Netherlands, 2014, pp. 1205–1213. doi: 10.1007/978-94-007-7262-5_137.

[5] J. Krimmling and S. Peter, "Integration and evaluation of intrusion detection for CoAP in smart city applications," in 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA: IEEE, Oct. 2014, pp. 73–78. doi: 10.1109/CNS.2014.6997468.

[6] Y. M. Thant, M. M. Su Thwin, and C. S. Htwe, "IoT Network Intrusion Detection Using Long Short-Term Memory Recurrent Neural Network," in 2023 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar: IEEE, Feb. 2023, pp. 334–339. doi: 10.1109/ICCA51723.2023.10182005.

[7] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, "Using Deep Learning Techniques for Network Intrusion Detection," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar: IEEE, Feb. 2020, pp. 171–176. doi: 10.1109/ICIoT48696.2020.9089524.

[8] B. Susilo and R. F. Sari, "Intrusion Detection in IoT Networks Using Deep Learning Algorithm," Information, vol. 11, no. 5, p. 279, May 2020, doi: 10.3390/info11050279.

[9] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for Anomaly-Based Network Intrusion Detection," in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW: IEEE, Nov. 2018, pp. 1–3. doi: 10.1109/ATNAC.2018.8615300.

[10] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," IEEE Trans. Signal Process., vol. 45, no. 11, pp. 2673–2681, Nov. 1997, doi: 10.1109/78.650093.

[11] A. Graves and J. Schmidhuber, "Framewise phoneme classification with bidirectional LSTM and other neural network architectures," Neural Networks, vol. 18, no. 5–6, pp. 602–610, Jul. 2005, doi: 10.1016/j.neunet.2005.06.042.

[12] "UNSW Canberra." https://www.unsw.adfa.edu.au/ (accessed Jun. 30, 2020).

[13] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia: IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.

[14] T. Janarthanan and S. Zargari, "Feature selection in UNSW-NB15 and KDDCUP'99 datasets," in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, United Kingdom: IEEE, Jun. 2017, pp. 1881–1886. doi: 10.1109/ISIE.2017.8001537.