Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach

Tooba Hasan, Jahanzaib Malik, Iram Bibi, Wali Ullah Khan, Member, IEEE, Fahd N. Al-Wesabi, Kapal Dev, Senior Member, IEEE, and Gaojian Huang, Member, IEEE

Abstract—Industrial Internet of Things (IIoT) formation of a richer ecosystem of intelligent, interconnected devices while enabling new levels of digital innovation has transformed and revolutionized global manufacturing and industry 4.0. Conversely, the general distributed nature of IIoT, Industrial 5G, underlying IoT sensing devices, IT/OT convergence, Edge Computing, and Time Sensitive Networking makes it an impressive and potential target for cyber-attackers. Multi-variant persistent and sophisticated bot attacks are considered catastrophic for connected IIoTs. Besides, botnet attack detection is highly complex and decisive. Thus, efficient and timely detection of IIoT botnets is a dire need of the day. We propose a hybrid intelligent Deep Learning (DL) mechanism to secure IIoT infrastructure from lethal and sophisticated multi-variant botnet attacks. The proposed mechanism has been rigorously evaluated with the latest dataset, standard and extended performance evaluation metrics, and current DL benchmark algorithms. Besides, cross-validation of our results is also performed to show overall performance clearly. The proposed mechanisms outperform accurately identifying multi-variant sophisticated bot attacks by achieving a 99.94% detection rate. Besides, our proposed technique attains 0.066 (ms) time, which also shows promising results in terms of speed efficiency.

Index Terms—Deep learning (DL), IIoT botnet detection, Internet-of-thing (IoT), network security, time efficient algorithms.

I. INTRODUCTION

NO DOUBT, the Industrial Internet of Things (IIoT) is exponentially growing to make an incredible digital landscape and thus becoming part and parcel of our daily lives [1]–[3]. The IIoT ecosystems are contributing to smart agriculture, e-health, e-government, smart cities, e-logistics, home automation, industrial systems, e-wearables, and transportation [4], [5]. The shift from traditional network to IIoTs have revolutionized the global world. Smart devices are intelligent, interconnected, and location-aware while generating big IIoT data that is the new gold mine to be subsequently used for various behavioral analytic, varied computational intelligence [6] and decision-making [7], [8]. In recent statistical report, approximately 75 billion IoT smart devices are expected to be connected by the end of 2025 [9], [10].

However, the diverse landscape of IoT protocols, heterogeneity in transmission of data and devices, resource constraints, and one time embedded deployment of IoT [11], [12] devices; make them more insecure towards prevalent cyber threats and attacks [13]. The diverse attacks, including phishing, denial of service (DoS), man-in-the-middle (MITM), and Botnet are executed on victimized IoT devices for information theft, data loss, and full compromise of the entire system [14]. Among the attacks mentioned above, Botnets are considered the most sophisticated and lethal attack used to paralyze network as a whole [15]. Botnet is purposefully crafted malware that possesses the capability to propagate over the network and intelligent devices through exploiting vulnerabilities, in turn leveraging remote access to cyber adversaries [16], [17].

For the security of heterogeneous IIoT devices and generated traffic [18], existing solutions for the identification of cyber threats and attacks predominantly focused on pre-defined signature vectors for pattern matching, which is also known as signature-based detection. However, this approach proves to be insufficient in the digital infrastructure of IoT as it requires continuous updates of signatures for the latest prevalent threats. Therefore, it is incapable of detecting zero-day threats, attacks, and vulnerabilities due to its dynamic and heterogeneous nature [19]. The DL-driven intelligence-based solutions can empower zero-day threat detection and are considered adaptive, resilient, reliable, and efficient for botnet identification in IIoT [20]. Therefore, in this work, we propose a hybrid novel DL-Driven intelligent threat detection mechanism to combat sophisticated Botnet threats and attacks in IIoT environment, as shown in Fig. 1.
Contributions: The core contributions of our work are as follows:

- An efficient, scalable and flexible AI-enabled hybrid model for effective identification of lethal IIoT-based multi-variant attacks employing Long short-term memory-Deep Neural Network (LSTM-DNN).
- For multi-class attack classification, well known IoT dataset (i.e., N_BaIoT) has been utilized.
- The standard performance parameters are practiced to compute the actual potential of the proposed technique to provide a thorough evaluation.
- We have also compared our proposed method to other hybrid algorithms and current DL benchmarks. Our devised mechanism outperforms detection accuracy with a minor trade-off in time efficiency.
- In addition, a 10-fold cross-validation technique is used to ensure that the results are unbiased.

Structure: The rest of the work is organized as follows. The background and related work are discussed in Section II. Section III defines the suggested methodology, including a description of the framework, dataset and initialization, DL architectures, experimental setup, and assessment metrics. While Results and discussion are presented in Section IV. The paper concludes with Section V, which discusses future road maps.

II. BACKGROUND AND RELATED WORK

With the rise of emerging AI-empowered technology, deep learning architectures draw the wide attention of many academic and industrial researches in the field of information security, computer vision, sound and text analysis, and pattern recognition because of their self-learning ability which helps to accomplish high classification accuracy in complex environments [21]. Table I outlines the current literature detailing attacks, dataset, strengths, limitations, and future directions. For cyber threat and attack detection, [22] shows a DL-based mechanism using LSTM for detecting botnet. The dataset is collected by examining the network packets of Technical University called Czech. The algorithm gets 99.90% detection rate. The authors in [23], demonstrate a framework for identifying the botnet by analyzing the packets using Bidirectional LSTM. The self-generated Mirai and benign instances dataset has been considered and acquired 96% accuracy. Meanwhile, [24] observe the network flow by deploying the CNN and RNN in contradiction. The CTU-13 and ISOT dataset execute that holds the signature of normal as well as attack records. The proposed system gained detection percentage of 99.3%. In [25], the exploitation by enhancing the power of LSTM has been performed to detect the attack. The scheme gain the accuracy of 98%; whereas the dataset gathered from
| Ref | Attack / Mechanism | Dataset / Methodology | Strength | Limitations | Future Work |
|-----|-------------------|-----------------------|----------|-------------|-------------|
| [09] | SMTP, SPAM, HTTP / LSTM | CTU-13 / Provide an analysis of the viability of RNN to detect the behavoir of network traffic | Analysis network behaviour. | LSTM has failed in detecting most of the HTTP and HTTPS traffic due to imbalance labels | More experiments must be conducted, analyze detail’s for possible solutions |
| [10] | UDP, ACK DNS / Bidirectional LSTM | Mini botnet dataset and Self-generated normal data / DL models in conjunction with Word Embedding | Packet-level detection in IoTs and network | The bidirectional approach causes computational overhead | Explore different ways to identify Botnets. |
| [11] | IRC, DDoS, SPAM, PS, HTTP, CF, P2P / LSTM, CNN | CTU-13, ISOT / Botnet detection by modeling network traffic traces b/w communication endpoints represents traffic in graph. | Inspect the statistical based network flow feature | Time complexity | Not defined |
| [12] | TCP, HTTP, UDP / LSTM | Cresci, and collaborators / Exploit the content and metadata through LSTM, use synthetic minority oversampling on data | Deep analysis showed that LSTM could detect Botnet behaviors that were significantly different from Normal. | High processing power | Not defined |
| [13] | Mirai Botnet / LSTM, RNN, CNN, CNN-LSTM | Data collected from Alexa and 17-JGA / Detect and classify pseudo-random domain names using DL. | Detect and classify the domain names to specific malware family by domain generation algorithms | Lack in presenting inner mechanics of DL model that is important for real-time deployment. | A comprehensive study is required for complex architectures |
| [14] | N/A / CNN-RNN | N/A Deep Learning | Discuss the importance of deep learning in different scenarios i.e image, text, audio, and video | No implementation | Not defined |
| [15] | DoS, Probe, Remote or local attack, Reconnaissance / Restricted Boltzmann Machines (RBM) | KDD99 / Provide a secure framework of IoT based on SDN for intrusion detection. | Provide scalable, resilient, and security in IoT | Low detection accuracy rate. | Analysis is required in the practical implementation to improve the detection rate. |
| [16] | Botnet Traffic / Deep learning-based Autoencoder, CNN | ISCX / Provide deep learning-based Botnet traffic analyzer to detect the botnet. | Identify the correlation between original features and extract the new feature on every autoencoder layer. | The detection accuracy is not optimal for botnet identification. | Use LSTM that improves the detection accuracy of botnet traffic. |
| [17] | Botnet Traffic / MLP’s Deep learning algorithm | CTU-13, ISOT / extracts features from the traffic of each session. It segregates the infected machine | Infected machine isolates by using FW and VLAN using SDN | Experiment did not conduct on an infected terminal that was infected by bots. | Need to explore whether network isolation is performed on the infected host or not. |
| [18] | N/A / SDN-IoT framework | N/A / Present a comprehensive survey on technology provide security on IoT | Identify some research direction on security for SDN-IoT and SDN for IoT | No implementation | Not defined |
| [19] | DDoS / Decision Tree | ISOT, ISCX2012/Flow based feature employed for botnet detection using machine learning | Review flow based feature techniques and examine their applicability to detect the botnet | Detection accuracy is 99% which is not good. | Combine flow level features with pair level features or conversational level features to improve detection rate. |
| [20] | IRC Botnet/Naive Bayes, J48 and Bayesian | Dataset from Dartmouth wireless campus network/Identify command and control traffic of IRC botnets | Label the IRC traffic as botnet and non botnet by telltale | Lack in demonstrating the accuracy. The value of FPR and FNR are presented | Analyze the collection of various IoT devices and their communication technolgies |
| [21] | DDoS/Random Forest | Self Generated dataset | Extract the features that identify the IoT devices types as malicious and benign from the white list | Need to enhance the dataset that identifies the malicious devices with well efficient detection accuracy rate | Analyze the collection of various IoT devices and their communication technologies |
| [23] | Mirai Attack/GRU | Collected through real-time deployment/D-IoT self-automated learning system for detecting the compromised IoT devices | Gated Recurrent Unit performs well in detecting the cyber attack | Dataset should be more enough to detect the attack on time with efficient detection rate | Not defined |
| [24] | DOS, Cache Poisoning, Malicious Packet and Botnet/Passive Aggressive Classifier | KDD99 | The duplicated and redundant leads to poor classification | Need to utilized updated dataset | To broaden the investigation for other malware classifications |
the Cresci and collaborators. The authors in [26], proposed DL techniques by practicing on LSTM, RNN and CNN for detection of malicious domain. The dataset comprised of normal samples gathered from OPEN-DNS and Alexa. However, the malevolent records are collected from 17-DGA. The identification rate of the proposed scheme is 90%.

The authors in [27] implemented an intrusion detection to safeguard the IoT by deploying SDN and depict the testing rate of 95%. The KDD99 dataset considers attack detection (i.e., DoS, Login, and Probe) with Restricted Boltzmann Machine (RBM). Consequently, [28] presented a botnet traffic analyzer based Convolutional Neural Network (CNN) and Auto-encoder and achieved 91% rate. The Botnet Traffic Shark (BoT-Shark) uses for network arrangements, and the utilized data is ISCX. In [29], the authors proposed an approach that prevents the detection of host after infection by using deep learning in SDN. The ISOT and CTU-13 dataset has been considered for implementation. The detection accuracy of the work is 99.2% by considering MLP. Moreover, [31] proposed the varied attack detection framework in IoT through GRU/LSTM with the NSLKDD dataset. The proposed model attained an accuracy of 87.9% and compared the traditional schemes. The authors in [30], developed an application for providing security policies and access control in various IoTs using the open-flow interface. The research also discussed the significant security vulnerabilities in IoT networks and the potential of SDN for providing security in IoT. In [31], the authors proposed a network flow capability scheme to identify botnet attacks. ML algorithm called Decision Tree Algorithm (DT) is employed to deal with the attack. ISCX2012 and ISO8 dataset has been utilized and gets 99% rate. The author, in [32], used ML models such as Naïve Bayes (NB), J48, and Bayesian to detect the botnet. The detection rate of FN, FPR is defined as 1020 % and 3040 %, respectively. The dataset is collected from the Dartmouth campus wireless network and tagged via detectors. In [33], the authors detect the DDoS attack by considering the Random Forest algorithm and achieve 99% percentage. The self-generated dataset is Wire-shark through port mirroring on the switch to catch network traffic data. The author in [34] presents DIOT, a distributed self-learning system for efficiently detecting compromised IoT devices. The proposed method detects devices compromised by the Mirai attack using Gated Recurrent Unit (GRU). Data is collected from implementation settings in the lab and in the real world. The proposed framework achieved a detection rate of 95.6%. In [35], the author shows the system that can memorize the behavior of harmful network activities, detect and prevent different types of Botnet infections. The devised approach achieved a detection accuracy of 98% employing the KDD99 dataset. In the [20], the author proposed the IoT-based paper that considered the power of DL based algorithm (i.e. LSTM) for the detection of botnet attack. The paper utilized the NIoT 2018 dataset, which contained varied IoT devices’ data and got a detection rate of 99.90%.

In this section, the algorithms used in this paper are described.

A. Long-Short-Term Memory (LSTM)

The most advanced variant of the Recurrent Neural Network (RNN) family is LSTM which addresses the problem of limited learning in simple RNN. RNN suffered from the problem of learning long sequences as RNN has short term memory. LSTM model was initially proposed to address the learning of longer sequences in data to solve these issues. LSTM has a similar control flow as an RNN for long-term memory which bridges the time gap to solve the gradient vanishing problem. Recurrent neural network (RNN) utilized fewer data pre-processing efforts by learning from past sequences through back-propagation [40]. The back-propagation eliminates error signals that make the execution of the system poorer. The main concept of LSTM is based on cell state, activation functions, and gates. The cell state act as a communicator which transfers meaningful information to the next cell. It acts as a “memory” of the current LSTM cell. The cell state carries important information all through the process. As the cell state goes on, information get’s added or taken out from the cell state through the memory gate. The gate can learn what information is relevant and is necessary to keep or forget during training.

B. Deep Neural Network (DNN)

Deep Neural Network is a neural network designed to simulate the activities of the human brain to recognize patterns [37]. DNN architecture has an input layer, output layer, and hidden layer. Each layer in DNN is comprised of neurons. In contrast, these neurons take information and pass on to the next layer till the output layer by performing addition and multiplication operation on weights [41]. The computation in DNN is performed on neurons which is the single unit for the multi-step procedure of pattern recognition [38]. The node performs computation on input data and weights and passes the information to the next layer until it reaches the output layer. By following the subsequent occurrence, the framework would be fit for improving the analysis of the botnet and perhaps leading defensive measures.

IV. METHODOLOGY

The proposed hybrid Deep Learning (DL) based attack detection framework for IoT infrastructure is presented in this section. The proposed model aims to secure IoT devices from varied attacks. The initial step is to utilize a state-of-the-art updated dataset for thorough experimentation. Moreover,
the sequence diagram of IIoT presented in Fig. 3 shows the communication process between layers. Further, we have performed pre-processing of the dataset, including removing data redundancy, data cleansing, transformation, visualization, and feature engineering. After the pre-processing aspect, the data is practiced to be entered into classifiers to identify multiple IIoT attacks.

A. Dataset

For the training of the proposed algorithm, we considered the recent updated N_BaIoT [42] IoT dataset. The dataset consists of benign and latest IoT malware (i.e., Gafgyt, Mirai) that are two malware from Botnet family specifically designed to target IoT devices. The dataset contains network traces from execution of Gafgyt and Mirai on 9 different IoT devices (i.e., Doorbells, Thermostat, Baby Monitor, Security Camera’s and Webcam). The complete distribution of N_BaIoT dataset for proposed approach is outlined in Table III.

B. Pre-Processing

The pre-processing of N_BaIoT is performed to improve the effectiveness and performance of our proposed hybrid deep learning methodology. Initially, we verified data integrity by scanning and removing missing nan and infinity values from the dataset. Moreover, To enhance the learning process, we used MinMaxScaler to normalize data between 0 and 1. We also performed One-hot Encoding (OHE) on target labels to train the deep learning algorithm.

The steps followed for model construction are also depicted in Fig. 7 as a flow chart.

| Algorithm | Layers | Neurons/Kernal | AF/ LF | Optimizer | Epochs | Batch-size |
|-----------|--------|---------------|--------|-----------|--------|------------|
| **DNN-LSTM** | DNN Layer (3) | (450, 300, 50) | RelU/CC-E | - | Adam | 5 | 32 |
| LSTM Layer(3) | (450, 300, 50) | - | - | | | |
| Merge Layer | 40 | - | - | | | |
| Dense Layer | 15 | - | - | | | |
| Output Layer | 3 | softmax | | | | |
| **CNN2D-LSTM** | Conv Layer (3) | (400, 300, 50) | RelU/CC-E | - | Adam | 5 | 32 |
| LSTM Layer(3) | (400, 300, 50) | - | - | | | |
| Merge Layer | 40 | - | - | | | |
| Dense Layer | 15 | - | - | | | |
| Output Layer | 3 | softmax | | | | |
| **DNN-DNN** | DNN Layer (3) | (400, 300, 50) | RelU/CC-E | - | Adam | 5 | 32 |
| DNN Layer (3) | (400, 300, 50) | - | - | | | |
| Merge Layer | 40 | - | - | | | |
| Dense Layer | 15 | - | - | | | |
| Output Layer | 3 | softmax | | | | |
| **CNN2D-CNN3D** | Conv Layer (3) | (400, 300, 50) | RelU/CC-E | - | Adam | 5 | 32 |
| Conv Layer(3) | (400, 300, 50) | - | - | | | |
| Merge Layer | 40 | - | - | | | |
| Dense Layer | 15 | - | - | | | |
| Output Layer | 3 | softmax | | | | |

AF = Activation Function, LF = Loss Function, CC-E = categorical cross-entropy.

Algorithm 1: 10 Fold for proposed algorithm (DNN-LSTM).

Require: Training set S, Testing set T, DNN-layers D, LSTM-layers L, Classifier1 C1, Classifier2 C2, Dense-layer E, N-Folds N, Epochs P, Batch-Size B, Weights G

Ensure: N-Fold Validation & Save Output

1: function N-Fold Validation()
2: for Fold = 1, 2, ..., N do
3: Classifier1 C1 add DNN Layer
4: Classifier2 C2 add LSTM Layer
5: Merge-out w.r.t C1 and C2
6: Dense Layer
7: for Epoch = 1, 2, ..., P do
8: for Sample = 1, 2, ..., S do
9: Train the Model w.r.t B from S
10: Calculate Loss w.r.t B
11: if PredictFalse then
12: Update G
13: end if
14: end for
15: end for
16: Save Output for N
17: end for
18: end Function

C. Proposed Framework

The proposed deep learning framework is intended to detect botnet attacks in IIoT by combining Long short-term memory (LSTM) and Deep Neural networks (DNN) to design a hybrid model. Hybrid models are highly efficient to achieve high detection accuracy in less time [43]. Subsequently, to simultaneously benefit from various deep learning classifiers, we have considered LSTM and DNN to
improve overall results. Consequently, in the proposed hybrid framework, LSTM is considered due to its ability to achieve effective learning for longer sequences of data. As IIoT devices generate massive surge data quickly, DNN is used to enhance the algorithm’s predictive power by improving speed efficiency. The detailed arrangement of our proposed hybrid architecture is elaborated in Table II, while the modeling phases of our proposed model are portrayed in Fig. 2.

Fig. 2. Proposed simplified view of Hybrid framework (DNN-LSTM).

Fig. 3. Sequence diagram of IIoT with proposed monitoring system.

D. Experimental Setup

This section provides the experimentation and evaluation of our proposed attack detection and performance mechanism. The experimental setup comprises of tensor-flow framework [44]. Python library named Keras [45] is also utilized to design and implement the proposed hybrid model for botnet detection. The performance evaluation of the proposed system is conducted using the sklearn library. The details of our experimental setup are presented in Table IV.
E. Evaluation Parameters

Various diverse evaluation parameters are used to evaluate the capabilities of the proposed hybrid deep learning algorithm. The primary classification of true positive, true negative, false positive and false negative is presented through a confusion matrix. In contrast, other basic evaluation metrics like accuracy, precision, recall, and F1-score values are derived from confusion metrics. The mathematical formulas and basic description is defined below.

Accuracy: Accuracy shows the numbers of correctly classify records. Accuracy is the primary metric to determines the performance of the algorithm.

\[ \text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \] (1)

Precision: Precision is also called the Positive Predictive Value (PPV) which shows the closeness of two or more values with each other.

\[ \text{Precision} = \frac{TP}{TP + FP} \] (2)

Recall: Recall known as True Positive Rate (TPR) referred as the percentage of total correctly classified values by algorithm.

\[ \text{Recall} = \frac{TP}{TP + FN} \] (3)

F1-Score: It is a measure of test accuracy using the average between precision and recall.

\[ F - \text{score} = \frac{2 \times TP}{2 \times TP + FP + FN} \] (4)

ROC Curve: The ROC curve plots the TP and FP rates in 2D and illustrates the system’s detection ability. The overall performance of the system is the area under the curve. The ROC curve of various algorithms are depicted in Fig. 6.

V. RESULTS AND DISCUSSION

We conducted a rigorous evaluation based on multiple parameters to fully demonstrate the performance of our proposed detection framework. Besides, we carried out 10-fold cross validation shown in Fig. 4. The confusion matrix presents in Fig. 5 to show the overall performance of our proposed hybrid DL technique.

The proposed algorithms gain the detection rate are shown in Fig. 8. Our hybrid DNN-LSTM performed best with 99.94% detection accuracy compare to contemporary algorithms. The Hybrid model CNN2D-LSTM and DNN-DNN reached 99.93% detection accuracy; Whereas, the hybrid model CNN2D-CNN3D attain 99.92% detection accuracy.

An algorithm with low prediction values of FPR, FNR, FDR, and FOR is considered an effective and efficient model. False Positive Rate (FPR) shows the correlation between known attack samples precisely classified from total attack records. False Discovery Rate (FDR) is a statistical approach used in testing to correct for multiple contrasts. False Omission Rate (FOR) is the ratio of benign records that were incorrectly identified. The hybrid model DNN-LSTM achieved FPR, FDR, FNR, and FOR of 0.0051%, 0.0071%, 0.0031%, and 0.0039% respectively, as shown in Fig. 9. Hybrid CNN2D-LSTM achieved 0.0048%, 0.0013%, 0.0013%, and 0.0051% for FPR, FDR, FNR and FOR respectively. On the contrary, the hybrid model DNN-DNN achieved 0.0045%, 0.0013%, 0.0012%, and 0.0047% for FPR, FDR, FNR, and FOR respectively. Consequently, the hybrid model achieved TNR, MCC, and NPV of 99.96%, 99.91%, and 99.95% respectively.

We have also calculated the extended parameters, i.e., True Negative Rate (TNR), Matthews correlation coefficient (MCC), and negative predictive value (NPV), as depicted in Fig. 10. The TNR, MCC, and NPV of the proposed Hybrid DNN-LSTM model are 99.96%, 99.91%, and 99.95%. The Hybrid model CNN2D-LSTM and DNN-DNN attains TNR, MCC, and NPV of 99.95%, 99.88%, 99.94%, and 99.95%, 99.89%, and 99.95% respectively.

The proposed algorithm’s time and space complexity are significant because they measure the technique’s inherent demand for computation and storage complexity regarding the ability to resolve the problem. The time complexity of proposed algorithms is manifest in Fig. 11. Hybrid model DNN-LSTM model took 0.066 (milliseconds); whereas the
testing time of hybrid CNN2D-LSTM and DNN-DNN algorithms were 0.061 and 0.068 (milliseconds) respectively. Consequently, the testing time of the hybrid CNN2D-CNN3D model is 0.067 (milliseconds).

We compared our proposed hybrid DNN-LSTM model with current advanced algorithms for detailed analysis. Table V compares benchmark algorithms based on the proposed algorithm, dataset, evaluation parameters, and detection time. The table represents that our proposed algorithm is highly efficient in detection accuracy and speed efficiency. Moreover, our proposed model also attained higher results for other metrics (i.e., Precision, Recall, F1-score).
Fig. 7. Flow chart of proposed work.

Fig. 8. Accuracy, precision, recall and F1-score of hybrid algorithms.

Fig. 9. FPR, FDR, FNR and FOR of hybrid algorithms.

Fig. 10. TNR, MCC and NPV of hybrid algorithms.

Fig. 11. Time complexity of proposed hybrid algorithm.
VI. CONCLUSION

The growing number of IIoT devices has prompted research to consider the tremendously advanced security threats associated with them. The current literature shows that IIoT devices are vulnerable to varied botnet attacks. Further, botnet attacks carry extensive capabilities to throw the entire IIoT network into chaos. Consequently, there is a dire need for an efficient, adaptive, cost-effective, and highly scalable solution that can identify multi-vector botnet attacks to identify zero-day attacks. We proposed a novel, flexible, and adaptive hybrid DL algorithm employing DNN-LSTM. Our proposed mechanism outperforms with 99.94% detection accuracy with comparatively high-speed efficiency. The future road map is to implement various DL-driven tools for the timely detection of varied, sophisticated threats and cyber attacks in computational IoTs.

REFERENCES

[1] W. U. Khan, A. Ihsan, T. N. Nguyen, M. A. Javed, and Z. Ali, “NOMA-enabled backscatter communications for green transportation in automotive-industry 5.0,” *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2022.3161029.

[2] I. Butun, *Industrial IoT*. Berlin, Germany: Springer, 2020.

[3] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jantti, “Reinforcement learning in blockchain-enabled IIoT networks: A survey of recent advances and open challenges,” *Sustainability*, vol. 12, no. 12, 2020, Art. no. 5161.

[4] K. A. Abuhaseel and M. A. Khan, “A secure industrial Internet of Things (IIoT) framework for resource management in smart manufacturing,” *IEEE Access*, vol. 8, pp. 117354–117364, 2020.

[5] W. U. Khan et al., “Learning-based resource allocation for backscatter-aided vehicular networks,” *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2021.3126766.

[6] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, “An ensemble deep learning-based cyber-attack detection in industrial control system,” *IEEE Access*, vol. 8, pp. 83965–83973, 2020.

[7] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial Internet of Things (IIoT): An analysis framework,” *Comput. Ind.*, vol. 101, pp. 1–12, 2018.

[8] W. U. Khan, M. A. Javed, T. N. Nguyen, S. Khan, and B. M. Elhalawany, “Energy-efficient resource allocation for 6G backscatter-enabled IIoT IoV networks,” *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2021.3110942.

[9] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jantti, and Z. Han, “Spectral efficiency optimization for next generation NOMA-enabled IoV networks,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15284–15297, Dec. 2020.

[10] D. Shome, O. Waqar, and W. U. Khan, “Federated learning and next generation wireless communications: A survey on bidirectional relationship,” 2021, arXiv:2110.07649.

[11] X. Li et al., “Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things,” *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.

[12] W. U. Khan, F. Jameel, X. Li, M. Bilal, and T. A. Tsiltsis, “Joint spectrum and energy optimization of NOMA-enabled small-cell networks with QoS guarantee,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8337–8342, Aug. 2021.

[13] J. Sengupta, S. Ruj, and S. D. Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IIoT and IIoT,” *J. Netw. Comput. Appl.*, vol. 140, 2020, Art. no. 102481.

[14] A. Al Shorman, H. Faris, and I. Aljarah, “Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection,” *J. Ambient Intell. Human. Comput.*, vol. 11, no. 7, pp. 2809–2825, 2020.

[15] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, “A survey of machine and deep learning methods for Internet of Things (IoT) security,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1646–1685, Jul.–Sep. 2020.

[16] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, “BOTNETS: A survey of anomaly detection,” *Comput. Netw.*, vol. 57, no. 2, pp. 378–403, 2013.

[17] Y. Li et al., “Robust detection for network intrusion of industrial IoT based on multi-CNN fusion,” *Measurement*, vol. 154, 2020, Art. no. 107450.

[18] X. Jiang, M. Lora, and S. Chattopadhyay, “An experimental analysis of security vulnerabilities in industrial IoT devices,” *ACM Trans. Internet Technol.*, vol. 20, no. 2, pp. 1–24, 2020.

[19] M. Roopak, G. Y. Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” *IEEE Access*, vol. 8, pp. 45–102, 2020.

[20] T. Hasan, A. Adnan, T. Giannetsos, and J. Malik, “Orchestrating SDN control plane towards enhanced IoT security,” in *Proc. 6th IEEE Conf. Netw. Softwarization*, 2020, pp. 457–464.

[21] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018.

[22] P. Torres, C. Catania, S. Garcia, and C. G. Garino, “An analysis of recurrent neural networks for botnet detection behavior,” in *Proc. IEEE Biennial Congress Argentina*, 2016, pp. 1–6.

[23] C. D. McDermott, F. Majdani, and A. V. Petrovski, “Botnet detection in the Internet of Things using deep learning approaches,” in *Proc. Int. Joint Conf. Neural Net.*, 2018, pp. 1–8.

[24] A. Pekta and T. Acarman, “Botnet detection based on network flow summary and deep learning,” *Int. J. Netw. Manage.*, vol. 28, no. 6, 2018, Art. no. c2039.

[25] S. Radosavljevic and E. Ferrara, “Deep neural networks for bot detection,” *Inf. Sci.*, vol. 467, pp. 312–322, 2018.

[26] R. Vinayakumar, K. Soman, P. Poornachandran, and S. Sachin Kumar, “Evaluating deep learning approaches to characterize and classify the DGA’s at scale,” *J. Infell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1265–1276, 2018.

[27] A. Dawoud, S. Shahravani, and R. Chun, “Deep learning and software-defined networks: Towards secure IoT architecture,” *Internet Things*, vol. 3, pp. 82–89, 2018.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
[28] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, “BotShark: A deep learning approach for botnet traffic detection,” in Cyber Threat Intelligence, Berlin, Germany: Springer, 2018, pp. 137–153.

[29] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, “A botnet detection method on SDN using deep learning,” in Proc. IEEE Int. Conf. Consum. Electron., 2019, pp. 1–6.

[30] P. Krishnan, J. S. Najm, and K. Athanath, “SDN framework for securing IoT networks,” in Proc. Int. Conf. Ubiquitous Comput. Netw. Comput., 2017, pp. 116–129.

[31] E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, “Towards effective feature selection in machine learning based botnet detection approaches,” in Proc. IEEE Conf. Commun. Netw. Secur., 2014, pp. 247–255.

[32] L. Carl et al., “Using machine learning techniques to identify botnet traffic,” in Proc. 31st IEEE Conf. Local Comput. Netw., 2006, pp. 967–974.

[33] Y. Meidan et al., “Detection of unauthorized IoT devices using machine learning techniques,” 2017, arXiv:1709.04647.

[34] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, “DiDoT: A federated self-learning anomaly detection system for IoT,” in Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst., 2019, pp. 756–767.

[35] I. Indre and C. Lemmaru, “Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things,” in Proc. IEEE 12th Int. Conf. Intell. Comput. Commun. Process., 2016, pp. 175–182.

[36] S. Hochreuter and J. Schmidthuber, “Long short-term memory,” Neural Netw., vol. 9, no. 8, pp. 1735–1789, 1997.

[37] J. Schmidhuber, “Deep learning in neural networks: An overview,” Neural Netw., vol. 61, pp. 85–117, 2015.

[38] Y. Bengio et al., “Learning deep architectures for AI,” Found. Trends Mach. Learn., vol. 2, no. 1, pp. 1–127, 2009.

[39] A. Graves, “Long short-term memory,” in Supervised Sequence Labeling With Recurrent Neural Networks, Berlin, Germany: Springer, 2012, pp. 37–45.

[40] M. Sundermeyer, R. Schlüter, and H. Ney, “LSTM neural networks for language modeling,” in Proc. 13th Annu. Conf. Int. Speech Commun. Assoc., 2012.

[41] G. Montavon, W. Samek, and K.-R. Müller, “Methods for interpreting and understanding deep neural networks,” Digit. Signal Process., vol. 73, pp. 1–15, 2018.

[42] Y. Meidan et al., “N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018.

[43] M. M. Hassan, A. Gumaei, A. Alsanaid, M. Alrubaiyan, and G. Fortino, “A hybrid deep learning model for efficient intrusion detection in Big Data environment,” Inf. Sci., vol. 513, pp. 386–396, 2020.

[44] M. Abadi et al., “Tensorflow: A system for large-scale machine learning,” in Proc. 12th USENIX Symp. Oper. Syst. Des. Implementation, 2016, pp. 265–283.

[45] A. Gulli and S. Pal, Deep Learning With Keras. Birmingham, U.K.: Packt Publishing Ltd., 2017.

[46] V. Rey, P. M. S. Sánchez, A. H. Celdrán, G. Bovet, and M. Jaggri, “Federated learning for malware detection in IoT devices,” 2021, arXiv:2104.09994.

[47] T. V. Khoa et al., “Collaborative learning model for cyberattack detection systems in IoT industry 4.0,” in Proc. IEEE Wireless Commun. Netw. Conf., 2020, pp. 1–6.

[48] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, “Detecting Internet of Things attacks using distributed deep learning,” J. Netw. Comput. Appl., vol. 163, 2020, Art. no. 102662.

[49] D. Zheng, Z. Hong, N. Wang, and P. Chen, “An improved LDA-based ELM classification for intrusion detection algorithm in IoT application,” Sensors, vol. 20, no. 6, 2020, Art. no. 1706.

[50] H. Alazzam, A. Alsamady, and A. A. Shorman, “Supervised detection of IoT botnet attacks,” in Proc. 2nd Int. Conf. Data Sci., E-Learning Intf. Syst., 2019, pp. 1–6.

[51] J. Liu, S. Liu, and S. Zhang, “Detection of iot botnet based on deep learning,” in Proc. Chin. Control Conf., 2019, pp. 8381–8385.

[52] A. Pandey, S. Thaseen, C. A. Kumar, and G. Li, “Identification of botnet attacks using hybrid machine learning models,” in Proc. Int. Conf. Hybrid Intell. Syst., 2019, pp. 249–257.

[53] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, “IoT botnet detection approach based on PSL graph and DGCNN classifier,” in Proc. IEEE Int. Conf. Inf. Commun. Signal Process., 2018, pp. 118–122.

Tooba Hasan received the B.S. (Hons.) degree in information technology from Women University Multan, Pakistan, in 2016 and the M.Sc. degree in information security from COMSATS University, Islamabad, Pakistan, in 2021. She is currently working as a Research Officer at Vision Tech 360. Her research interests include software defined networking, Internet of Things (IoT), attack detection and prevention, malware analysis, cyber security, computer networks, computer vision, application of deep learning and machine learning in cyber defence, and medical disease prediction and detection.

Jahanzaib Malik received the M.Sc. degree in information security from COMSATS University, Islamabad, Pakistan. He is currently working toward the Ph.D. degree in the Interdisciplinary Centre of Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg. He has been a Researcher with the National Cyber Security Auditing and Evaluation Laboratory (NCSAEI), National University of Science and Technology, Islamabad, Pakistan. His research interests include software defined networking, devices security, threat detection and intelligence, malware analysis and detection, application of deep learning and machine learning in cyber defence, distributed computing, and Big Data.

Iram Bibi received the B.S. (Hons.) in software engineering degree from National University of Modern Languages (NUML) Islamabad, Pakistan, in 2017 and the master of science degree in information security from COMSATS University, Islamabad, Pakistan, in 2020. She was with Prosact Technologies as a Research Assistant. Her research interests include analysis and detection of network based cyber threat and attacks for android, Internet of Things, and software defined networking.

Waliullah Khan (Member, IEEE) received the master’s degree in electrical engineering from COMSATS University Islamabad, Pakistan, in 2017, and the Ph.D. degree in information and communication engineering from Shandong University, Qingdao, China, in 2020. He is currently working with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg. He has authored or coauthored more than 50 publications, including international journals, peer-reviewed conferences, and book chapters. His research interests include convex/nonconvex optimizations, non-orthogonal multiple access, reflecting intelligent surfaces, ambient backscatter communications, Internet of Things, intelligent transportation systems, satellite communications, physical layer security, and applications of machine learning.

Fahd N. Al-Websay received the B.S. degree in computer science from the University of Science and Technology, Taiz, Yemen, in 2006, the M.S. degree in computer information systems from The Arabic Academy for Banking and Financial Sciences, Sana’a branch, Yemen, in 2009, and the Ph.D. degree in computer science from Swami Ramanand Teerth Marathwada University, Nanded, India, in 2015. From 2006 to 2009, he was a Research Assistant, and from 2010 to 2015, he was a Lecturer with the Faculty of Engineering, University of Science and Technology. From 2015 to 2018, he was an Assistant Professor with the Faculty of Computer and Information Technology, Sana’a University, Sana’a Yemen, and since October 2018, he has been an Assistant Professor with the Computer Science Department, King Khalid University, Abha, Saudi Arabia. He is the author of ten books, more than 80 articles, and many funded research projects. His research interests include AI, IoT, smart cities, machine learning, biomedical, software engineering, applied soft computing, information security, and enterprise systems.
Kapal Dev (Senior Member, IEEE) received the Ph.D. degree from the Politecnico di Milano, Milan, Italy. He is currently an Assistant Lecturer with Munster Technological University (MTU), Ireland, and formerly he was a Senior Researcher with same University. Previously, he was a Postdoctoral Research Fellow with the CONNECT Centre, School of Computer Science and Statistics, Trinity College Dublin (TCD). He was a 5G Junior Consultant and Engineer with Altran Italia S.p.A., Milan, Italy, on 5G use cases. He worked for OCEANS Network as the Head of Projects funded by European Commission. His Ph.D. was awarded under the prestigious Fellowship of Erasmus Mundus funded by European Commission. He has authored or coauthored more than 40 research papers majorly in top IEEE Transactions, top Magazine and Conferences. He is serving as an Associate Investigator (AI) by CONNECT Centre, Trinity College Dublin (TCD) funded by Science Foundation. He is also serving as an Associate Editor in NATURE, Scientific Reports, Springer WINE, IET Quantum Communication, IET Networks, Springer HCIS, Area Editor in Elsevier PHYCOM, Technical Committee Member in Elsevier COMCOM, and the Editorial Board Member of IEEE Future Directions Newsletter: Technology, Policy and Ethics. He performed duties as the Guest Editor (GE) in several journals, IEEE NETWORK, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE STANDARD COMMUNICATION MAGAZINE. He was/is the Lead Workshop Chair in one of IEEE Blockchain2022, IEEE ICDCS 2022, IEEE CCNC 2021, IEEE Globecom 2021, IEEE PIMRC 2021 and ACM MobiCom 2021 workshops. He is the TPC Member of IEEE ICC 2021 (Aerial Communication Track), IEEE ISC2 (Security and Privacy Track)2021, ICBC 2021, DICG Co-located with Middleware 2020. He is a founding Chair of IEEE ComSoc special interested group titled as Industrial Communication Networks under CSIM technical committee. He is an Expert External Evaluator of several MSCA Co-Fund schemes, Elsevier, IET, Springer Book proposals and top scientific journals and conferences.

Gaojian Huang (Member, IEEE) received the bachelor’s degree in electronic information engineering and the Ph.D. degree in information and communications engineering from the Guilin University of Electronic Technology, Guilin, China, in 2013 and 2021, respectively. From October 2017 to October 2018, he was a Visiting Researcher with Queen’s University Belfast, Belfast, U.K. He is currently a Lecturer with the School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo, China. His research interests include integrated sensing and wireless communication designs, antenna array, physical layer security, emerging modulation techniques, and 5G/6G related areas.