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

Preprint · March 2022

DOI: 10.36227/techrxiv.19313318.v3

7 authors, including:

Tooba Hasan
Vision Tech 360
7 PUBLICATIONS **49** CITATIONS
SEE PROFILE

Jahanzaib Malik
University of Luxembourg
15 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Iram Bibi
Eindhoven University of Technology
13 PUBLICATIONS **158** CITATIONS
SEE PROFILE

Wali Ullah Khan
University of Luxembourg
164 PUBLICATIONS **2,263** CITATIONS
SEE PROFILE

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

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

***Abstract*—Industrial Internet of Things (IIoT) formation of richer ecosystem of intelligent interconnected devices while enabling new levels of digital innovation has essentially transformed and revolutionized global manufacturing and industry 4.0. Conversely, the prevalent 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 connects IIoTs. Besides, botnet attack detection is extremely 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)-enabled mechanism to secure IIoT infrastructure from lethal and sophisticated multi-variant botnet attacks. The proposed mechanism has been rigorously evaluated with latest available dataset, standard and extended performance evaluation metrics, and current DL benchmark algorithms. Besides, cross validation of our results are also performed to clearly show overall performance. The proposed mechanisms outperforms in identifying accurately multi-variant sophisticated bot attacks by achieving 99.94% detection rate. Besides, our proposed technique attains 0.066(ms) time that also shows the promising results in terms of speed efficiency.**

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

I. Introduction

No doubt, Industrial internet of Things (IIoT) is exponentially growing to make a tremendous digital landscape and thus becoming part and parcel of our daily lives [1], [2]. The IIoT ecosystems are contributing to smart agriculture, e-health, e-government, smart cities, e-logistics, home automation, industrial systems, e-wearables, and transportation [3], [4]. The shift from traditional network to IoTs have revolutionized the global world. Smart devices are intelligent, interconnected and location-aware that creates smart world around users while generating big IoT data that is the new gold mine to be subsequently used for various behavioral analytic, varied computational intelligence [5]and decision making [6], [7]. In recent statistical report, approximately 75 billion IoT smart devices are expected to be connected by the end of 2025 [8], [9].

However, the diverse landscape of IoT protocols, heterogeneity in transmission of data and devices, resource constraints, and one time embedded deployment of IoT [10], [11] devices; make them more insecure towards prevalent cyber threats and attacks [12]. 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 [13]. Among aforementioned attacks, Botnets are considered as the most sophisticated and lethal attack used to paralyze the entire network [14]. Botnet is purposefully crafted malware that possesses the capability to propagate over the network and smart devices through exploiting vulnerabilities in-turn leveraging remote access to cyber adversaries [15], [16].

For the security of heterogeneous IIoT devices and generated traffic [17], existing solutions for 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 digital infrastructure of IoT as it requires continuous updates of signatures for latest prevalent threats, therefore; it is incapable to detect zero-day threats, attacks, and vulnerabilities due to its dynamic and heterogeneous nature [18]. 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 [19]. 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:

- 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 practised to compute the actual potential of proposed technique to provide a thorough evaluation.
- We have also compared our proposed method to other hybrid algorithms and current DL benchmarks. With a minor trade-off in time efficiency, our devised mechanism outperforms in terms of detection accuracy.
- In addition, 10-fold cross validation technique is used to ensure that the results shown are unbiased.

Tooba Hasan, Jahanzaib Malik and Iram Bibi are with the Department of Computer Science, COMSATS University Islamabad (emails: toobahasan.int@gmail.com, researcher.mjm@gmail.com, Ask4iram@gmail.com)

Wali Ullah Khan is with the SnT, University of Luxembourg (email: waliullah.khan@uni.lu)

Fahd N. Al-Wesabi is with the Department of Computer Science, College of Science Art at Mahayil, King Khalid University, Saudi Arabia and also with the Department of information Systems, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen (email: falwesabi@kku.edu.sa)

Kapal Dev is with the Department of Institute of Intelligent Systems, University of Johannesburg, South Africa (email: kapal.dev@ieee.org)

Gaojian Huang is with the Physics and Electronic Information Engineering, Henan Polytechnic University (email: g.huang@hpu.edu.cn)

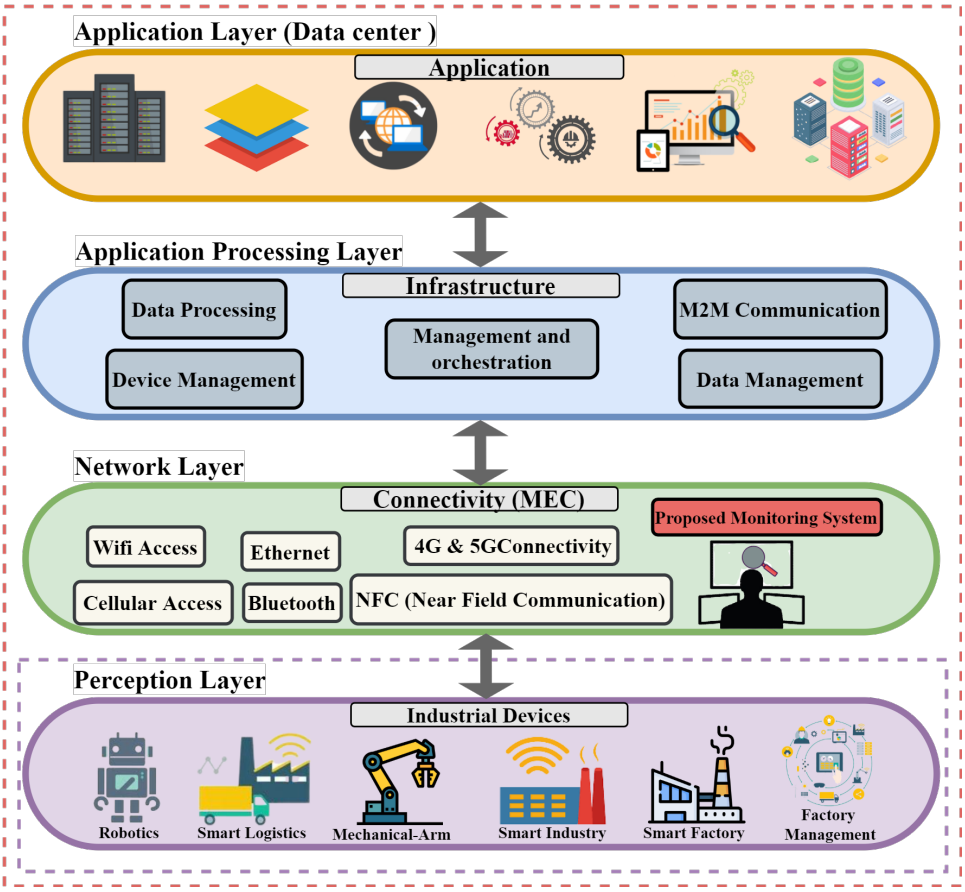

Fig. 1. Architecture of Industrial Internet of Things (IIoT)

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 description of 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 wide attention of many academic and industrial researchers in the field of information security, computer vision, sound and text analysis and pattern recognition because of its self learning ability which helps to accomplish high classification accuracy in complex environments [20]. Table I outlines the current literature detailing attacks, dataset, strength, limitations, and future directions. For cyber threat and attack detection, [21] shows a DL-based mechanism using LSTM for detecting botnet. The dataset is collected by examine the network packets of Technical University called Czech. Algorithm gets 99.90% detection rate. The authors in [22], demonstrate a framework of identifying the botnet by analyzing the packets using Bidirectional LSTM. The self generated dataset of Mirai and benign instances has been considered and acquire 96% accuracy. Meanwhile, [23] 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 [24], 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 the Cresci and collaborators. The authors in [25], 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 [26], implemented an intrusion detection to safeguard the IoT by deploying SDN and depict the testing rate of 95%. The KDD99 dataset take into consideration for attack detection (i.e. DoS, Login and Probe) with Restricted Boltzmann Machine (RBM). Consequently, [27] 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 utilized data is ISCX. In [28], the authors proposed an approach that prevents the detection of host after infection by utilizing 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, [20] proposed the varied attack detection framework in IoT through

TABLE I
RELATED WORK.

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 behavior of network traffic	Analysis of network behavior.	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	Mirai 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 Auto-encoder,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 auto encoder 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 traffic of each session and segregates the infected machine	Infected machine isolates by using FW and VLAN using SDN	Experiment did not conduct on infected terminal that infected by bots.	Need to explore that network isolation performed on the actual infected host o 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
[20]	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 feature with pair level features or conversational level feature to improve detection rate-
[21]	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 telltales	Lack in demonstrating the accuracy. The value of FPR and FNR are presented	
[22]	DDoS/Random Forest	Self Generated dataset	Extract the features that identify the IoT devices types as malicious and benign from white list	Need to enhance the dataset that identify 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 broad the investigation for other malware classifications

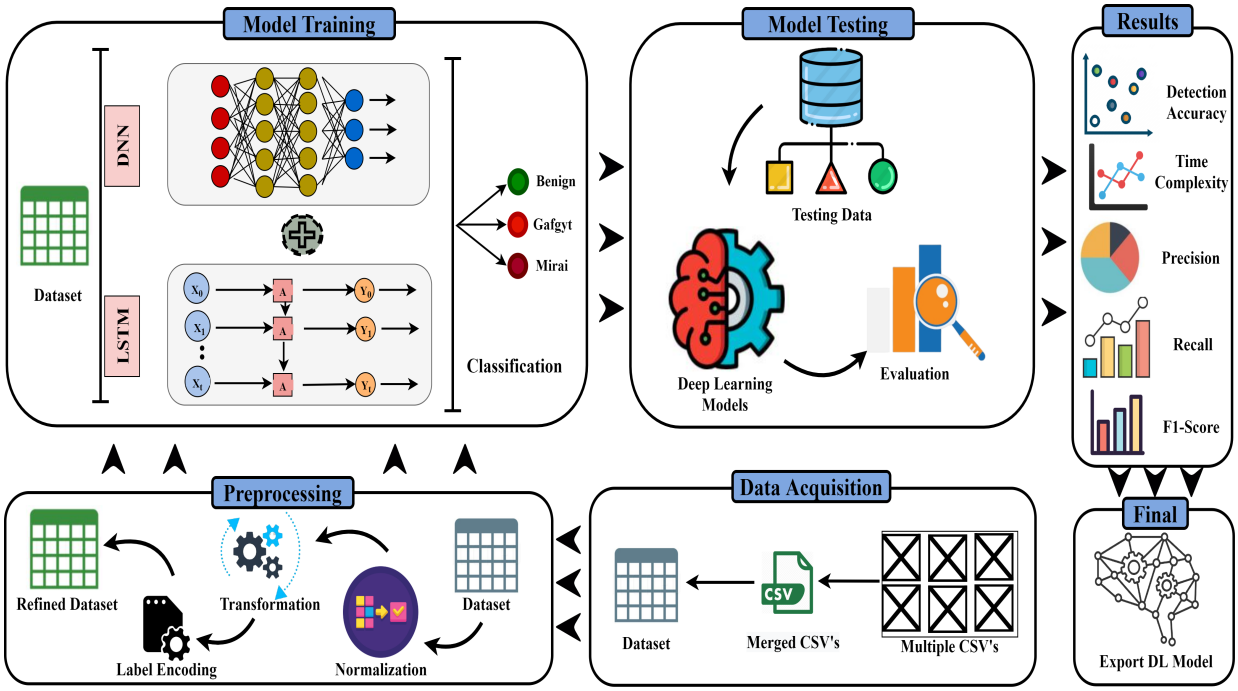

Fig. 2. Proposed simplified view of Hybrid framework (DNN-LSTM).

GRULSTM with the NSLKDD dataset. The proposed model attained an accuracy of 87.9% and provides a comparison with the traditional schemes. The authors in [29], developed an application for providing security policies and access control in various IoTs using open-flow interface. The research also discussed the major security vulnerabilities in IoT networks and the potential of SDN for providing security in IoT. In [30], the authors proposed a network flow capability scheme to identify botnet attacks. Ml algorithm called Decision Tree Algorithm (DT) is employed to deal with attack. ISCX2012 and ISOT dataset has been utilized and gets 99% rate. The author, in [31], used ML models such as Naive Bayes (NB), J48 and Bayesian to detect the botnet. The detection rate of FNR, FPR is defined as 1020 % and 3040 % respectively. The dataset is collected from the Dartmouth campus wireless network and tagged via detectors. In [32], the authors detect the DDoS attack by considering the Random Forest algorithm and achieves 99% percentage. The self-generated dataset is Wireshark through port mirroring on the switch to catch network traffic data. The author in [33] presents DIOT, a distributed self-learning system for efficiently detecting compromised IoT devices.The proposed system 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 [34], 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 detection accuracy of 98% employing KDD99 dataset. In the [19], the author proposed the IoT based paper that considered the power of DL based algorithm (i.e. LSTM) for detection of botnet attack. The paper utilized the N_IoT 2018 dataset which contained the data of varied IoT devices and gets the detection rate of 99.90%.

In general, the current literature either does not have a detailed evaluation, against state-of-the-art IoT-based datasets, or fewer instances are used both for training and testing. Conversely, our proposed hybrid DL-algorithm that leverages Long-short-term memory (LSTM) [35] and Deep Neural Network (DNN)[36][37] is devised. Our proposed work is efficient and highly scalable IIoT botnet detection framework.Besides, it comprehensively identifies lethal and sophisticated multi attacks in IIoT environment.

III. Preliminaries

In this section, the algorithms that are utilized in this paper are described.

A. Long-Short-Term Memory (LSTM)

The most advanced variant of Recurrent Neural Network (RNN) family is LSTM that addresses problem of limited learning in simple RNN. RNN suffered from the problem to learn long sequences as RNN has short term memory [35]. To solve these issues, the LSTM model was initially proposed to address the learning of longer sequences in data. LSTM has a similar control flow as a RNN for long term memory [38] 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 [39]. The back-propagation eliminates error signals that make execution of the system poorer. The main concept of LSTM is based on cell state, activation functions, and gates. The cell state act as communicators which transfer meaningful information to the next cell. It acts like “memory” of the current LSTM cell. The cell state carries significant

TABLE II
PRACTICAL ASPECT OF VARIED PROPOSED MODELS.

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		-			
	Dense 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		-			
	Dense 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		-			
	Dense 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		-			
	Dense Layer	40	-			
	Dense Layer	15	-			
	Output Layer	3	*softmax*			

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

information all through the process. As the cell state goes on, information get's added or taken out from the cell state through memory gate. The gate is capable to 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 that is designed to simulate the activities of human brain to recognize patterns [36]. DNN architecture has an input layer, output layer, and hidden layer. Each layer in DNN is comprised of neurons whereas these neurons take information and pass on to the next layer till output layer by performing addition and multiplication operation on weights [40]. The computation in DNN is performed on neurons which is the single unit for multi-step procedure of pattern recognition [37]. The node performs computation on input data and weights and passed the information to the next layer till it reaches 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 IIoT infrastructure is presented in this section. The purpose of the proposed model is to secure the IoT devices from varied attacks. The initial step is to utilize state-of-the-art updated dataset for thorough experimentation. Moreover, the sequence diagram of IIoT presented in Fig.3 that shows the communication process between each layer. Further, we have performed pre-processing of dataset which includes removal of data redundancy, data cleansing, and transformation, visualization, and feature engineering. After the preprocessing aspect, the data is practiced to be entered into classifiers for the identification of multiple IIoT attacks.

A. Dataset

For the training of the proposed algorithm, we considered the recent updated N_BaIoT [41] 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.

TABLE III
DISTRIBUTION OF DATASET

Name	Benign	Mirai	Gafgyt
Thermostat	6,666	10,000	10,000
737E Security Camera	6,666	10,000	10,000
838E Security Camera	6,667	10,000	10,000
1011 Web Cam	6,667	–	10,000
1002 Security Camera	6,667	10,000	10,000
1003 Security Camera	6,667	10,000	10,000
Total Records	**40,000**	**50,000**	**60,000**

B. Pre-processing

The pre-processing of N_ BaIoT is performed to improve the effectiveness and performance of our proposed hybrid deep

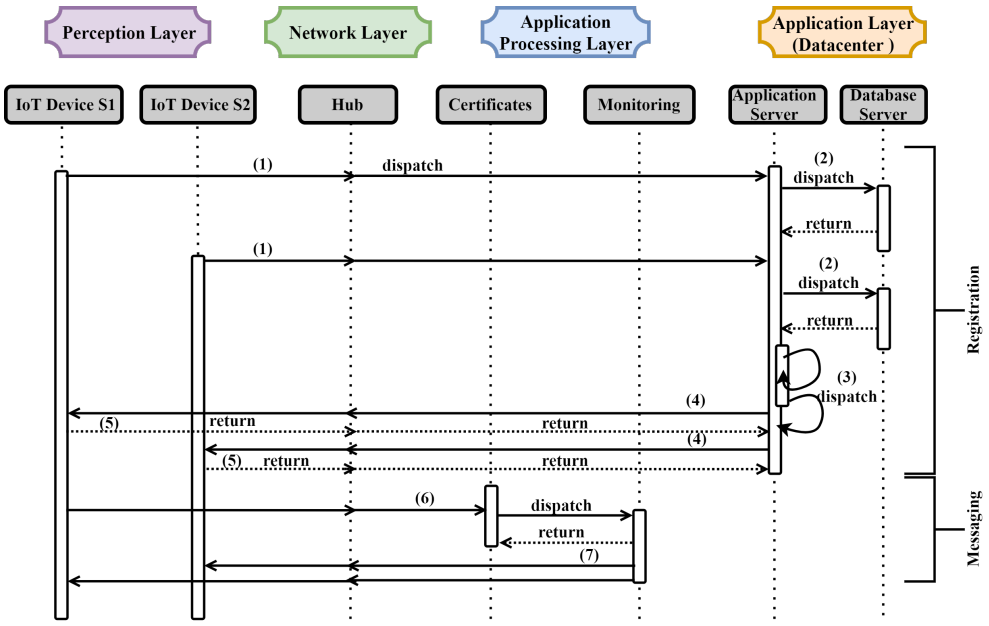

Fig. 3. Sequence diagram of IIoT with proposed monitoring system.

learning methodology. Initially, we verified the integrity of data by scanning and removing missing, nan and infinity values from 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 for training of deep learning algorithm.

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

```
function N-FOLD VALIDATION()
    for Fold = 1,2,....N do
        Classifier1 C1 add DNN Layer D
        Classifier2 C2 add LSTM Layer L
        Merge-out w.r.t C1 and C2
        Dense Layer D
        for Epoch = 1,2,....P do
            for Sample = 1,2,....S do
                Train the Model w.r.t B from S
                Calculate Loss w.r.t B
                if Predict False then
                    Update G
                end if
            end for
        end for
        Save Output for N
    end for
end function
```

The steps in the underway of model construction are also depicted in Fig.7 as a flow chart.

TABLE IV
SYSTEM ASPECTS FOR EXPERIMENTATION

Aspects	Specification	Version
Resources	Processor	Core-i7
	Generation	Eighth(8th)
	Model	81FV
	OS	Windows 10
	RAM	16GB
Environment	Anaconda Platform	2.0.3
	Spyder Tool	3.3.3
	Python Language	3.6
Libraries	Numpy	1.8.2
	TensorFlow	1.1.4
	Scikit-Learn	0.15.2
	Pandas	1.3.4
	Keras	2.6.2

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 Network (DNN) to design a hybrid model. Hybrid models are highly efficient to achieve high detection accuracy in less time [42]. Subsequently, to get benefit from varied deep learning classifiers simultaneously, we have considered LSTM and DNN for improving overall results. Consequently, in proposed hybrid framework, LSTM is considered due to its capability to achieve effective learning for longer sequences of data as IIoT devices generate huge amount of surge data in short time; whereas, DNN is used to enhance the predictive power of algorithm by improving speed efficiency. The detailed arrangement of our proposed hybrid architecture is elaborated in Table II. The modeling phases of our proposed model are portrayed in Fig.2.

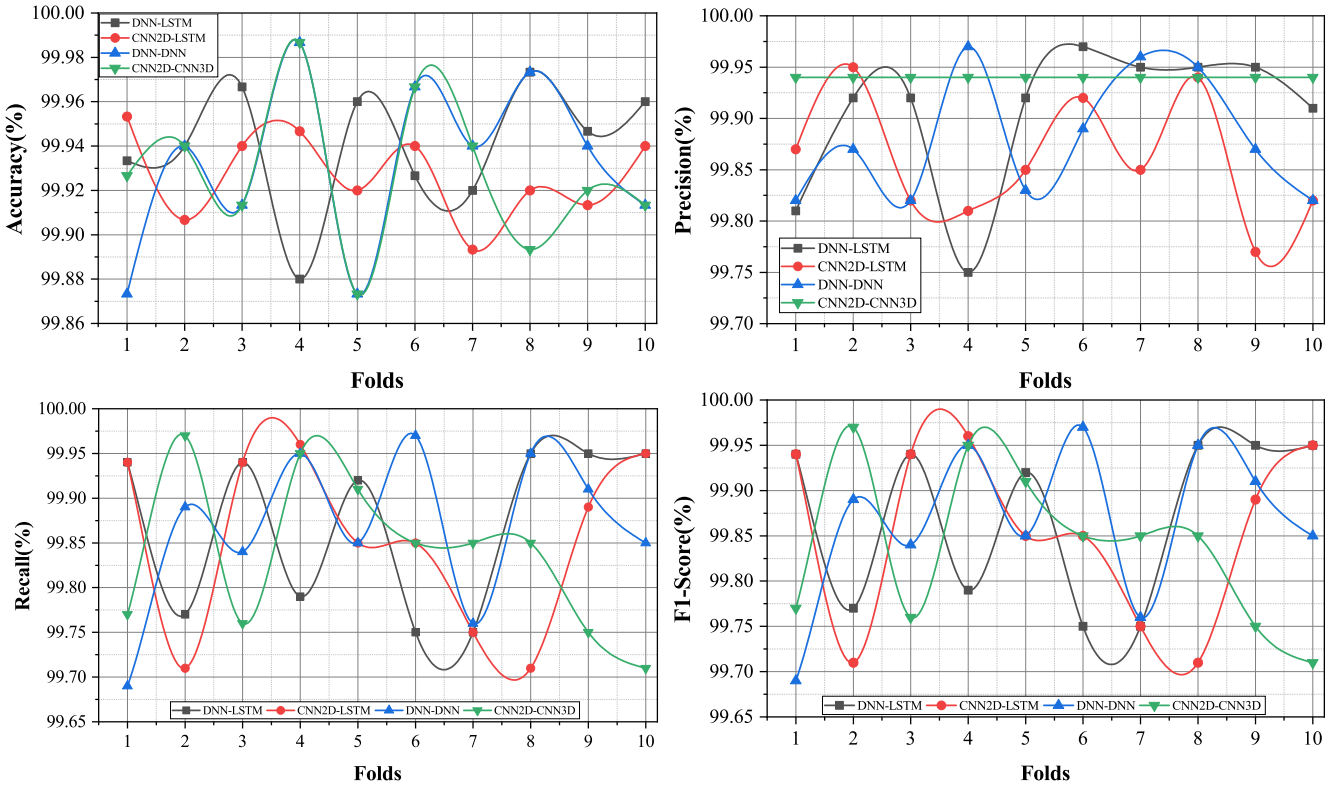

Fig. 4. 10 Folds of DNN-LSTM, CNN2D-LSTM, DNN-DNN and CNN2D-CNN3D.

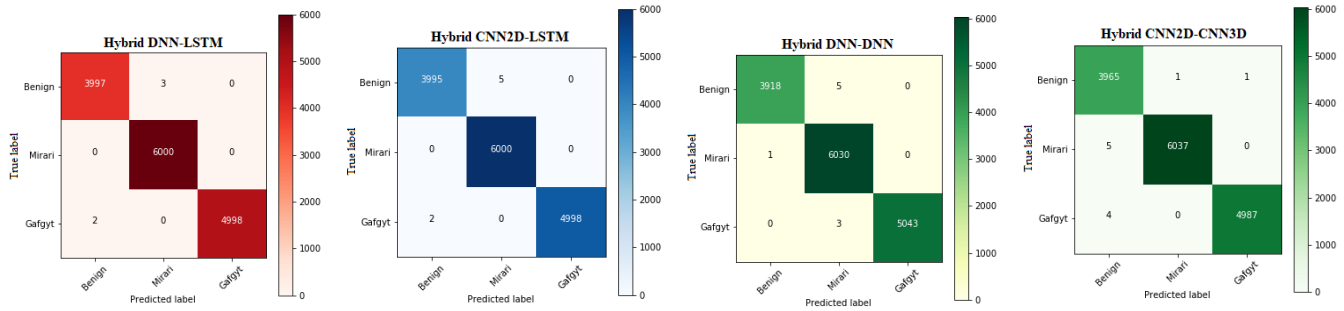

Fig. 5. Confusion Matrices of Hybrid Algorithms.

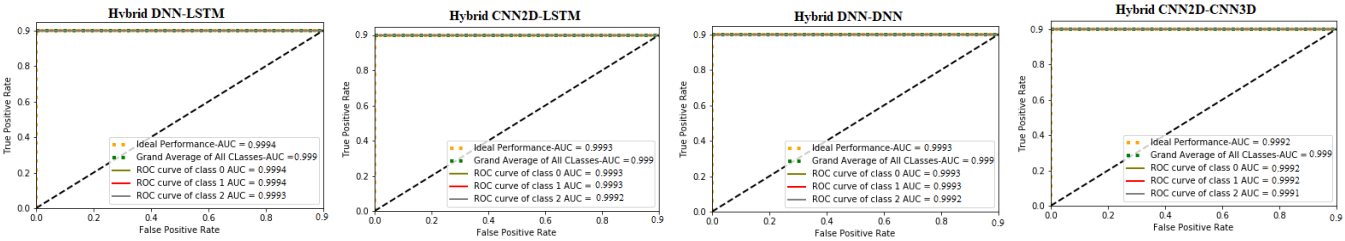

Fig. 6. ROC Curve of Hybrid Algorithms.

D. Experimental Setup

This section provides the experimentation and evaluation of our proposed mechanism for attack detection and performance. The experimental setup comprises of tensor-flow framework [43]. Python library named keras [44] is also utilized to design and implement the proposed hybrid model for botnet detection. The performance evaluation of the proposed system is conducted using sklearn library. The details of our experimental

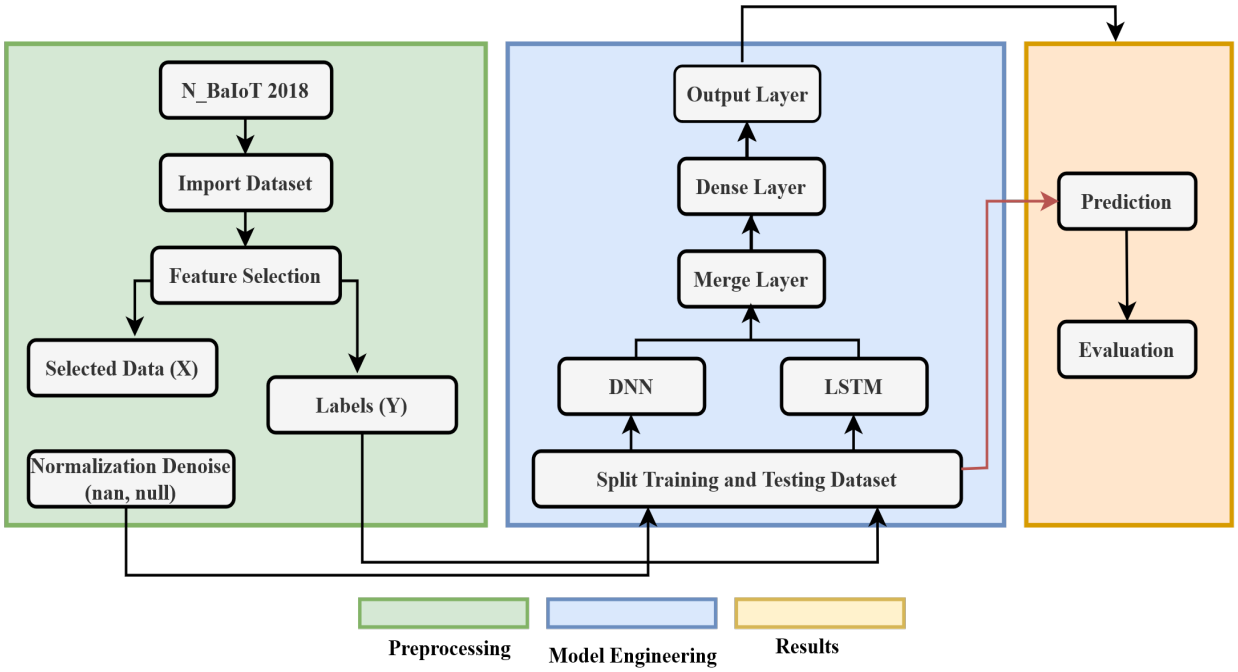

Fig. 7. Flow Chart of proposed work.

setup are presented in Table IV.

E. Evaluation Parameters

Various diverse evaluation parameters are used to evaluate the capabilities of proposed hybrid deep learning algorithm. The basic classification of true positive, true negative, false positive and false negative is presented through confusion matrix. While, 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.

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

Precision

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

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Recall

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

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

F1-score

It is a measure of test accuracy using the average between precision and recall.

$$F - score = \frac{2 * TP}{2 * TP + FP + FN} \tag{4}$$

ROC curve

The ROC curve, which plots the TP and FP rates in 2D, illustrates the system's detection ability. The overall performance of the system is the area under curve. The ROC-curve of varied algorithms are depict 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 are considered as an effective and efficient model. False Positive Rate (FPR) shows the correlation between known attack samples that are precisely classified from total attack records. False Discovery Rate (FDR) is a statistical approach that is used in testing to correct for multiple contrasts. False Omission Rate (FOR) is the complement of the PPV and NPV that measures the ratio of false negatives which are incorrectly rejected. The False Negative Rate (FNR) is the ratio

TABLE V
COMPARISON WITH EARLIEST DETECTION SOLUTIONS.

Schemes	Year	Algorithms	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	D.Time
Our	Our	DNN-LSTM	N_BaIoT 2018	99.94	99.91	99.86	99.86	0.066(ms)
[45]	2021	MLP-AE	N_BaIoT 2018	99.25	98.84	98.00	98.00	3.75(ms)
[5]	2020	DNN-DT	ICS-2015,2018	97.83	95.81	96.36	96.38	-
[16]	2020	Multi-CNN Fusion	NSL-KDD	86.95	89.56	87.25	88.41	-
[46]	2020	DBN	N_BaIoT 2018	95.60	98.27	92.82	92.82	-
[47]	2020	CNN,LSTM	N_BaIoT 2018	94.30	93.48	93.67	93.58	-
[48]	2020	LDA-ELM	NSL-KDD	92.35	-	-	-	0.163(ms)
[49]	2019	KNN, RF, NB	N_BaIoT 2018	99.00	86.65	99.00	99.00	-
[50]	2019	CNN	ISCX 2012	99.57	99.02	99.26	99.10	2078(ms)
[51]	2019	RF-SVM	ISCX 2012	85.30	82.70	73.50	73.50	-
[52]	2018	PSI Graph-CNN	IoTPOT 2017	92.00	89.20	94.00	94.00	-

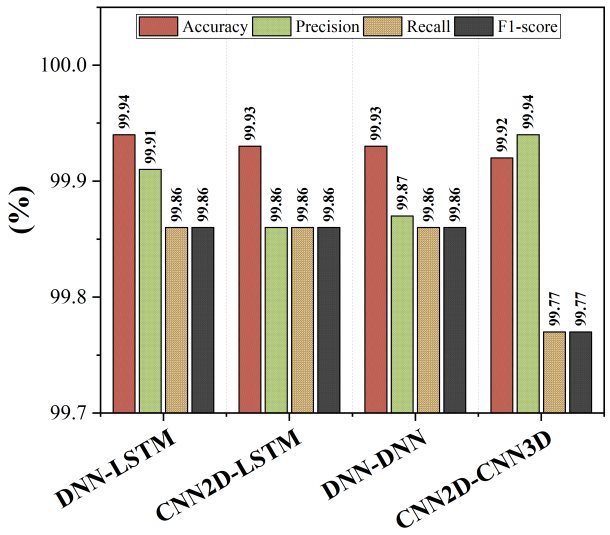

Fig. 8. Accuracy, Precision, Recall and F1-Score of Hybrid Algorithms.

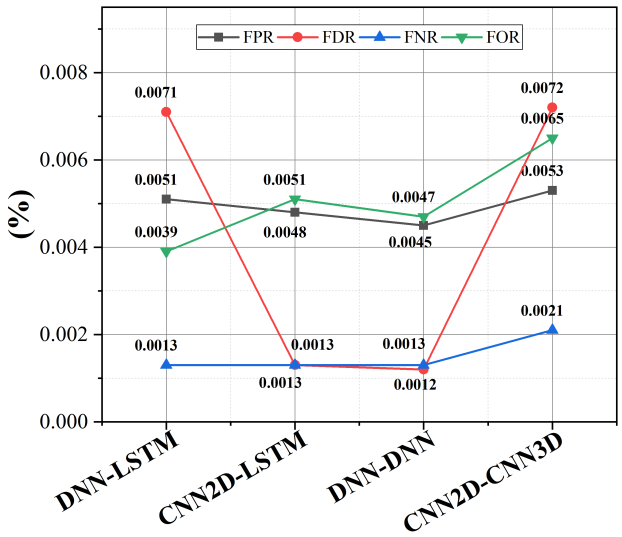

Fig. 9. FPR, FDR, FNR and FOR of Hybrid Algorithms.

of benign records that were incorrectly identified. The hybrid model of 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, hybrid model DNN-DNN achieved 0.0045%, 0.0013%, 0.0012%, and 0.0047% for FPR, FDR, FNR and FOR respectively. Consequently, hybrid CNN2D-CNN3D model achieved 0.0053%, 0.0072%, 0.0021% and 0.0065% values of FPR, FDR, FNR and FOR 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 values of TNR, MCC and NPV of proposed Hybrid DNN-LSTM model are 99.96%, 99.91% and 99.95%. The Hybrid model CNN2D-LSTM and DNN-DNN attain TNR, MCC and NPV of 99.95%, 99.88%, 99.94% and 99.95%, 99.89%, and 99.95% respectively.

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

For detailed analysis, we compared our proposed hybrid DNN-LSTM model with current advanced algorithms. Table V represents a thorough comparison with benchmark algorithms based on 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).

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 proven to be vulnerable to varied botnet attacks. Further, botnet attacks carry large capabilities to throw entire IIoT

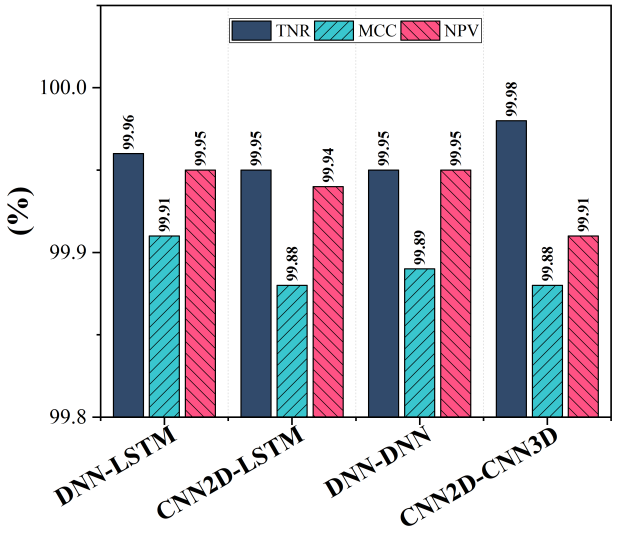

Fig. 10. TNR, MCC and NPV of Hybrid Algorithms.

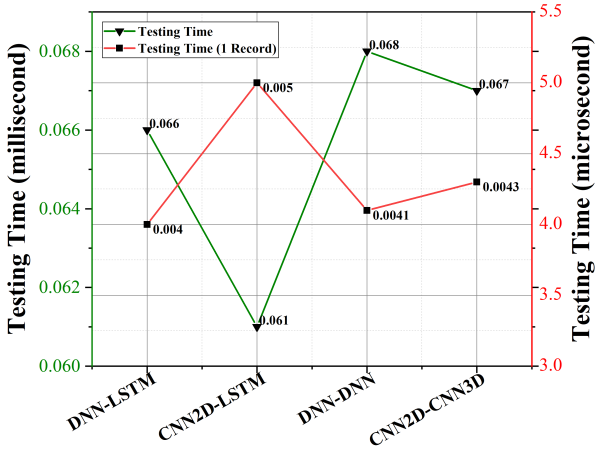

Fig. 11. Time Complexity of Proposed Hybrid Algorithm.

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 with capability of identifying 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 varied DL-driven mechanisms for timely detection of varied sophisticated threats and cyber attacks in computational IIoTs.

REFERENCES

[1] I. Butun, *Industrial IoT*. Springer, 2020.
[2] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jäntti, "Reinforcement learning in blockchain-enabled iiot networks: A survey of recent advances and open challenges," *Sustainability*, vol. 12, no. 12, p. 5161, 2020.
[3] K. A. Abuhasel and M. A. Khan, "A secure industrial internet of things (iiot) framework for resource management in smart manufacturing," *IEEE Access*, vol. 8, pp. 117 354–117 364, 2020.
[4] W. U. Khan, T. N. Nguyen, F. Jameel, M. A. Jamshed, H. Pervaiz, M. A. Javed, and R. Jantti, "Learning-based resource allocation for backscatter-aided vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2021.
[5] 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. 83 965–83 973, 2020.
[6] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in industry*, vol. 101, pp. 1–12, 2018.
[7] W. U. Khan, M. A. Javed, T. N. Nguyen, S. Khan, and B. M. Elhalawany, "Energy-efficient resource allocation for 6g backscatter-enabled noma iov networks," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
[8] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jäntti, and Z. Han, "Spectral efficiency optimization for next generation noma-enabled iot networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 284–15 297, 2020.
[9] D. Shome, O. Waqar, and W. U. Khan, "Federated learning and next generation wireless communications: A survey on bidirectional relationship," *https://arxiv.org/abs/2110.07649*, pp. 1–18, 2021.
[10] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, 2021.
[11] W. U. Khan, F. Jameel, X. Li, M. Bilal, and T. A. Tsiftsis, "Joint spectrum and energy optimization of noma-enabled small-cell networks with qos guarantee," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2021.
[12] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.
[13] 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," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 7, pp. 2809–2825, 2020.
[14] 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 Communications Surveys & Tutorials*, 2020.
[15] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013.
[16] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, "Robust detection for network intrusion of industrial iot based on multi-cnn fusion," *Measurement*, vol. 154, p. 107450, 2020.
[17] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–24, 2020.
[18] 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.
[19] T. Hasan, A. Adnan, T. Giannetsos, and J. Malik, "Orchestrating sdn control plane towards enhanced iot security," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 457–464.
[20] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.
[21] P. Torres, C. Catania, S. Garcia, and C. G. Garino, "An analysis of recurrent neural networks for botnet detection behavior," in *2016 IEEE biennial congress of Argentina (ARGENCON)*. IEEE, 2016, pp. 1–6.
[22] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in *2018 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2018, pp. 1–8.
[23] A. Pektaş and T. Acarman, "Botnet detection based on network flow summary and deep learning," *International Journal of Network Management*, vol. 28, no. 6, p. e2039, 2018.
[24] S. Kudugunta and E. Ferrara, "Deep neural networks for bot detection," *Information Sciences*, vol. 467, pp. 312–322, 2018.
[25] R. Vinayakumar, K. Soman, P. Poornachandran, and S. Sachin Kumar, "Evaluating deep learning approaches to characterize and classify the dgas at scale," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1265–1276, 2018.
[26] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: towards secure iot architecture," *Internet of Things*, vol. 3, pp. 82–89, 2018.
[27] S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "Botshark: A deep learning approach for botnet traffic detection," in *Cyber Threat Intelligence*. Springer, 2018, pp. 137–153.

[28] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, "A botnet detection method on sdn using deep learning," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019, pp. 1–6.

[29] P. Krishnan, J. S. Najeem, and K. Achuthan, "Sdn framework for securing iot networks," in *International Conference on Ubiquitous Communications and Network Computing*. Springer, 2017, pp. 116–129.

[30] E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, "Towards effective feature selection in machine learning-based botnet detection approaches," in *2014 IEEE Conference on Communications and Network Security*. IEEE, 2014, pp. 247–255.

[31] L. Carl *et al.*, "Using machine learning technliques to identify botnet traffic," in *Local Computer Networks, Proceedings 2006 31st IEEE Conference on. IEEE*, 2006.

[32] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of unauthorized iot devices using machine learning techniques," *arXiv preprint arXiv:1709.04647*, 2017.

[33] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "Dïot: A federated self-learning anomaly detection system for iot," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 756–767.

[34] I. Indre and C. Lemnaru, "Detection and prevention system against cyber attacks and botnet malware for information systems and internet of things," in *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)*. IEEE, 2016, pp. 175–182.

[35] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[36] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural networks*, vol. 61, pp. 85–117, 2015.

[37] Y. Bengio *et al.*, "Learning deep architectures for ai," *Foundations and trends® in Machine Learning*, vol. 2, no. 1, pp. 1–127, 2009.

[38] A. Graves, "Long short-term memory," in *Supervised sequence labelling with recurrent neural networks*. Springer, 2012, pp. 37–45.

[39] M. Sundermeyer, R. Schlüter, and H. Ney, "Lstm neural networks for language modeling," in *Thirteenth annual conference of the international speech communication association*, 2012.

[40] G. Montavon, W. Samek, and K.-R. Müller, "Methods for interpreting and understanding deep neural networks," *Digital Signal Processing*, vol. 73, pp. 1–15, 2018.

[41] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[42] 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.

[43] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard *et al.*, "Tensorflow: A system for large-scale machine learning," in *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, 2016, pp. 265–283.

[44] A. Gulli and S. Pal, *Deep learning with Keras*. Packt Publishing Ltd, 2017.

[45] V. Rey, P. M. S. Sánchez, A. H. Celdrán, G. Bovet, and M. Jaggi, "Federated learning for malware detection in iot devices," *arXiv preprint arXiv:2104.09994*, 2021.

[46] T. V. Khoa, Y. M. Saputra, D. T. Hoang, N. L. Trung, D. Nguyen, N. V. Ha, and E. Dutkiewicz, "Collaborative learning model for cyberattack detection systems in iot industry 4.0," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2020, pp. 1–6.

[47] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting internet of things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, p. 102662, 2020.

[48] 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, p. 1706, 2020.

[49] H. Alazzam, A. Alsmady, and A. A. Shorman, "Supervised detection of iot botnet attacks," in *Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems*, 2019, pp. 1–6.

[50] J. Liu, S. Liu, and S. Zhang, "Detection of iot botnet based on deep learning," in *2019 Chinese Control Conference (CCC)*. IEEE, 2019, pp. 8381–8385.

[51] A. Pandey, S. Thaseen, C. A. Kumar, and G. Li, "Identification of botnet attacks using hybrid machine learning models," in *International Conference on Hybrid Intelligent Systems*. Springer, 2019, pp. 249–257.

[52] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "Iot botnet detection approach based on psi graph and dgcnn classifier," in *2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP)*. IEEE, 2018, pp. 118–122.