sustainability

MDPI

Article

Secure IIoT-Enabled Industry 4.0

Zeeshan Hussain [1], Adnan Akhunzada [2], Javed Iqbal [1], Iram Bibi [3] and Abdullah Gani [4,*]

[1] Computer Science Department, Comsats University, Islamabad 45550, Pakistan; zeeshan.h1993@gmail.com (Z.H.); javediqbal@comsats.edu.pk (J.I.)
[2] Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia; adnan.akhunzada@ums.edu.my
[3] Centre for Security, Reliability and Trust, University of Luxembourg, L-4365 Luxembourg, Luxembourg; Ask4iram@gmail.com
[4] Faculty of Computing and Informatics, University Malaysia Sabah, Labuan 88400, Malaysia
* Correspondence: abdullahgani@ums.edu.my

Abstract: The Industrial Internet of things (IIoT) is the main driving force behind smart manufacturing, industrial automation, and industry 4.0. Conversely, industrial IoT as the evolving technological paradigm is also becoming a compelling target for cyber adversaries. Particularly, advanced persistent threats (APT) and especially botnets are the foremost promising and potential attacks that may throw the complete industrial IoT network into chaos. IIoT-enabled botnets are highly scalable, technologically diverse, and highly resilient to classical and conventional detection mechanisms. Subsequently, we propose a deep learning (DL)-enabled novel hybrid architecture that can efficiently and timely tackle distributed, multivariant, lethal botnet attacks in industrial IoT. The proposed approach is thoroughly evaluated on a current state-of-the-art, publicly available dataset using standard performance evaluation metrics. Moreover, our proposed technique has been precisely verified with our constructed hybrid DL-enabled architectures and current benchmark DL algorithms. Our devised mechanism shows promising results in terms of high detection accuracy with a trivial trade-off in speed efficiency, assuring the proposed scheme as an optimal and legitimate cyber defense in prevalent IIoTs. Besides, we have cross-validated our results to show utterly unbiased performance.

Keywords: Industrial Internet of Things; Internet-of-Things; network security; deep learning

Citation: Hussain, Z.; Akhunzada, A.; Iqbal, J.; Bibi, I.; Gani, A. Secure IIoT-Enabled Industry 4.0. *Sustainability* **2021**, *13*, 12384. https://doi.org/10.3390/su132212384

Academic Editors: Mohsin Raza, Ghufran Ahmed, Muhammad Awais and Jawad Ahmad

Received: 27 July 2021
Accepted: 18 October 2021
Published: 10 November 2021

1. Introduction

The Industrial Internet of Things, also known as Industrial IoT, is an industrial framework in which a large number of devices or machines are connected and synchronized using software tools and third platform technologies for providing varied services to internet users, public and private sector organizations, and smart industries and Industry 4.0 [1,2]. In the recent era, the IIoTs are experiencing astonishing growth rates due to their sensing, storing, and intelligence power in the current smart world [3,4]. From a recent statistical report, 70 billion IoT devices are expected to be connected over the internet in 2025 [5]. Such dependence on IoT results in the generation of a significant amount of data, processing, and examination. No doubt, big data analysis is also valuable for business development [6]. However, the biggest threat to potentially reduce the growth of IIoTs are numerous cyber threats that can compromise the integrity of user data and underlying IoT application for further exploitation. Besides, the risk of being physically compromised that underlies IoT devices due to their prevalent nature is also considered a critical threat in IIoTs environment [7]. Cyber defense is a pivotal prerequisite for potential growth of IIoT [8].

Therefore, adversaries practice diverse kinds of malware techniques to obtain access to an IoT device for malfunctioning the entire IIoT network [9]. Attacks performed on a network are fundamentally resilient to detect and have been a proven strategy to compromise

interconnected systems and devices [10]. The adversary breaks the security and obtains the benefit to access the user's records, steal sensitive information, and inject malicious code for further exploitation or hijacked hardware. The heterogeneous and dynamic nature of IoT gadgets and various resource constraints such as energy, memory, and processing power amplifies the potential cyber threats exponentially that may prompt Denial of Service (DoS), distributed Denial of Service (DDoS), information infusion, advance persistent threat (APT), and modern malware botnet attacks altogether [11,12]. Moreover, the IIoT devices are prone to complex hacking approaches, physical security dangers for the accessibility and classification of data, or even compromise the complete IoT-based network. Hence, IIoT requires an adaptable, robust, and cost-effective technique for the identification of pervasive and prevalent cyberthreats [13].

In recent years, research has been executed for addressing various security challenges for IIoTs such as confidentiality, privacy, policy enforcement, and key management issues, and so forth [14]. Besides, traditional techniques such as antiviruses and firewall protection can be easily evaded by zero-day intrusions [15]. Machine learning (ML) techniques are also considered powerful and mostly rely on analysis of the features of existing patterns. However, the extant ML schemes become less effective for zero-day attack variants. The prime challenge for malware identification framework is to find a means for extraction of useful features and detect sophisticated malware efficiently [16]. Deep learning is considered an ideal current shift for the identification of pervasive IIoT cyber malware threats and attacks [17,18]. To address the aforementioned challenges, we present an efficient hybrid DL-driven multiclass cyberthreat and -attack detection scheme for proficiently identifying distributed variant malware botnet attacks in IIoTs. The offered key contributions are as follows:

1.1. Contributions

- We propose an efficient hybrid DL-enabled technique for the detection of sophisticated distributed IIoT botnet attacks by deploying Long short-term memory (LSTM) and Convolutional Neural Network (CNN).
- Extensive simulations have been performed on N_BaIoT 2018 dataset to evaluate the performance of proposed algorithms by utilizing extended performance metrics (accuracy, precision, recall, F1-score, etc.).
- For corroboration purposes, the proposed approach is compared with our constructed hybrid DL-driven architectures (i.e., DNN-DNN and CNN-CNN) and current benchmarks. Our proposed mechanism outperforms the others in terms of detection accuracy.
- Extensive experimental results demonstrate that our proposed method is an effective and efficient approach for multivector botnet detection.
- We also performed 10-fold cross-validation to avoid showing biased performance results.

1.2. Organization

The remaining parts of the paper are organized in the following way. Section 2 presents the literature review with background knowledge. Section 3 contains the research approach, dataset description, preprocessing of dataset, architectural description of hybrid LSTM-CNN. Section 4 consists of software and hardware requirements and experiment results discussion. At last, Section 5 comes to an end with the proposed scheme and future map.

2. Background and Related Work

The Internet of Things (IoTs) is a conversion from a basic physical conventional object to a smart object through the utilization of cutting-edge technologies such as communication technologies, applications, sensor networks, internet protocols, and pervasive computing. Due to the wide range of applications of IoTs in the smart city ecosystem, the flawless implementation of a secure IoT network is necessary. The IoT environment can

be explained as the enormous interconnected heterogeneous devices and systems with different communication protocols and patterns [13,19]. To deliver intelligence-enabled services to users, the IIoT architecture has consisted of computational objects linked with IoT infrastructure. Moreover, the IoT network has been developed as a four-layer architecture named as the devices layer, network layer, infrastructure layer, and application layer. The taxonomic simple architectural diagram of IIoT can be visualized in Figure 1.

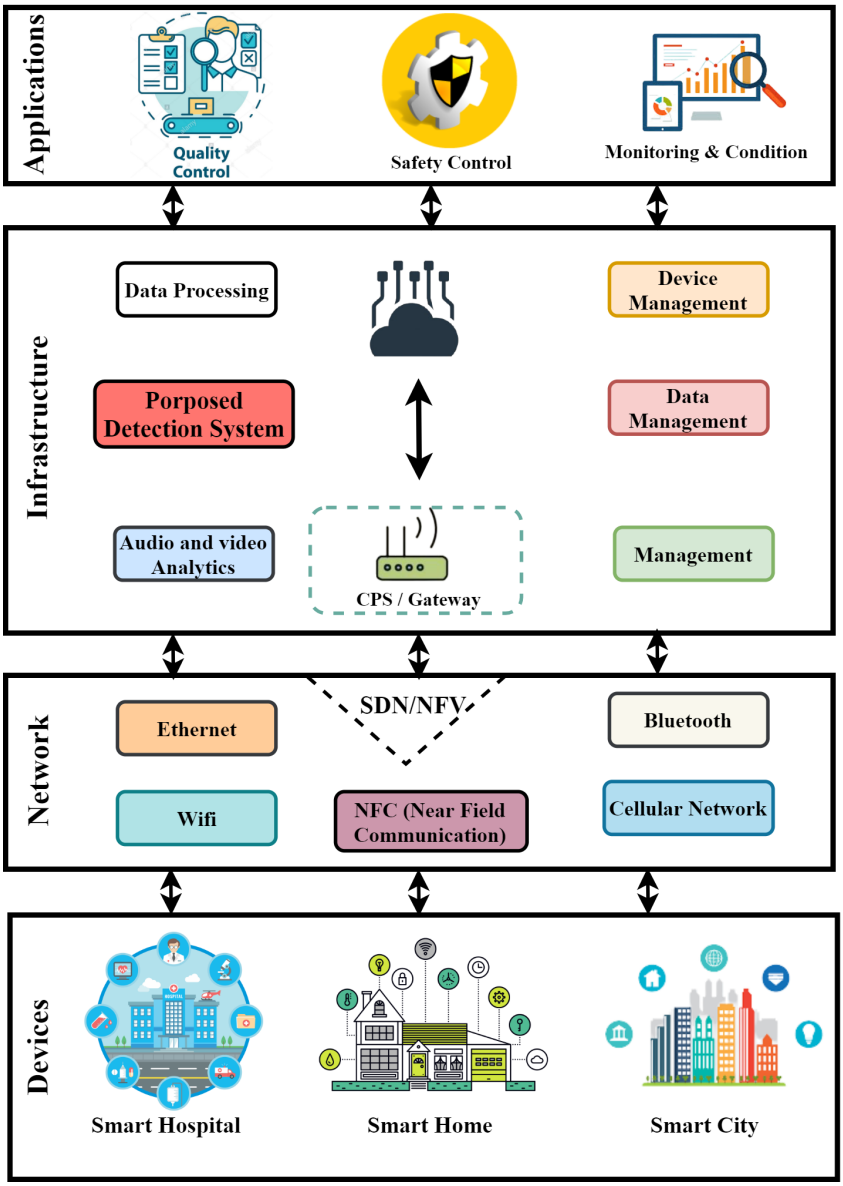

Figure 1. The Industrial Internet of Things system architecture.

The perception layer is included with the connected physical objects and their connectivity through different access points such as a radio tower, satellite, wireless access point, and satellite dish. The physical sensors are physical objects and the objective is to sense, gather, and process information. As the IoT devices are resource-constrained devices due to limited processing capabilities, data delivery is the key step for designing a context-aware IoT system. The higher number of IoT devices and ever-increasing data on a daily basis generated through these devices indicate a correlation with big data and expansion in intelligence-based ecosystems. The connectivity of heterogeneous devices helps to provide smart services to users that should be low-powered communication for transmission of data [20,21].

The network layer enables the corporation between diverse IoT devices so they can interact with each other effortlessly. Moreover, the network layer also provides interoperability and scalability in the IoT realm. The main function of this middle layer is context awareness and device discovery, which should be provided to support the surrounding IoT objects. The security and privacy of IoT devices are also handled at the middle layer because the data gathered from these devices are mostly industry or human-related and the security mechanisms are also deployed for IoT security. The IoT-based system has applications in several domains including smart healthcare, transportation, smart grids, and smart cities. At the application level, the services are delivered to consumers and the data gathered and analyzed are integrated for the business objective. The integrated data through different levels of IoT models are used for social and economic growth [11].

Due to the advancement of varied IoT devices in the industry, the security of IoT networks has become the prime focus. To provide a practical solution from the existing security vulnerabilities in IoT systems, researchers have focused on presenting DL//ML-based attack identification frameworks [22–25]. In [26], the author proposed an ensemble technique of Recurrent families that are required to identify various IoT cyberattacks through analysis of network traffic. The dataset considered is Modbus/TCP network traffic dataset synthetic based on an industrial automation context. The proposed technique obtained 99% detection accuracy. Consequently, [27] presented a scheme for IoT-based phishing and botnet attacks through distributed deep learning. The LSTM classifier has been practiced and employed with the N_BaIoT dataset and achieved 94.3% and 94.80% accuracy for phishing and botnet attacks, respectively. Chen et al., in [28], introduced an intrusion detection method for conversation-based traffic analysis employing five different machine learning classifiers named Random Forest, REP tree, Random Tree, Bayes-Net, and Decision Tree. Using the CTU-13 dataset, the approach has achieved a detection rate of 93.6%.

In another study, Bansal et al. [29] proposed anomaly-based IDS using three different deep learning classifiers named Clustering, Neural Network stimulated by LSTM, and Recurrent Neural Networks for IoT's. The proposed mechanism has been experimented with using ISCX and CTU-13 datasets, achieving the detection accuracy of 98.8%, 98.39%, and 83.09% for Clustering, NN-LSTM, and RNN, respectively. For malicious traffic detection, Pektaş et al. in [30] proposed a DL-Driven network traffic flow behavior analysis leveraging Neural Network. This approach has been evaluated for binary classification utilizing the ISOT and CTU-13 datasets, and achieved the detection accuracy of 99.3% and 99.1% respectively. Moreover, Sharma et al. in [31] presented a machine-learning-based approach for the detection of evolving malware through analyzing the network traffic features. The dataset contains 11,688 malware collected from the Malicia project and 4006 benign gathered from multiple systems connected over the network. The framework has been executed using diverse machine learning classifiers (i.e., RF (random forest), LMT (Logistic model tree), NBT (Naïve Bayes Tree), FT (Functional Tree), and J48) whereas RF achieved an accuracy of 97.95%. In [32], a K-Mean Clustering technique for labeling the dataset was presented. The decision tree has been experimented for the detection of cyberthreats in IoT communication using the ISCX dataset, achieving the accuracy of 88%, which can be improved by using loss function to reduce classification error. Whereas, in [33], the authors proposed a Logistic-Regression-enabled botnet detection technique for IoT. The proposed scheme can scale enormous malware samples into groups of clusters based on their behavior. The technique achieved 97.3% detection accuracy.

The author in [33] used features selection to minimize the features that are helpful to detect the bots in IoT. These features provide a high accuracy detection rate over the IoT to detect the botnet. Machine learning technique called decision tree classifier is experimented on N-BaIoT dataset. Deep learning provides a flexible environment for detecting malware.

The research work of [34] presented an efficient IoT-based malware detection through packet-level analysis by implementing a Bidirectional Long Short-Term Memory based Recurrent Neural Network (BLSTM-RNN). The paper also generated a labeled dataset having

attack vectors such as a botnet and benign traffic. Experimental results showed detection accuracy for Mirai, DNS, and UDP as 99%, 98%, and 98%, respectively. Consequently, in [35], the authors provided a technique through LSTM to inspect the statistical-based network flow feature. The experimental results are achieved through the Cresci dataset and achieved 99% detection accuracy for IoT malware detection. The datasets utilized for the proposed scheme are CTU-13 and ISOT, which are pure binary (i.e., botnet, normal). These datasets are a combination of both botnet and normal traffic. Machine learning and deep learning classifiers i.e., SVM, Logistic Regression, Random Forest, KNN stand-alone LSTM, stand-alone dense, and combined layer are used and showed an accuracy of 99.3%. All convolutional approaches are executed on CPU and all deep learning approaches are executed on GPU.

In [36], the author focuses on finding domain names that do not belong to data in context, statistical information, etc. For this, Deep-learning-based classifiers known as LSTM, RNN, CNN, and CNN-LSTM are employed. However, the dataset composed of one billion records of benign collected from Alexa, open-DNS, and malicious records was created from 17-DGA. Deep-learning-based IDS in [37] was presented for identification of intrusions, leveraging Gated Recurrent Neural Network in IoT network. The proposed classifier achieved a detection accuracy of 98.91% and FAR of 0.76%. Consequently, the article [38] employed deep Auto Encoder and Deep Forward Neural Network for detection of malware attacks in IoTs. This model scored a detection accuracy of 99%.

As per the findings from the literature review, despite achieving high detection accuracies, there still exist several limitations including high computational complexity, reliability on humans, extensive data modifications, and also inconsistent accuracy levels. Researchers have been working on hybrids, ensembles, and also experimenting on diverse hyperparameters (e.g., training, optimization, activation, and classification) to come up with the most accurate and time-saving solution for anomaly detection. Existing research also demonstrates that ensemble or hybrid techniques have a lot of potential in the field of network security anomaly detection. The goal of deep hybrid learning techniques is not to surpass existing classifiers, but to make use of their capability for not misclassifying unseen data. Nonetheless, in contrast with other existing intrusion detection schemes for IoT, we present a comprehensive hybrid framework based on cutting-edge deep learning from the IoT security perspective. This paper presents an efficient approach to identify sophisticated attacks in IoT environments through utilizing the predictive power of deep learning.

3. Research Methodology

This section presents the proposed hybrid DL-enabled multivector attack detection framework for IoT systems. The foundation of the presented model is a combination of several processes. The initial step is the dataset description and observation of features. In the subsequent step, the preprocessing of the dataset is performed, which is included with removing data redundancy, cleaning data, visualization, feature engineering, and data transformation. After preprocessing, data were prepared for input to classifiers for IoT attack identification. Consequently, the hybrid Long short-term memory (LSTM) [39] and Convolutional Neural Network (CNN)-based [40] efficient and scalable malware detection framework is presented.

3.1. Dataset

The features of IoT devices can be analyzed through the internet protocols and services they utilize. Network traffic analysis is the ideal choice for the identification and classification of cyberattacks. In any exploration, to obtain precise results, authentic and accurate data must be provided as input data. To design a reliable and applicable intrusion detection system, the data gathered from real devices are optimal to use. However, most of the present analysis approaches utilized datasets collected using the sandbox, which is not precise for the real deployment of identification frameworks in IoT infrastructure. In this study, we used the N_BaIoT 2018 dataset captured through real IoT devices. This

dataset fills a gap in the public botnet databases, particularly for IoT devices. The dataset N_BaIoT 2018 contains the features of real normal traffic [41] and 9 different IoT devices (i.e., Doorbells, Thermostat, Baby Monitor, Security Cameras, and Webcam). The N_BaIoT dataset considers the two malware families of a botnet: GAFGYT and MIRAI. The available dataset traffic were comprehensively recorded for normal and 2 distinct botnet attacks. For our experiment, we considered 6 diverse IoT devices and two botnet families, Gafgyt and Mirai, to detect Botnet attacks. The dataset distribution for the proposed scheme is defined in Table 1.

Table 1. N_BaIoT Dataset for Practical Experimentation.

Classes	Number of Records
Benign	27,892
Gafgyt	199,651
Mirai	246,559
Total	**468,102**

3.2. Preprocessing Phase

Deep learning requires a comprehensive data analysis to predict IoT traffic as malicious and benign. So, the very first step was to arrange information in such arrangement that it would be compatible with the input to any deep learning classifier. The dataset contains missing values, infinity, and nan values. In data denoising, these unexpected values were removed from the dataset. In the following step, the types of features were identified, such as numerical and categorical data. The conversion of categorical to numeric data was also performed through label encoding.

3.3. Detection Phase

In this research, a robust, proficient, scalable, and highly accurate hybrid IoT multi-variant botnet attack detection scheme is presented through leveraging Long-short-term-memory (LSTM) and Convolutional Neural Network (CNN), as portrayed in Figure 2. The proposed approach aims to design a system for the identification of Gafgyt and Mirai attacks. The proposed LSTM-CNN architecture mainly included three steps to recognize intrusion in smart devices.

Step 1. Modeling of data dimension

At the start, the pre-processed network traffic data is mapped into two-dimensional (2D) feature vector for CNN. As the variants of CNN classifier can be of different dimensions starting from 1D to 3D, the data for the experimentation are the number of samples (features, records); so, they are mapped into 2D.

Step 2. Initialization of CNN and LSTM network

For the experimentation, the CNN network was designed with an input layer, three hidden layers, and an output layer. To facilitate the CNN algorithm for feature learning, the input layer converted the 1D network dataset into 2D plane data. Three convolution layers and a flatten layer were included in the implied layer. The convolution layer continually maps the sample data to a high-dimensional space and learns the network connection data feature information. By lowering the dimension of the retrieved features, the flatten layer decreases computation and enhances the model detection efficiency. However, the LSTM network consists of an input layer; three hidden LSTM layers; and finally, an output layer. The data were mapped on the input layer to feed forward to LSTM cells. The LSTM layers were attributed to achieving success in recognizing network anomalies efficiently.

Step 3. The combined output

Once both the classifiers were initialized and executed for the identification of attacks in IoT, the additive merge was performed to manifest the ultimate performance of a proposed algorithm.

The complete design of hybrid LSTM-CNN architecture, including layer architecture, number of neurons set in each layer, activation function, loss function, number of epochs, and batch size, are detailed in Table 2. Moreover, we constructed other contemporary hybrid architectures (i.e., CNN-CNN, DNN-DNN) for a comprehensive evaluation of our proposed technique. To address bias, we also performed 10-fold cross-validation.

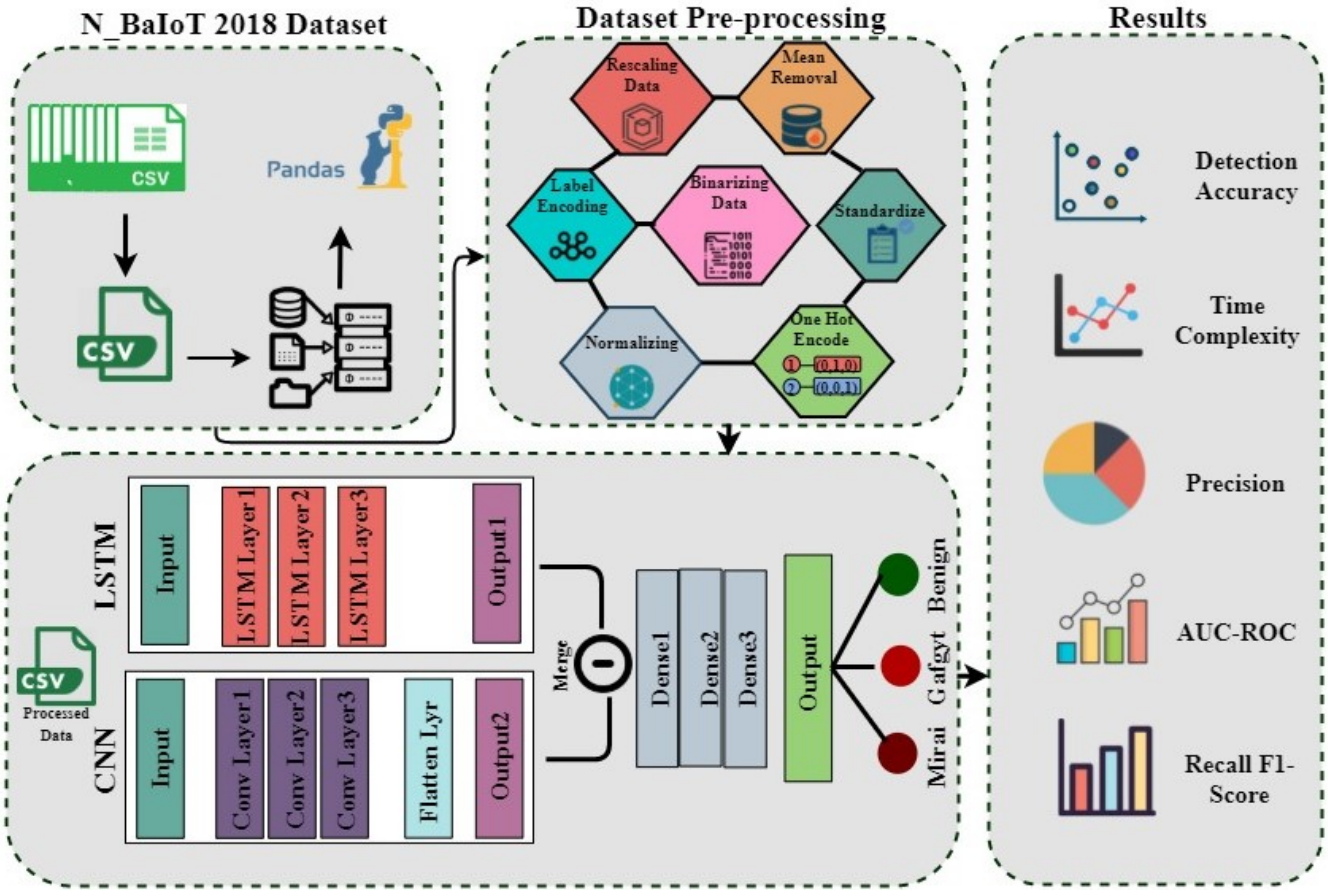

Figure 2. Architectural description for the proposed hybrid LSTM-CNN framework.

Table 2. Description of algorithms for the system model.

Algorithm	Layers	Type	Neuron	Output	MergeOut	Output
CNN	*CNN Layer*	Convolution	25	CNN Output	Dense Layer(15) Dense Layer(10) Dense Layer(3)	Output
	CNN Layer	Convolution	20			
	CNN Layer	Convolution	15			
	CNN Layer	Flatten				
LSTM	*LSTM Layer*		25	LSTM Output		
	LSTM Layer		20			
	LSTM Layer		15			

Table 2. *Cont.*

Algorithm	Layers	Type	Neuron	Output	MergeOut	Output
DNN	*Dense Layer* *Dense Layer* *Dense Layer*		25 20 15	DNN Output	Merge	Output
DNN	*Dense Layer* *Dense Layer* *Dense Layer*		25 20 15	DNN Output		
CNN	*CNN Layer* *CNN Layer* *CNN Layer* *CNN Layer*	Convolution Convolution Convolution Flatten	25 20 15	CNN Output	Dense Layer(15) Dense Layer(10) Dense Layer(3)	Output
CNN	*CNN Layer* *CNN Layer* *CNN Layer* *CNN Layer*	Convolution Convolution Convolution Flatten	25 20 15	CNN Output		

Batch Size = 256, ***Epochs*** = 5, ***Optimizer*** = Adam, ***Activation Function*** = Relu, ***Loss Function*** = *Categorical Cross-Entropy*.

4. Experimental Results and Discussion

This section presents our simulation results and a basic description of performance metrics. For framework development and evaluation, the Anaconda (python distribution platform) was utilized. The detailed software and hardware system specifications for the proposed DL IoT malware detection scheme are defined in Table 3. Moreover, the proposed solution was evaluated using a set of classification metrics as Detection Accuracy, Recall, Precision, Area Under Curve (AUC), True Positive Rate (TPR), False Positive Rate (FPR), False Omission Rate (FOR), False Negative Rate (FNR), Matthews Correlation Coefficient (MCC), Negative Predictive Value (NPV), and F1 Score. The proposed hybrid LSTM-CNN was also evaluated against the 10-fold cross-validation technique. The *k*-Fold validation technique is a statistical model to evaluate supervised AI-based classifiers. *k*-Fold provides prediction accuracy and also avoids overfitting in the model, where it repeats to obtain maximum scoring while it lacks in obtaining predictions.

Table 3. Hardware and software specifications for evaluation of proposed algorithms.

Component	Software
CPU: Corei7-8750H@2.21 GHz	Windows 10
RAM: 16 GB	Python, TensorFlow, Pandas, Keras
Graphic Card: 4 GB 1050 Ti	Numpy, Scikit-Learn, Matplot

Discussion

To show the legitimacy and productiveness of our proposed methodology, we performed some experiments to show a basic implementation of a model for multiple attacks of IoT botnet. For evaluation, the experiment is executed for three classes, two botnet attacks (i.e., Marai, gafgyt), and one benign class.

To assess the performance of our experiment, we evaluated our model on various parameters, i.e., Accuracy, Recall, Precision, Confusion Matrix, and F1-Score. The values of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) were taken from the confusion matrix, which was further used to calculate other standard parameters (i.e., accuracy, precision, recall, F1-score, etc.). The confusion matrices for the proposed and other constructed hybrid classifiers are defined in Tables 4–6. According to the graph, LSTM-CNN classified 46,794 samples accurately and misclassified 18 samples overall, which is a more accurate classification compared with DNN-DNN (27 misclassified) and CNN-CNN (20 misclassified).

Table 4. Confusion matrix for LSTM-CNN.

Actual Class / Predicted Class	Benign	Gafgyt	Mirai
Benign	2786	4	0
Gafgyt	9	19,957	0
Mirai	1	4	24,051

Table 5. Confusion matrix for DNN-DNN.

Actual Class / Predicted Class	Benign	Gafgyt	Mirai
Benign	2784	9	0
Gafgyt	6	19,778	1
Mirai	2	9	24,222

Table 6. Confusion matrix for CNN-CNN.

Actual Class / Predicted Class	Benign	Gafgyt	Mirai
Benign	2875	7	0
Gafgyt	3	19,755	1
Mirai	5	4	24,165

Standard evaluation parameters such as Accuracy, Precision, Recall, and F1-score were evaluated to show the performance of the proposed framework, defined in Figure 3. The hybrid LSTM-CNN performed better with 99.95% detection accuracy, 99.72% precision, 99.58% recall, and 99.58% F1-score compared with other hybrid classifiers. The high detection rate of LSTM-CNN is due to the combined predictive power of two distinct classifiers (i.e., LSTM, CNN) from two different families of deep learning. The results for the 10-fold cross-validation technique are presented in Table 7.

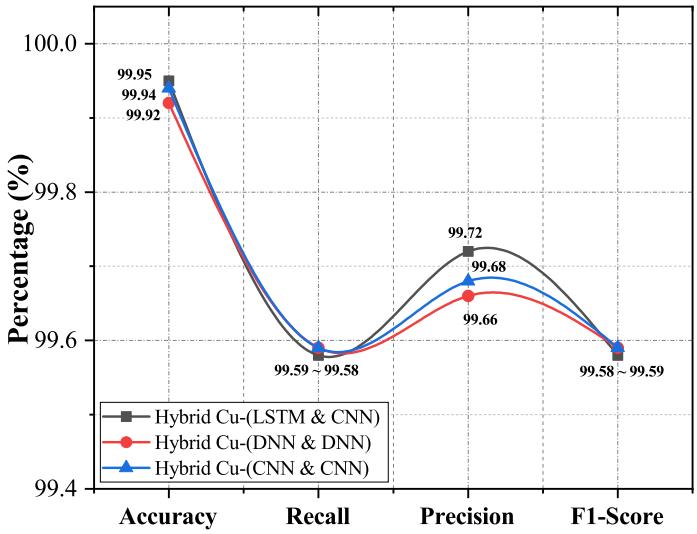

Figure 3. Accuracy, precision, recall, and F1-score of proposed algorithms.

Table 7. 10-fold of Our proposed algorithms.

	Accuracy (%)			Recall (%)			Precision (%)		
Folds	**L-C**	**D-D**	**C-C**	**L-C**	**D-D**	**C-C**	**L-C**	**D-D**	**D-D**
1	99.9	99.9	99.9	99.5	99.3	99.7	99.8	99.6	99.7
2	99.9	99.9	99.9	99.6	99.6	99.5	99.8	99.3	99.6
3	99.9	99.9	99.9	99.6	99.5	99.5	99.7	99.7	99.7
4	99.9	99.9	99.9	99.5	99.7	99.4	99.7	99.8	99.8
5	99.9	99.9	99.9	99.7	99.6	99.5	99.6	99.6	99.9
6	99.9	99.9	99.9	99.6	99.6	99.6	99.6	99.7	99.2
7	99.9	99.9	99.9	99.2	99.6	99.6	99.7	99.4	99.6
8	99.9	99.9	99.9	99.6	99.5	99.5	99.7	99.7	99.8
9	99.9	99.9	99.9	99.3	99.5	99.7	99.8	99.6	99.5
10	99.9	99.9	99.9	99.7	99.5	99.5	99.3	99.7	99.7

Abbreviation Terms: **C-L** Hybrid (LSTM and CNN), **D-D** Hybrid (DNN and DNN) **C-C** Hybrid (CNN and CNN).

False Positive Rate (FPR) is additionally called False Alarm Rate (FAR), and it speaks to the proportion between the erroneously classified negative examples to the complete number of negative examples. False Discovery Rate (FDR) and False Omission Rate (FOR) measures complement the PPV and NPV, respectively. The False Negative Rate (FNR) or miss rate is the proportion of positive samples that were incorrectly classified. The hybrid of LSTM-CNN achieved rates for FPR, FDR, FNR, FOR as 0.017%, 0.027%, 0.041%, and 0.026% respectively (Figure 4).

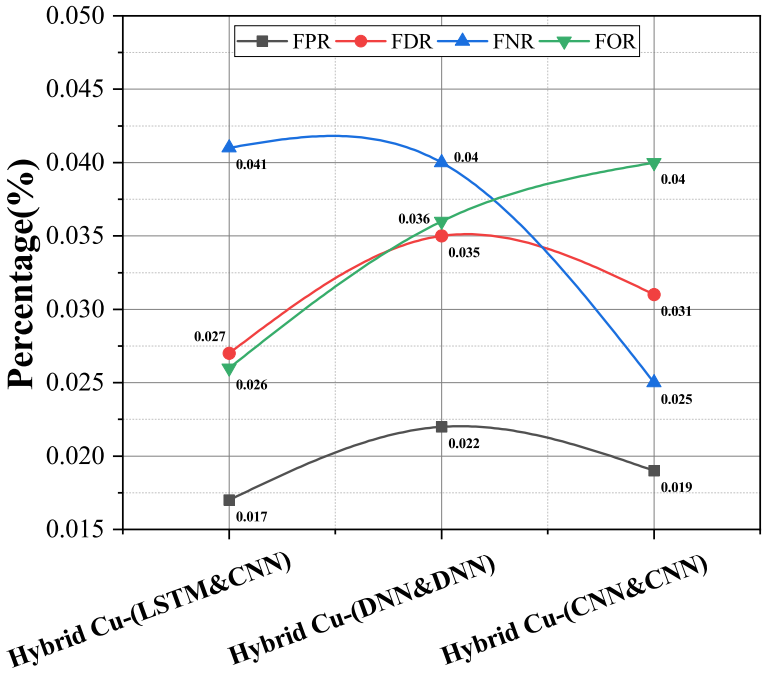

Figure 4. FNR, FPR, FDR, and FOR of proposed algorithms.

In addition, the TNR, MCC, and NPV values were calculated from the confusion matrix. The true negative rate (TNR) is the ratio of correctly classified attack samples to the total number of attacks. The Matthews Correlation Coefficient (MCC) measurement shows the correlation between the observed and predicted rankings. Negative Predictive Value (NPV) calculates the ratio of correctly classified attack dataset to the total predicted attack dataset. The calculated values are portrayed in Figure 5.

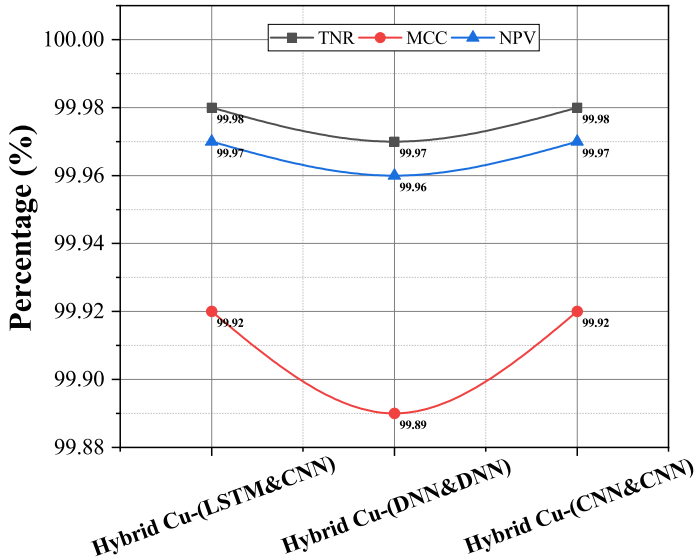

Figure 5. TNR, MCC, and NPV Rate of Proposed Algorithms.

Table 8 shows the comparison of our proposed technique with four very similar approaches for malware identification in IoT. The compared results clearly show efficient results in terms of detection accuracy and other standard performance metrics. Moreover, none of the compared schemes were executed for multivector attacks.

Table 8. The table of comparison for our findings and other existing benchmarks.

Parameters	**[42]**	**[43]**	**[44]**	**[41]**	**Proposed**
Dataset	ISCX2012	CTU-13	POT	N_BaIoT	N_BaIoT
Algorithm	CNN	MLP	Deep CNN	Autoencoder	LSTM-CNN
Binary_class	–	✓	✓	–	–
Multi_class	✓	–	–	–	✓
10-fold	–	–	–	–	✓
Accuracy	99.57	99.20	92.00	99.95	
Precision	99.02	98.80	86.65	98.80	99.72
Recall	99.26	98.92	91.85	98.92	99.58
F1-score	99.10	98.92	94.00	98.92	99.58
Testing Time	2078 (ms)	–	–	–	1.58 (ms)
FPR	0.11	–	–	–	0.013
Other Metrics	✓	–	–	–	✓

Others = *TNR, FNR, FDR, FOR, BM, MCC, TS, NPV.*

The execution time for the proposed classifier is defined as shown in Figure 6. Three milliseconds were taken by the model LSTM-CNN higher compared with other hybrids (DNN-DNN, CNN-CNN). It can be viewed from the graph that LSTM-CNN has a trivial trade-off with other algorithms in testing time. Consequently, there is a need for improvement to minimize the execution time of the proposed algorithm. AU-ROC is considered an essential graphical observation parameter. The relationship between True Positive Rate (TPR) and False Positive Rate (FPR) has been shown through AU-ROC. The line representation of every class near to axis indicates its potential. AU-ROCs for proposed and constructed contemporary classifiers are presented in Figure 7. The achieved results of more than 90% for TP rate for almost all 3 distinct classes direct the AU-ROC curve close to unity.

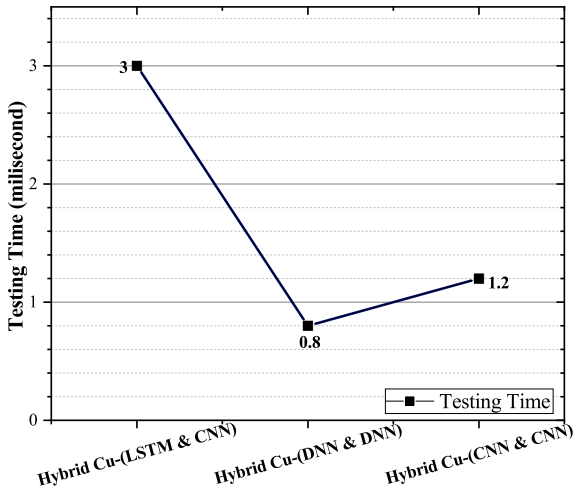

Figure 6. Testing time of proposed algorithms.

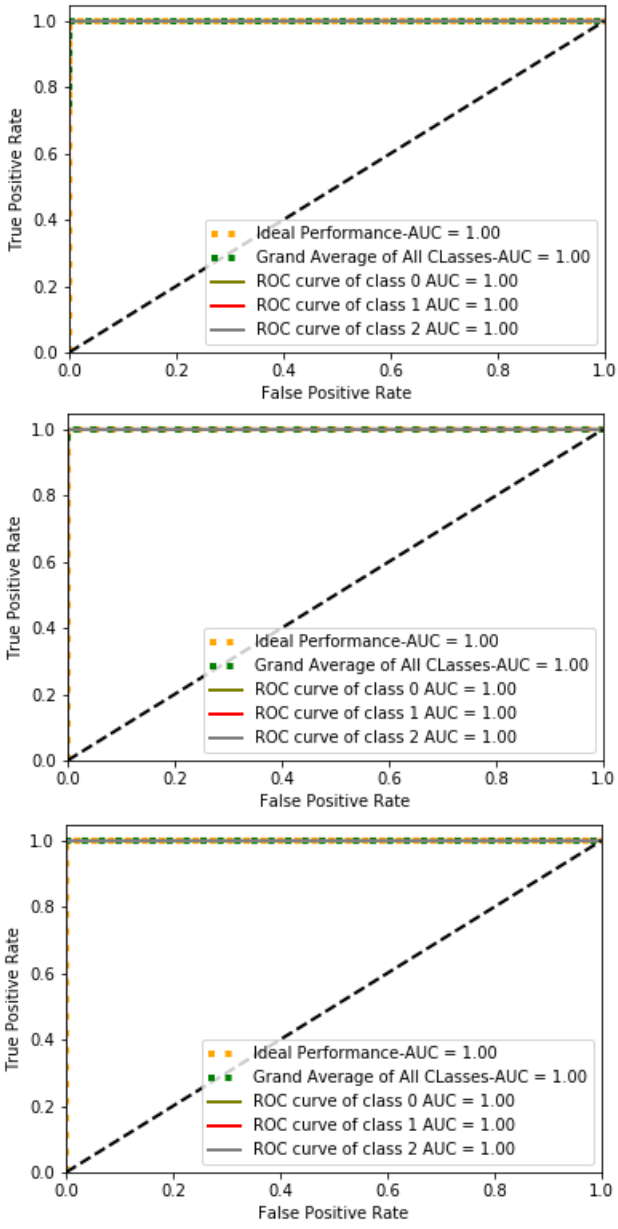

Figure 7. AU-ROC curve of proposed algorithms.

5. Conclusions

The inadequate security measures of diverse IoT devices and prevalent environments expose them to diverse sophisticated threats and attacks in IIoTs. In this study, we proposed a hybrid DL-driven architecture leveraging Long short-term memory (LSTM) and Convolutional Neural Network (CNN) for cyberthreats and lethal botnet distributed attack detection in IIoTs. The proposed method outperformed 99.95% in attack detection rate against multivector attacks, and after careful evaluation, we found a negligible trade-off in terms of speed efficiency. Finally, we inscribe and investigate the other hybrid architecture of deep learning for the detection of varied cyberattacks in diverse IoT communication and computational environments.

Author Contributions: Conceptualization, Z.H. and A.A.; Methodology, Z.H.; software, Z.H.; validation, A.A., J.I.; formal analysis, I.B.; investigation J.I.; writing—original draft preparation, Z.H.; writing—review and editing, I.B.; visualization, I.B.; supervision, J.I.; project administration, A.G.; funding acquisition, A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received funding from Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu, Malaysia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Komatwar, R.; Kokare, M. A survey on malware detection and classification. *J. Appl. Secur. Res.* **2021**, *16*, 390–420. [CrossRef]
2. Liang, F.; Yu, W.; Liu, X.; Griffith, D.; Golmie, N. Toward edge-based deep learning in industrial Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 4329–4341. [CrossRef]
3. Khan, W.Z.; Rehman, M.H.; Zangoti, H.M.; Afzal, M.K.; Armi, N.; Salah, K. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Comput. Electr. Eng.* **2020**, *81*, 106522. [CrossRef]
4. Akhunzada, A.; ul Islam, S.; Zeadally, S. Securing cyberspace of future smart cities with 5g technologies. *IEEE Netw.* **2020**, *34*, 336–342. [CrossRef]
5. Top Emerging IoT Trends Business Should Look for in 2021. Available online: https://www.fintechnews.org/top-emerging-iot-trends-business-should-look-for-in-2021 (8 April 8 accessed on 2021).
6. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of a machine and deep learning methods for the internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
7. Guo, Y.; Zhao, Z.; He, K.; Lai, S.; Xia, J.; Fan, L. Efficient and flexible management for industrial Internet of Things: A federated learning approach. *Comput. Netw.* **2021**, *192*, 108122. [CrossRef]
8. Liaqat, S.; Akhunzada, A.; Shaikh, F.S.; Giannetsos, A.; Jan, M.A. SDN orchestration to combat evolving cyber threats on Internet of Medical Things (IoMT). *Comput. Commun.* **2021**, *160*, 697–705. [CrossRef]
9. Martinez, B.; Cano, C.; Vilajosana, X. A square peg in a round hole: The complex path for wireless in the manufacturing industry. *IEEE Commun. Mag.* **2019**, *57*, 109–115. [CrossRef]
10. Ferdowsi, A.; Saad, W. Deep learning for signal authentication and security in massive internet-of-things systems. *IEEE Trans. Commun.* **2018**, *67*, 1371–1387. [CrossRef]
11. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
12. Zulfiya, K.; Gulmira, B.; Altynbek, S.; Assel, O. A model and a method for assessing students' competencies in e-learning system. In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems, Dubai, United Arab Emirates, 2–5 December 2019.
13. Aceto, G.; Persico, V.; Pescapé, A. A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 3467–3501. [CrossRef]
14. Hasan, T.; Adnan, A.; Giannetsos, T.; Malik, J. Orchestrating sdn control plane towards enhanced IoT security. In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 457–464.
15. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]

16. Bibi, I.; Akhunzada, A.; Malik, J.; Ahmed, G.; Raza, M. An effective Android ransomware detection through multi-factor feature filtration and recurrent neural network. In Proceedings of the 2019 UK/China Emerging Technologies (UCET), Glasgow, UK, 21–22 August 2019; pp. 1–4.
17. Bibi, I.; Akhunzada, A.; Malik, J.; Iqbal, J.; Mussaddiq, A.; Kim, S. A dynamic DL-driven architecture to combat sophisticated Android malware. *IEEE Access* **2020**, *8*, 129600–129612. [CrossRef]
18. Schmidhuber, J. Deep learning in neural networks: An overview. *Neural Netw.* **2015**, *61*, 85–117. [CrossRef] [PubMed]
19. Hoque, N.; Bhattacharyya, D.K.; Kalita, J.K. Botnet in DDoS attacks: Trends and challenges. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2242–2270. [CrossRef]
20. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the internet of things. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1636–1675. [CrossRef]
21. Malik, J.; Akhunzada, A.; Bibi, I.; Talha, M.; Jan, M.A.; Usman, M. Security-aware data-driven intelligent transportation systems. *IEEE Sens. J.* **2020**, *21*, 15859–15866. [CrossRef]
22. Homayoun, S.; Ahmadzadeh, M.; Hashemi, S.; Dehghantanha, A.; Khayami, R. BoTShark: A deep learning approach for botnet traffic detection. In *Cyber Threat Intelligence*; Springer: Cham, Germany, 2018; pp. 137–153.
23. Malik, J.; Akhunzada, A.; Bibi, I.; Imran, M.; Musaddiq, A.; Kim, S.W. Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN. *IEEE Access* **2020**, *8*, 134695–134706. [CrossRef]
24. Dawoud, A.; Shahristani, S.; Raun, C. Deep learning and software-defined networks: Towards secure IoT architecture. *Internet Things* **2018**, *3*, 82–89. [CrossRef]
25. Bibi, I.; Akhunzada, A.; Malik, J.; Khan, M.K.; Dawood, M. Secure Distributed Mobile Volunteer Computing with Android. *ACM Trans. Internet Technol. (TOIT)* **2021**, *22*, 1–21. [CrossRef]
26. Saharkhizan, M.; Azmoodeh, A.; Dehghantanha, A.; Choo, K.K.R.; Parizi, R.M. An ensemble of deep recurrent neural networks for detecting iot cyber attacks using network traffic. *IEEE Internet Things J.* **2020**, *7*, 8852–8859. [CrossRef]
27. Parra, G.D.L.T.; Rad, P.; Choo, K.K.R.; Beebe, N. Detecting Internet of Things attacks using distributed deep learning. *J. Netw. Comput. Appl.* **2020**, *163*, 102662. [CrossRef]
28. Chen, R.; Niu, W.; Zhang, X.; Zhuo, Z.; Lv, F. An effective conversation-based botnet detection method. *Math. Probl. Eng.* **2017**, *2017*, 4934082. [CrossRef]
29. Bansal, A.; Mahapatra, S. A comparative analysis of machine learning techniques for botnet detection. In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 13–15 October 2017.
30. Pektaş, A.; Tankut, A. Deep learning to detect botnet via network flow summaries. *Neural Comput. Appl.* **2019**, *31*, 8021–8033. [CrossRef]
31. Sharma, A.; Sahay, S.K. An effective approach for classification of advanced malware with high accuracy. *arXiv* **2016**, arXiv:1606.06897.
32. Kaur, G. A novel distributed machine learning framework for semi-supervised detection of botnet attacks. In Proceedings of the 2018 Eleventh International Conference on Contemporary Computing (IC3), Noida, India, 2–4 August 2018.
33. Prokofiev, A.O.; Smirnova, Y.S.; Surov, V.A. A method to detect Internet of Things botnets. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow/St. Petersburg, Russia, 29 January–1 February 2018.
34. McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018.
35. Kudugunta, S.; Ferrara, E. Deep neural networks for bot detection. *Inf. Sci.* **2018**, *467*, 312–322. [CrossRef]
36. Vinayakumar, R.; Soman, K.P.; Poornachandran, P.; Sachin Kumar, S. Evaluating deep learning approaches to characterize and classify the DGAs at scale. *J. Intell. Fuzzy Syst.* **2018**, *34*, 1265–1276. [CrossRef]
37. Ibitoye, O.; Shafiq, O.; Matrawy, A. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019.
38. Muna, A.H.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* **2018**, *41*, 1–11.
39. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef]
40. Seide, F.; Li, G.; Yu, D. Conversational speech transcription using context-dependent deep neural networks. In Proceedings of the Twelfth Annual Conference of the International Speech Communication Association, Florence, Italy, 27–31 August 2011.
41. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baiot—Network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
42. Liu, J.; Liu, S.; Zhang, S. Detection of IoT botnet based on deep learning. In Proceedings of the 2019 Chinese Control Conference (CCC), Guangzhou, China, 27–30 July 2019.
43. Maeda, S.; Kanai, A.; Tanimoto, S.; Hatashima, T.; Ohkubo, K. A botnet detection method on SDN using deep learning. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019.
44. Nguyen, H.T.; Ngo, Q.D.; Le, V.H. IoT botnet detection approach based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018.