electronics

MDPI

Article

SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT

Danish Javeed [1], Tianhan Gao [1,*] and Muhammad Taimoor Khan [2]

[1] Software College, Northeastern University, Shenyang 110169, China; thedanishkhn@gmail.com
[2] Riphah Institute of Science and Engineering, Islamabad 44000, Pakistan; taimourkhan86@gmail.com
* Correspondence: gaoth@mail.neu.edu.cn

Abstract: The Internet of Things (IoT) has proven to be a billion-dollar industry. Despite offering numerous benefits, the prevalent nature of IoT makes it vulnerable and a possible target for the development of cyber-attacks. The diversity of the IoT, on the one hand, leads to the benefits of the integration of devices into a smart ecosystem, but the heterogeneous nature of the IoT makes it difficult to come up with a single security solution. However, the centralized intelligence and programmability of software-defined networks (SDNs) have made it possible to compose a single and effective security solution to cope with cyber threats and attacks. We present an SDN-enabled architecture leveraging hybrid deep learning detection algorithms for the efficient detection of cyber threats and attacks while considering the resource-constrained IoT devices so that no burden is placed on them. We use a state-of-the-art dataset, CICDDoS 2019, to train our algorithm. The results evaluated by this algorithm achieve high accuracy with a minimal false positive rate (FPR) and testing time. We also perform 10-fold cross-validation, proving our results to be unbiased, and compare our results with current benchmark algorithms.

Keywords: deep learning; intrusion detection; Internet of Things (IoT); software-defined network (SDN); distributed denial of service attack (DDoS)

check for updates

Citation: Javeed, D.; Gao, T.; Khan, M.T. SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT. *Electronics* **2021**, *10*, 918. https://doi.org/10.3390/electronics10080918

Academic Editor: Antonio Pescapè, Mamoun Alazab, Andrii Shalaginov

Received: 28 February 2021
Accepted: 9 April 2021
Published: 12 April 2021

1. Introduction

With the growth of the Internet and the interconnectedness between each networking device, there is a dire need for security. The evolving Internet of Things (IoT) is raising various security concerns. The Internet of Things is described as a global network of interconnected devices that are assigned unique addresses. IoT devices use sensing features and different communication protocols. They have the computational capabilities to provide services and the capacity to analyze data. Some common IoT devices include cameras, video recorders, fire sensors, doorbells, electric switches and nearly all real-time sensing devices. The Internet of Things is an ever-changing technological world. It is a paradigm that links millions of smart devices, leading to the creation of a smart environment, such as smart health systems, smart cities, smart factories, intelligent vehicular networks and smart ecosystems [1]. This means that the lack of security can pose a serious risk to the devices and the entire system. The Internet of Things comprises heterogeneous networks and networking devices that use a variety of different protocols. The dynamic characteristics of IoT devices pose various concerns in the form of cybersecurity exploits such as denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and various other kinds of malware [2–4]. Cybersecurity analysts continuously monitor networks for threat identification and repair every vulnerability; however, an attacker must only search for a single vulnerability to exploit the system. About 60% of experts spend an hour or two per day handling the network's security and operation; however, 80% of experts deal with at least one security incident in a single day [5]. With the advancement in computing and hardware technologies in recent years, cyber-physical systems have also shown rapid development. However, with the improvement and development in such areas, the variety of cyber-attacks has also grown rapidly; e.g., DoS attacks, which make the resources of the system unavailable. Replay attacks and deception attacks have also been discussed. The attack detection approaches and security controls are reviewed on the industrial level in [6]. Different types of protocol-following devices have diverse kinds of security measures that need to be followed. An integrated approach has not yet been invented to secure the complete IoT infrastructure. The traditional intrusion detection schemes are deployed, working at the infrastructure level, with firewalls or with intrusion detection and prevention systems to protect devices from attacks. However, these security measures are not sufficient when it comes to the seamless nature of IoT devices.

Software-defined network (SDN)-enabled infrastructure not only enhances the abilities of the underlying heterogeneous and dynamic environment of the Internet of Things but also provides the potential to configure and simplify network management. Thus, SDN serves as a paradigm that leverages resource-constrained devices without exhaustion as well as providing a platform to implement a security solution that does not overburden the underlying resource-constrained devices and provides an efficient and effective detection. A network's security system consists of various features such as firewalls, antivirus software and intrusion detection systems (IDSs). An IDS identifies and generates alerts about unauthorized system behavior such as use, replication, alteration and destruction. Integrating an IDS in an SDN is one of the best approaches for the surveillance of software-defined networks [7]. With the advent and viability of Artificial Intelligence procedures and the programmable features of the SDN, AI-based security solutions can be integrated into SDNs for improved security levels. There have been many AI-based techniques that have been utilized as network traffic classifiers; some of these techniques include Decision Trees, support vector machine (SVM), artificial neural networks (ANNs), Naive Bayesian, fuzzy logic, Genetic Algorithms, and K-Nearest Neighbor, which have shown ideal results with certain levels of accuracies. The need to present a flexible and robust framework has motivated us to develop a hybrid deep learning-based threat detection solution.

We developed an SDN-enabled Deep learning (DL)-driven solution for the detection of threats in the Internet of Things (IoT) environment that is cost-effective and highly scalable, as shown in Figure 1. We used a hybrid technique comprising the Cuda-Deep Neural Network Long short-term memory (CuDNNLSTM) and Cuda-Deep Neural Network Gated Recurrent Unit (CuDNNGRU) algorithms for efficient threat detection. We also implemented two algorithms for the comparison of our results: Cuda-Deep Neural Network Gated Recurrent Unit (CuDNN-GRU) and Cuda-Bidirectional Long short-term memory (CuBLSTM). Upon comparison, we found our algorithm to perform both efficiently and accurately. We used standard evaluation metrics for the evaluation of our results. The detection techniques use algorithms that are Cuda-enabled (the details of which are provided in Section 2). We used the CICDDoS2019 dataset, which is publicly available. The dataset consists of 14 different attack types, including DDoS attacks, reflection attacks, exploitation attacks and their subtypes. Details of the dataset are presented in the upcoming sections. Our proposed algorithms provide a multiclass detection approach, which to our knowledge is a novel contribution that was previously not available in the literature. We have also implemented 10-fold cross-validation, proving our results to be unbiased.

We organize the structure of our paper as follows. Section 2 consists of the background details as well as relevant work. In Section 3, the proposed architecture is given in full detail, whereas Section 4 comprises the experimental setup. We discuss the detailed results in Section 5. Section 6 of this paper presents conclusions.

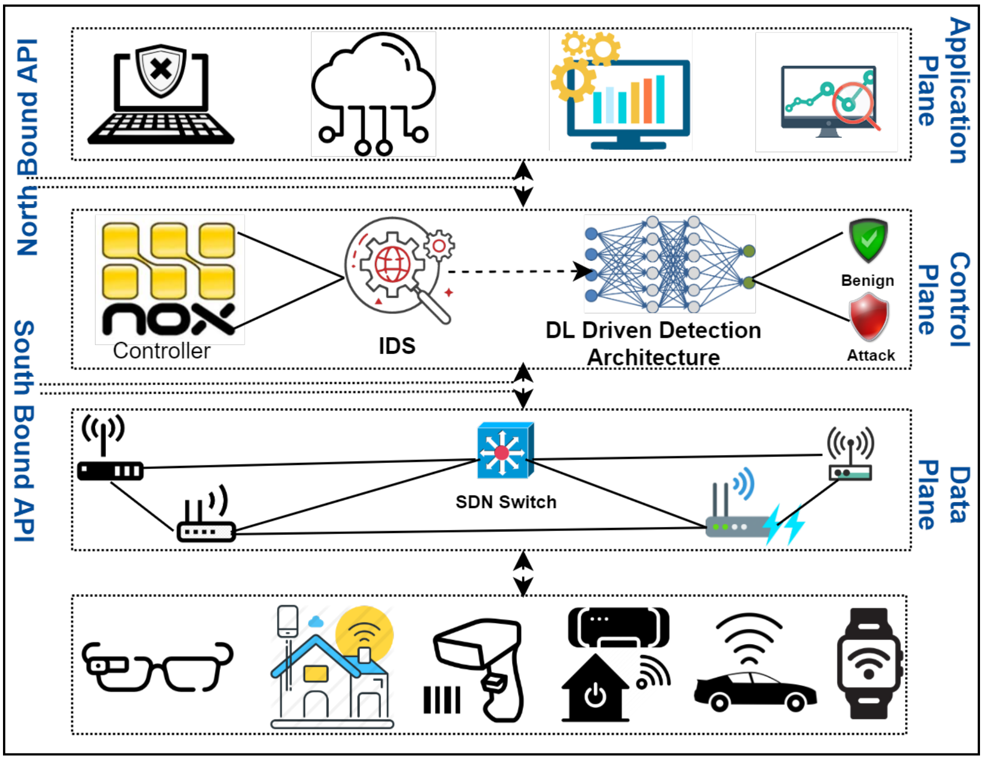


Figure 1. DL-driven software-defined network (SDN)-enabled framework. IDS: intrusion detection system.

2. Background and Related Work

2.1. Internet of Things

The Internet of Things is defined as an environment in which physical devices are integrated into the network in such a way that these objects become active participants of a business process. These objects can vary from network devices to sensors to household and health care items. These objects or devices are assigned a unique address and are together connected to the Internet. IoT contains a heterogeneous range of devices which can be wired or wireless using various kinds of protocols and can belong to different environments and networks [8]. According to recent Juniper research, it is estimated that more than 46 billion IoT devices will be in use by 2021. This consists of sensors and actuators as well as devices, demonstrating an increase of 200% compared to 2016 [9]. In any evolving paradigm of computing and networking, IoT is becoming an important component. The IoT revolution is growing enormously, resulting in immense growth in terms of monetary advantages and automation. The heterogeneous nature of IoT devices and the IoT environment brings with it a large number of challenges. These objects are designed to meet the requirements of specific user purposes, so it is difficult to come up with a common solution for all of them. As security is a prime concern in this era, achieving security for IoT devices is not simple. The diversities of these objects cannot be fit into a single protocol. Concerning the security challenges faced in the IoT environment, some real-time cybersecurity threats that are scanned for by antivirus software are specified. Symantec verified the presence of one of the first pieces of malware in IoT, Linux and Darlloz. Scanning the IoT devices in real-time for threat detection may result in a very unaffordable overhead.

Here, we introduce software-defined networks (SDN), the aim of which is to focus on network programmability. The control plane is separated from the data plane, giving the data plane merely the job of data forwarding. The control plane is in charge of all the decision-making for the entire network. By coming up with an SDN-based approach, we obtain a solution that can be applied to heterogeneous IoT devices. Therefore, in terms of its feasible real-world implementations, SDN guarantees a promising future for IoTs.

2.2. *Software-Defined Network Architecture*

Software-defined networking appears to be the most promising future networking framework. SDN consists of three layers: application, control and the data plane and corresponding north and south-bound APIs. The advent of the SDN paradigm has broken network management down to vendor-independent architecture through network programmability [10]. The separation of the control plane and data plane has led to the emergence of SDNs as a new networking paradigm. The novel and promising framework of SDN has shifted the entire control logic to a centralized control plane. Thus, the power and capability of SDNs lie in their centralized controlled architecture and intelligence. An SDN controller gathers insights (statistics) from the network elements by using the south-bound protocol. The south-bound protocol is the most important protocol of the SDN architecture and is responsible for the exchange of information between the controller and the networking devices [11]. One of the most important south-bound protocols is OpenFlow, which is a standard communication interface created by the Open Networking Foundation (ONF) and is characterized by the data and control planes of an SDN framework. This interface permits direct access to and manipulation of the forwarding plane of network devices such as routers and switches, thus enabling direct access as well as the control of the devices of the forwarding plane [12]. The SDN controller communicates with the switch through the south-bound API, where OpenFlow is the most used standard. Some other proposals are NOS, RYU and P4. There are multiple open software available for the NOS platform; i.e., Floodlight, POX, etc. SDN applications have the ability to program the network by using the north-bound API of the NOS [13]. OpenFlow comprises flow tables and activities that advise the switch how to process these flows and channels; as a result, the switch becomes associated with the controller, and in turn, the OpenFlow protocol is utilized by enabling the packets to be transmitted between a switch and the controller. A controller can view the entire network and govern all policies and decisions [14]. There are some appropriate concerns about the scalability of SDN; however, the limitations of scalability are not restricted to SDN only. The same challenges are also faced by the traditional control protocol design. Thus, we need to worry about the scalability issues in traditional networks instead of worrying about SDN. To preserve the scalability of SDN, control applications should be designed with the weakest level of consistency. In a typical data center, the switching elements can grow rapidly. This high amount of change in the control events generated in the network is enough to overload the centralized controller. One of the ways to avoid this problem is to install rules on the switches that result in the elimination of the control requests before they enter the control plane [15]. SDN faces a severe burden regarding the huge amount of control channel traffic because this may result in the increased delay of control messages. The programmable network virtualization based on SDN plays an important role in accommodating diverse services in cloud infrastructure [16]. The dynamic provisioning of virtual security functions enhances the scalability in the edge of networks to deal with the huge amount of traffic in the IoT. However, SDN plays a vital role in the dynamic reconfiguration of the network and provides new rules of networking on demand. The SDN has been proven to be a powerful and flexible enabler for network solutions. It plays a vital role in enhancing control decisions; in addition, SDN-based solutions provide scalability, dynamism, flexibility and centralized management [17]. The control plane of SDN is entirely programmable and can thus modify numerous functionalities. It can extend many networks on its data plane; e.g., edge, fog, vehicular networks and the Internet of Things [18–20].

2.3. *Related Work*

Deep learning has shown tremendous results in many fields of computer science. In [7], a network intrusion detection model is proposed that uses CNN. The raw data traffic is converted into image data format in real-time. By converting data to image format, the number of computation parameters was reduced, yielding improved results. In [21], the author used a seven-layered CNN network to train the dataset. A hierarchal Intrusion detection system is anticipated for SDNs in [22] which is trained on the Defense Advanced Research Projects Agency (DARPA) intrusion detection dataset using SVM. It combined the benefits of flow and packet-based IDSs to provide a high detection rate without affecting the network's performance. The authors in [23] used recurrent neural network (RNN) techniques to identify attacks and categorize them. A performance comparison was made of the RNN-based techniques and the non-RNN techniques. A network threat analysis strategy combined with long short-term memory (LSTM) is presented in [24]. To preserve the attack feature of input data, LSTM is presented to produce classifiers that categorize the attacks from the normal traffic. In [25], an RNN-based anomaly detection system is presented that, apart from capturing anomalies, generates flows to enable the network's dynamic access control.

Finding DDoS attacks in an SDN environment is carried out by using an advanced SVM algorithm, as given in [26]; the system is validated by using the Hierarchical Task Analysis method, which authenticates human errors to achieve certain results. The trending machine learning schemes—e.g., deep learning and hybrid AI techniques—provide greatly improved results compared to the conventional machine learning approaches. AI-based techniques have been found to be very beneficial when integrated with SDN architecture [27]. The author in [28] discussed numerous cyber-attacks and their detection strategies. The author proposed an embedded programming approach for the detection of denial of service attacks. Besides, the software engineering approach and AI techniques can enhance the detection strategies as they can detect zero-day attacks. Artificial intelligence has played an essential role in intrusion detection systems in recent years. In [29], the authors propose the Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System (RTS-DELM-CSIDS) security model. The proposed model first defines the relevance of security aspects by ranking them and establishes a robust intrusion detection system based on the most relevant ones. The proposed approach had an accuracy of 96.22% in training and 92.73% in validation. The authors in [30] combined the features of a traffic flow and the power system's inherent physical laws to detect lousy data injection in smart grids. The generalized detection model focuses on identical characteristics to ensure the accuracy of unknown datasets and reduce the computational time. The results show an increase in the detection rate by 20% on average over the Chi-square test; furthermore, the approach filters the majority of Snort false alarms and solves the Security-Oriented Cyber-Physical State Estimation (SCPSE) observability problem. Deep learning techniques have been implemented to develop an anomaly-based network intrusion detection system, and the fully connected neural network model demonstrates desired outcomes with an advanced accuracy compared to previous techniques such as SVM, Random Forest and Adaboost [31]. CNN and LSTM-based detection systems are used to detect adversarial attacks in SDNs [32].

The deep learning approach has proved to have a great potential for the detection of malevolent activities. The deep learning-based GRU-LSTM (gated recurrent unit–long short-term memory) model is implemented in an SDN environment for the detection of network-based intrusions [33]. In [34], the proposed intelligent attack detection model is proved to be efficacious in terms of achieving state-of-the-art performance, with notably less time consumption than many existing models. Deep autoencoders are used in [35] to analyze the reconstruction error for the network's traffic records. Deep autoencoder and big data visualization techniques are used along with statistical analysis methods for vulnerability detection in [36]. In [37], the authors propose a hybrid detection system for the detection of cyber threats based on Spark machine learning and convolutional LSTM. They achieved an accuracy of 97.29% using the ISCXUNB dataset. The authors of [38] came up with a hybrid Intrusion detection scheme that combined the genetic algorithm along with the deep belief network for the detection of cyber threats, achieving an accuracy of 99%. In [39] a technique for the detection of malicious attacks in industrial IoTs is presented, leveraging deep autoencoders and deep forward neural networks and achieving a detection accuracy of about 99%. The authors in [40] present a machine learning-based attack detection approach in order to recognize significant threats in the IoT. The detection model consists of a hybrid technique implementing One Class Support Vector Machines (OCSVM), Self-organizing map (SOM), Gaussian Mixture Modelling (GMM) and Isolation Forest with a detection accuracy of 98%. The authors in [41] focus on creating an ensemble-based GRU model and LSTM for efficient attack detection. The model achieved 99% detection accuracy for attack detection in the IoT under the Message Queuing Telemetry Transport MQTT protocol. The authors of [42] implemented a bio-inspired intrusion detection system for crossfire attacks. An average 80% detection rate was achieved with the proposed architecture. The study in [43] presented a deep learning-based cybersecurity architecture to identify threats in IoT networks. An accuracy of 95.5% was accomplished by this model, alongside a low false-positive rate. The nature of IoT traffic is comparatively different than other network types, as shown in [44], in which a Random Forest-based supervised machine learning algorithm is implemented which uses features extracted from the IoT traffic to identify the types of devices from the whitelist. In [45], the authors proposed a two-stage hierarchical network intrusion detection (H2ID) approach. The model achieves anomaly detection through a unique lightweight solution based on a multimodal deep autoencoder (M2-DAE), as well as attack classification, using soft-output classifiers. The research employed and validated the proposed model using the latest and up-to-date Bot-IoT dataset, containing four diverse attacks (i.e., DoS, Theft, Scan and DDoS), including unknown attacks. The proposed model is appropriate for privacy-preserving and distributed deployments. The authors in [46] presented an SDN-enabled hybrid deep learning technique in order to identify bots in the Internet of Medical Things. They implemented a hybrid of CNN and CuDNNLSTM algorithms for threat detection. The authors in [47] used CNNLSTM algorithm for gesture recognition. The authors proposed that the frame-level classification of CNNLSTM is consistent with the cognitive perception of gestures.

3. Methodology

This section presents the complete methodology of the proposed work; i.e., the proposed network model, hybrid deep learning detection scheme and dataset description.

3.1. Proposed Network Model

SDN has been evolving as a technology of integrated network design in recent years. The data and control plane are separated in SDN's design, which allows improvements in areas such as simplification and flexibility. Furthermore, in the conventional design, every router in the network can only see the local state of the network; the lack of an overview of the complete network makes it complicated to autonomously produce a good potential defense approach compared to attacks. Instead, SDN has a global view of the network and central control functions, simplifying the gathering of network statistics. Besides this, the SDN proposes a separate way to reduce the risk of DDoS attacks; however, using SDN features and intelligent regulation to mitigate DDoS attacks remains a problematic issue.

We came up with an SDN-enabled DL-driven solution for the detection of threats in the Internet of Things (IoT) environment, as shown in Figure 1. The proposed framework comprises the application plane, control plane and data plane. The application plane is designed to run various applications to provide multiple services to the end-users. However, the application mechanisms are controlled by the control plane of the SDN to manage routing decisions, data transfers and traffic monitoring. The proposed framework is a part of the control plane. The SDN controller in the control plane is programmed to manage the whole network. The SDN controller is a central decision-maker and primary source of centralized control intelligence. The reasons behind putting the proposed model in the control plane are as follows: firstly, it is entirely programmable and can thus modify functionalities—it is capable of extending many networks on its data plane and provides solutions for heterogeneity between the linked IoT devices and SDN controller through open-flow switches; secondly, it can simply leverage the underlying IoT devices without exhaustion, making it an appropriate revolution for IoT. The proposed SDN-enabled DL-driven framework is cost-effective, as it is customized and centralized. The integration of IoT and SDN offers an exact solution for network traffic inspection to identify attacks and suspicious activities. All the decisions for underlying devices and networks occur here because the global network view is maintained here. Further, we have a data plane that comprises various IoT devices, sensors, smart devices and wireless technologies. The IoT can be extended at the data plane by the SDN control plane. Moreover, the implemented module can also be customized and can form a part of other SDN commercial controllers.

3.2. Proposed Hybrid Detection Scheme

A hybrid deep learning technique for efficient threat detection in an IoT environment that comprises CuDNNLSTM and CuDNNGRU is proposed. The hybrid intrusion detection model is placed on the programmable control plane of the SDN. The schematic representation of our detection module is shown in Figure 2. We trained and tested our system on hybrid algorithms with a reduced number of false positives, resulting in greater detection accuracy. The proposed model comprises multiple layers. DNNLSTM consists of two layers with a combination of 500 and 300 neurons. Further, we have added one layer of DNNGRU with 200 neurons. For all the layers except the output layer, we have used Relu as the activation function. However, Softmax is used in the output layer. The experiments were performed until 10 epochs were reached with 32 batch sizes to achieve efficient results. We have used the Keras framework for Python with the TensorFlow backend. This uses GPU processing and a Cuda-enabled version for improved performance. The complexity of recurrent neural network optimization emerges from the reliance of state computation on time. In RNNs—i.e., GRU and LSTM—the calculation of each step is delayed until the preceding step is complete. The dependencies of the RNNs limit their performance, resulting in a reduction of speed. This nature of the RNN architecture limits their applicability. CuDNN is a GPU-augmented library that allows multithreading, leading it to be quick and easy for high sequence modeling-capacity LSTM networks. Different memory blocks are recurrently connected and make LSTM layers, giving the model the ability to forget the old states and replace them with new information so that the system can learn to its maximum capability. In backpropagation, LSTM is widely used to solve the problem of gradient descent as well as for the predictions of time series. However, LSTM uses gating mechanisms for long-term dependency that enhance the flow of information. Furthermore, the quick multiplication of matrixes enhances the overall performance and is also carried out by LSTM. CuDNNLSTM can solve the sequential dependence problems of BasicLSTMCell [48]. A comprehensive architecture of the proposed hybrid deep learning model is shown in Table 1.

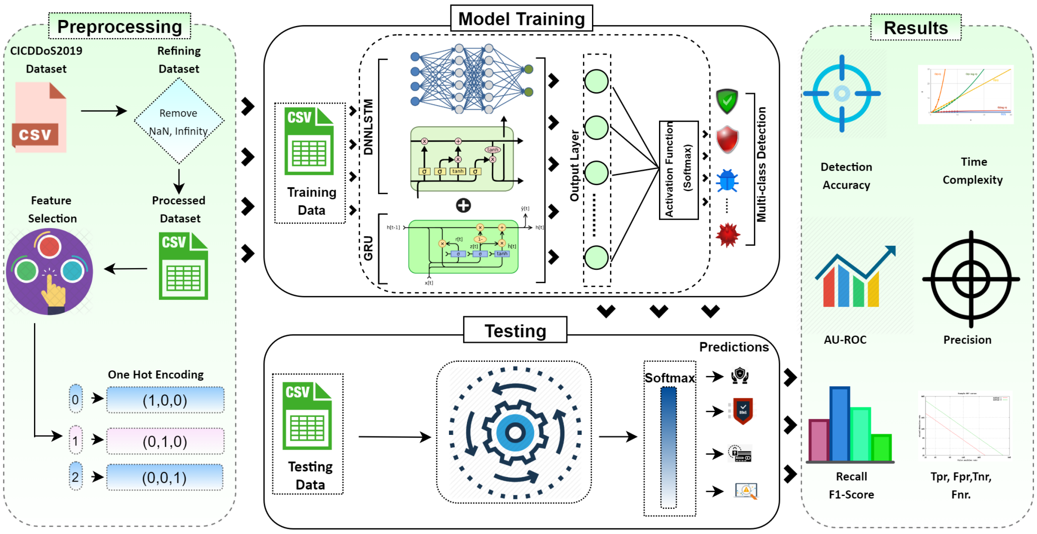


Figure 2. DL-driven SDN-enabled framework.

Table 1. Description of hybrid DL algorithms.

Algorithm	Layers	Neurons/Kernel	AF/LF	Epochs	Optimizer	Batch-Size
Cu-DNNLSTM + Cu-DNNGRU	Cu-DNNLSTM (2)	500, 300	Relu/CC-E	10	Adamax	32
	Cu-DNNGRU (1)	200	Relu/CC-E			
	Dropout		-			
	Dense (3)	200, 100, 50	-			
	Output Layer (1)	09	Softmax			
Cu-DNN-GRU	Cu-DNNGRU (3)	500, 300, 200	Relu/CC-E	10	Adamax	32
	Dropout		-			
	Dense (3)	200, 100, 50	-			
	Output Layer (1)	09	Softmax			
Cu-BLSTM	Cu-BLSTM (3)	500, 300, 200	Relu/CC-E	10	Adamax	32
	Dropout		-			
	Dense (3)	200, 100, 50	-			
	Output Layer (1)	09	Softmax			

3.3. Dataset Description

The selection of a suitable dataset makes an essential contribution to the evaluation of the efficiency of an intrusion detection system. In the literature, researchers have employed various datasets, some of which include KDD99, KDD CUP, NSLKDD, UNSWNB15, CICIDS 2017 and several others for intrusion detection in IoTs. These datasets lack IoT-supportive features. Some hackers create/use webpages that scan for local IoT devices in order to take control of them. The hacker can use domain name system (DNS) rebinding as well as malicious scripts to discover and attack local IoT devices to take control of them [49]. That is the reason that we have selected a state-of-the-art dataset, CICDDoS 2019 [50]. The dataset chosen is based on a set of network flow features. The dataset is publicly available and is multiclass. The dataset consists of 78,283 instances, among which 66,510 are benign and 11,773 are instances of attacks. Our selected dataset consists of more than 80 traffic features and the most up-to-date and common attacks, which include DDoS, refection and exploitation attacks and some subtypes of these. The proposed work is only concerned with eight attacks. Table 2 shows the attack types and related information in detail. The main reason for choosing this dataset is to focus on the detection of attacks that lead to system exploitation.

Table 2. Data set description. DoS: denial of service; DDoS: distributed denial of service; TCP: transmission control protocol; UDP: user datagram protocol.

Classes	Category	Sub-Category	Numbers
Benign	-	-	66,510
DrDoS_MSSQL	Reflection	TCP based	1497
DrDoS_SSDP		TCP based	1482
DR DoS		UDP based	1481
WebDDoS		TCP/UDP based	1469
PORTMAP		TCP/UDP based	1500
SYN	Exploitation	TCP based	1451
DrDoS_UDP		UDP based	1469
UDP-Lag		UDP based	1424
Total			78,283

4. Experimental Setup

Using Keras, we trained the proposed deep learning models with a version of Python, "Python 3.8". Furthermore, our PC server was assembled with TensorFlow and the CuDNN library based on the GPU to allow parallel processing. The experimental evaluations were done on a PC server equipped with Intel, Core i7-7700 HQ CPU @ 2.80 GHz processor, 16 GB of RAM and a 6 GB Nvidia GeForce 1060 graphics card.

Evaluation Metrics

To perform a thorough evaluation of the performance, standard evaluation metrics were implemented, including precision, recall, accuracy and F1-score. Moreover, true positive, true negative, false positive, Matthews correlation coefficient (MCC) and false negative values were calculated with a confusion matrix.

5. Result And Discussion

The outcomes from the complete assessment of the proposed technique of hybrid CuDNNLSTM and CuDNNGRU are presented here. For comparison with the benchmarks, we have compared the proposed model with Cu-DNN and Cu-BLSTM as well as the state-of-the-art hybrid Cuda-enabled deep learning detection techniques. To thoroughly illustrate the unbiased outcomes, 10-fold cross-validation was employed, as shown in Table 3. Average 10-fold results for the evaluation metrics were collected and are accordingly presented in various parts of this work.

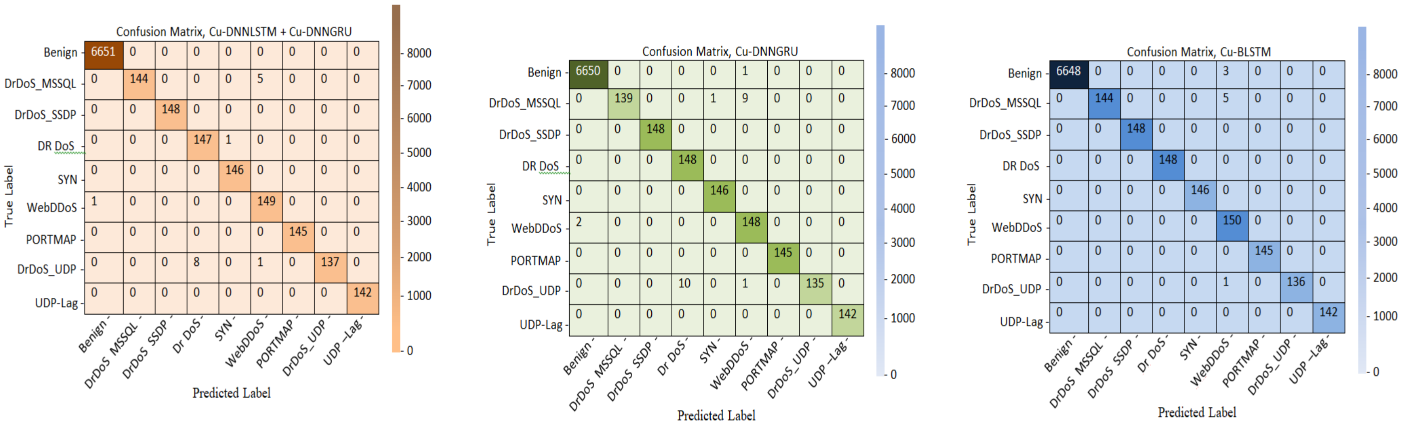
Table 3. Result of 10-fold cross-validation.

Folds	Accuracy %			F1-Score %			Recall %			Precision %		
	$$	##	&&	$$	##	&&	$$	##	&&	$$	##	&&
1	99.77	99.77	99.78	99.81	99.81	99.83	99.81	99.81	99.83	99.90	99.90	99.90
2	99.79	99.55	99.75	99.84	**99.85**	99.73	99.84	99.58	99.73	99.90	99.89	**99.98**
3	99.79	99.43	99.65	**99.87**	99.83	99.72	99.87	**99.83**	99.72	99.89	99.50	99.86
4	99.82	99.40	99.11	99.86	99.34	99.53	99.86	99.34	99.53	99.92	99.96	99.43
5	99.61	99.71	99.79	99.61	99.83	99.81	99.61	99.83	99.81	99.93	99.83	99.93
6	99.70	99.75	99.52	99.78	99.77	99.61	99.78	99.77	99.61	99.86	99.93	99.83
7	99.78	**99.79**	99.62	99.80	99.83	99.71	99.80	99.83	99.71	99.93	99.92	99.84
8	**99.87**	99.41	**99.85**	99.87	99.74	99.90	**99.87**	99.74	**99.90**	**99.96**	99.56	99.92
9	99.64	99.70	99.52	99.68	99.65	99.76	99.68	99.65	99.76	99.89	**100**	99.68
10	99.68	99.64	99.76	99.80	99.67	**99.84**	99.80	99.67	99.84	99.81	99.90	99.87

$$ = Cu-DNNLSTM + Cu-DNNGRU. ## = Cu-DNN-GRU. && = Cu-BLSTM.

5.1. Confusion Matrix Analysis

A confusion matrix shows the performance of the classification model on a set of test data. It is represented for either binary or multiclass data. It is beneficial for measuring accuracy, precision, recall and the receiver operating characteristic (ROC) curve. As shown in Figure 3, the proposed model identifies the nine different classes correctly.



Confusion Matrix, Cu-DNNLSTM + Cu-DNNGRU

	Benign	DrDoS MSSQL	DrDoS SSDP	Dr DoS	SYN	WebDDoS	PORTMAP	DrDoS_UDP	UDP –Lag
Benign	6651	0	0	0	0	0	0	0	0
DrDoS_MSSQL	0	144	0	0	0	5	0	0	0
DrDoS_SSDP	0	0	148	0	0	0	0	0	0
DR DoS	0	0	0	147	1	0	0	0	0
SYN	0	0	0	0	146	0	0	0	0
WebDDoS	1	0	0	0	0	149	0	0	0
PORTMAP	0	0	0	0	0	0	145	0	0
DrDoS_UDP	0	0	0	8	0	1	0	137	0
UDP-Lag	0	0	0	0	0	0	0	0	142

(**a**) Hybrid Cu-DNNLSTM and Cu-DNNGRU.

Confusion Matrix, Cu-DNNGRU

	Benign	DrDoS MSSQL	DrDoS SSDP	Dr DoS	SYN	WebDDoS	PORTMAP	DrDoS_UDP	UDP –Lag
Benign	6650	0	0	0	0	1	0	0	0
DrDoS_MSSQL	0	139	0	0	1	9	0	0	0
DrDoS_SSDP	0	0	148	0	0	0	0	0	0
DR DoS	0	0	0	148	0	0	0	0	0
SYN	0	0	0	0	146	0	0	0	0
WebDDoS	2	0	0	0	0	148	0	0	0
PORTMAP	0	0	0	0	0	0	145	0	0
DrDoS_UDP	0	0	0	10	0	1	0	135	0
UDP-Lag	0	0	0	0	0	0	0	0	142

(**b**) Hybrid Cu-DNNGRU.

Confusion Matrix, Cu-BLSTM

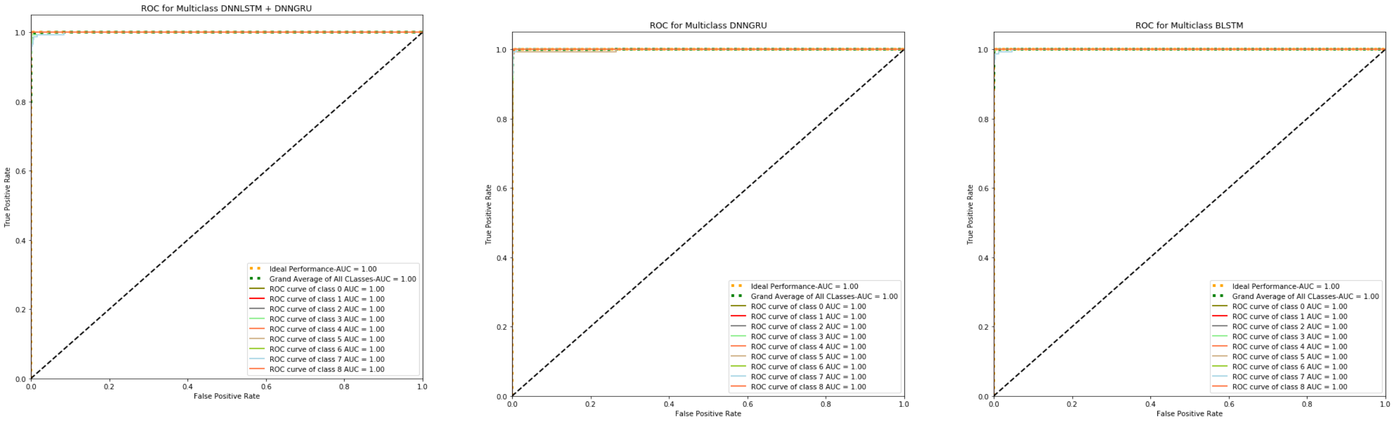
	Benign	DrDoS MSSQL	DrDoS SSDP	Dr DoS	SYN	WebDDoS	PORTMAP	DrDoS_UDP	UDP –Lag
Benign	6648	0	0	0	0	3	0	0	0
DrDoS_MSSQL	0	144	0	0	0	5	0	0	0
DrDoS_SSDP	0	0	148	0	0	0	0	0	0
DR DoS	0	0	0	148	0	0	0	0	0
SYN	0	0	0	0	146	0	0	0	0
WebDDoS	0	0	0	0	0	150	0	0	0
PORTMAP	0	0	0	0	0	0	145	0	0
DrDoS_UDP	0	0	0	0	0	1	0	136	0
UDP-Lag	0	0	0	0	0	0	0	0	142

(**c**) Cu-BLSTM.

Figure 3. Confusion metrics.

5.2. ROC Curve Analysis

The ROC curve plots the visualized outcomes in order to compare the false positive and true positive rates. The degree of separability primarily shows the performance of multi-class classification issues, which is shown by the ROC. The plot of the ROC curve is between the TP rate and the FP rate. Figure 4 represents the ROC of our proposed model, which shows that our proposed model exhibits better performance in comparison to the other architectures.



(**a**) Hybrid Cu-DNNLSTM and Cu-DNNGRU.

(**b**) Hybrid Cu-DNNGRU.

(**c**) Cu-BLSTM.

Figure 4. ROC Curves.

5.3. Accuracy, Precision, Recall and F1-Score

Accuracy is characterized as the percentage of true labeled records. The detection accuracy also indicates the efficiency of an algorithm and its performance analysis. We have calculated the percentage of accuracy to create the graphs. The detection accuracy of the hybrid detection algorithms on the testing data is given in Figure 5. The proposed model outclassed the Cu-DNNGRU and Cu-BLSTM with a detection accuracy of 99.74% and a precision of 99.89%. Precision, also known as the positive predicted value (PPV), indicates the number of correctly identified records. The TPR, also known as recall, indicates the amount of accurately predicted records out of the total data. The F1-score characterizes the harmonic mean of the recall and precision. The recall and F1-score of the proposed algorithms are both 99.79%.

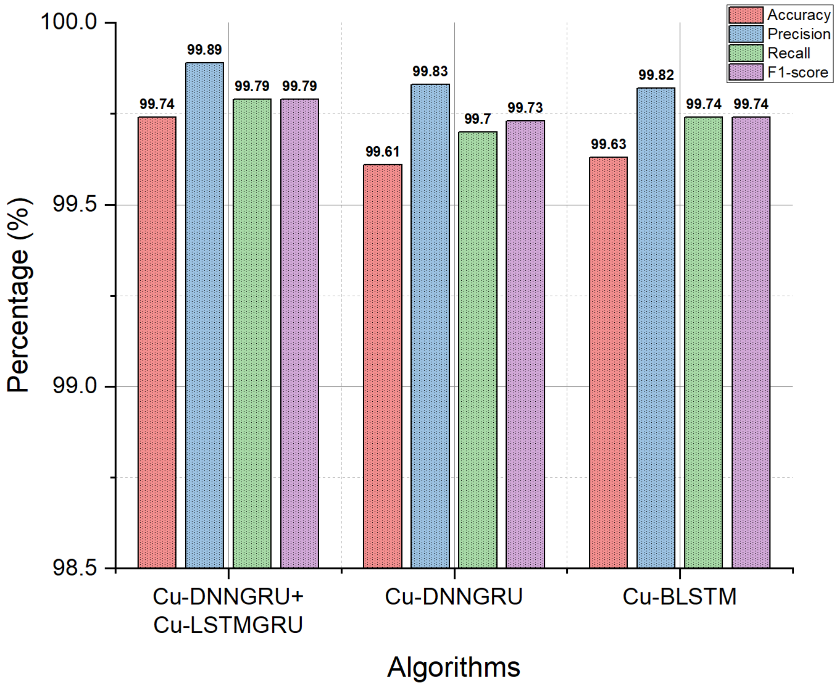


Figure 5. Accuracy, precision, recall and F1-score.

5.4. FPR, FDR, FNR and FOR Analysis

We have further estimated other performance evaluation measures for a better estimation of our proposed work, which are the false positive rate (FPR), false discovery rate

(FDR), false omission rate (FOR) and false negative rate (FNR). Figure 6 shows that our proposed model shows imporved rates of FPR, FDR, FNR and FOR of 0.528, 0.091, 0.198, and 1.138%. Further, Cu-BLSTM shows better results than Cu-DNNGRU.

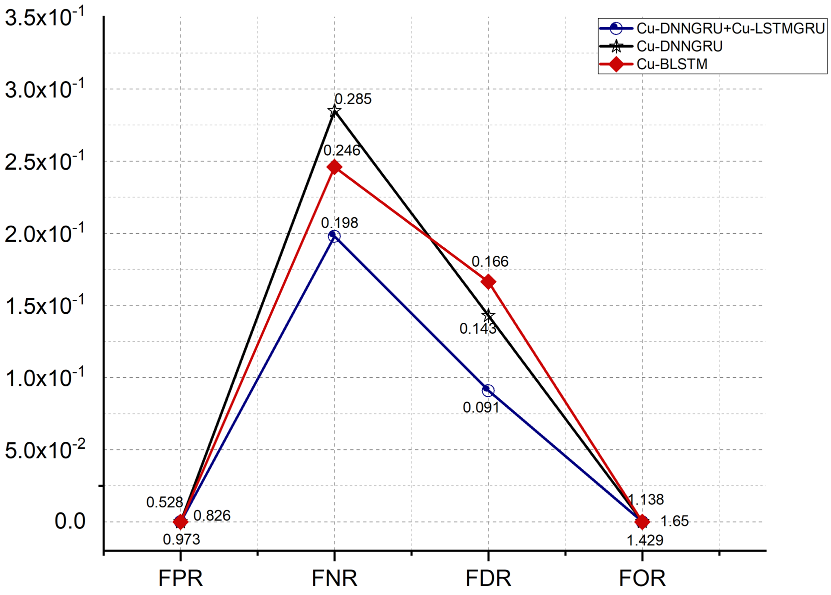


Figure 6. False positive rate (FPR), false negative rate (FNR), false discovery rate (FDR) and false omission rate (FOR).

5.5. TPR, TNR, MCC Analysis

An uncertainty matrix was used to get the values of TPR, TNR and MCC in order to perform a detailed evaluation as well as analysis. The proposed work calculated the classes from the confusion matrix. It is obvious that our proposed mechanism exhibited better TPR, TNR, and MCC outcomes. Figure 7 represents the TPR, TNR and MCC scores.

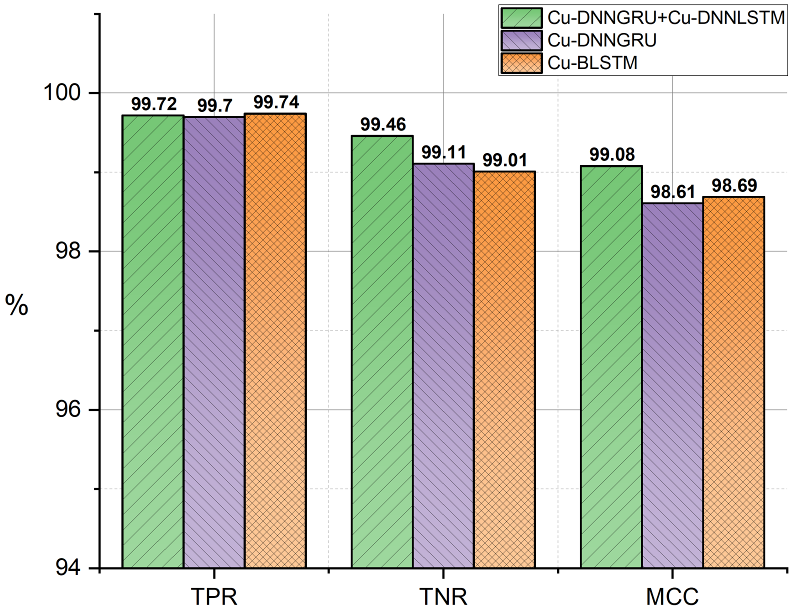


Figure 7. True positive rate (TPR), True Negative rate (TNR) and Matthews correlation coefficient (MCC).

5.6. Training Time and Testing Time

Figure 8 indicates the testing time and training time of the proposed implemented models, as well as the comparison of the time taken by each of the algorithms in the testing and training phase, respectively. The proposed model shows a better testing time of only 9.33 ms.

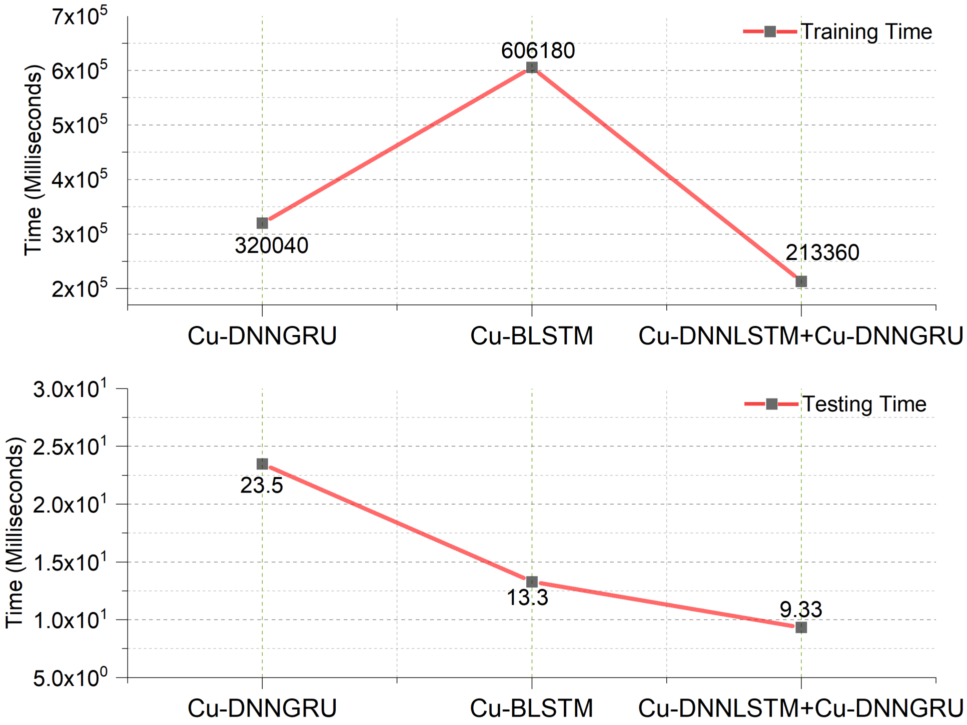


Figure 8. Training and testing time.

5.7. Comparison of Proposed Hybrid Technique with Hybrid DL Algorithm with CuBLSTM, CuDNNGRU

We developed a hybrid detection algorithm and implemented it on the dataset. Our detection scheme—i.e., hybrid CuDNNLSTM and CuDNNGRU—performed best in terms of all the considered evaluation metrics. We implemented CuBLSTM and CuDNNGRU as comparison algorithms on the same dataset, comparing the same evaluation metrics. The proposed hybrid algorithm gave the best results with a comparatively low testing time.

5.8. Comparison with Benchmark Algorithms

We compared our proposed algorithm with the current benchmarks. We evaluated the algorithms in terms of a comparison of some considered parameters. In [33], the NSL-KDD dataset was used for the detection leveraging of GRU-LSTM as a detection module, achieving an average accuracy of 87.90%, with a precision, recall and F1-score of 83.50, 77.90 and 80.60%, respectively. In [51], a hybrid DL detection scheme was made leveraging Cu(LSTM-CNN), which achieved an average detection accuracy of 98.60%, along with a precision of 99.37%, recall of 99.35% and F1-score of 99.35%. The algorithm had a testing time of 296 ms using the CICDDOS 2017 dataset. In [52], a hybrid detection framework was used, achieving an average detection accuracy of 98% with a precision of 91%. The proposed model showed an accuracy of 99.74% with a precision of 99.89%, with a recall and F1-score of 99.79% as shown in Table 4. The testing time of the proposed work was only 9.33 ms, which was less than the current benchmarks.

Table 4. Comparison with current benchmarks. GRU-LSTM: gated recurrent unit–long short-term memory.

Schemes	[33]	[51]	[52]	**Proposed Work**
Dataset	NSL-KDD	CICIDS2017	CICDDoS2019	CICDDoS2019
Algorithm	GRU-LSTM	Cu (LSTM-CNN)	Autoencoder (EDSA)	CuDNNLSTM + CuDNNGRU
System Specification	i5, 3.2 GHz, Nvidia GTX 1070	i9, 4.0 GHz, Nvidia GTX 1080	- -	i7, 2.8 GHz, Nvidia Geforce 1060 DDR5
Cuda enabled	-	✓	-	✓
10 fold	-	✓	-	✓
Multi-class	-	✓	-	✓
Accuracy (%)	87.90	98.60	98	99.74
Precision (%)	83.50	99.37	91	99.89
Recall (%)	77.90	99.35	-	99.79
F1-Score	80.60	99.35	-	99.79
Testing time	-	296 (ms)	-	9.33 (ms)
Evaluation metrics	-	✓	-	✓

5.9. Speed Efficiency

The suggested hybrid deep learning model was analyzed regarding the total time taken. The two phases of analysis consisted of the training and testing phase, respectively. Training time is usually not considered as the training phase is done offline. However, the testing phase is of prime importance as the testing time truly depicts the efficiency and the performance of the model. Figure 8 of our paper shows the testing time of our model, which was only 9.33 ms, which means that the hybrid CuDNNLSTM and CuDNNGRU showed the best testing time and was computationally efficient. The confidence intervals of the testing times of Cu-DNNLSTM and CuDNNGRU, CuBLSTM and CuDNNGRU are shown in Figure 9. The proposed work used a 95% confidence interval.

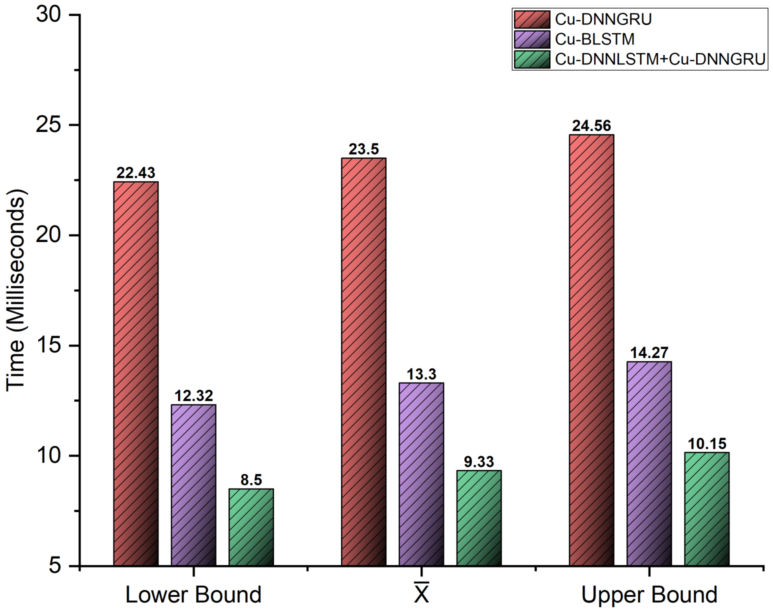


Figure 9. Confidence intervals of testing time.

6. Conclusions

With the advent of IoT, the risk of cyber-attacks has also increased to a great extent. As the IoT includes resource-constrained devices and the security of these devices is not an inbuilt feature, securing these devices is important. Traditional security mechanisms cannot be deployed immediately for their security due to the heterogeneous nature of these devices. Thus, the SDN paradigm is a promising solution to the securing of IoT infrastructure. This paper proposed a novel SDN-enabled hybrid DL-driven threat detection system for the IoT to fight advanced multivector cyber-attacks. Our proposed framework is a scalable, efficient and accurate solution. The proposed model obtains a detection accuracy of 99.74%. A comprehensive evaluation of the model is performed along with the evaluation of standard evaluation metrics, and we have made a comparison with the current benchmarks. The proposed mechanism of hybrid CuDNNLSTM and CuDNNGRU out-performs all benchmarks with regards to detection accuracy, precision and speed efficiency. Furthermore, the computational complexity of the proposed work is very low. The results of two Cuda-enabled algorithms—i.e., CuDNNGRU and CuBLSTM—were also compared to the proposed algorithm by implementing them on the same dataset, and their achieved results were beaten by the proposed hybrid algorithm. In the future, we aim to implement other deep learning classifiers to detect emerging cyber threats. In conclusion, the proposed work endorses the DL-driven framework for IoT ecosystems.

Author Contributions: Conceptualization, D.J.; methodology, D.J.; writing—original draft preparation, D.J.; writing—review and editing, T.G.; validation and formal analysis, M.T.K.; supervision, T.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by China Fundamental Research Funds for the Central 321 Universities under Grant Number N2017003 and Grant Number N182808003.

Acknowledgments: We thank the China Fundamental Research Funds for the Central 321 Universities under Grant Number N2017003 and Grant Number N182808003.

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

References

1. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. [CrossRef]
2. Bhunia, S.S.; Gurusamy, M. Dynamic attack detection and mitigation in IoT using SDN. In Proceedings of the 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6.
3. Ferdowsi, A.; Saad, W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. *IEEE Trans. Commun.* **2019**, *67*, 1371–1387. [CrossRef]
4. Haller, S.; Karnouskos, S.; Schroth, C. The internet of things in an enterprise context. In *Future Internet Symposium*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 14–28.
5. Ben-Asher, N.; Gonzalez, C. Effects of cybersecurity knowledge on attack detection. *Comput. Hum. Behav.* **2015**, *48*, 51–61. [CrossRef]
6. Ding, D.; Qing-Long, H.; Yang, X.; Xiaohua, G.; Xian-Ming, Z. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
7. Wu, K.; Chen, Z.; Li, W. A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks. *IEEE Access* **2018**, *6*, 50850–50859. [CrossRef]
8. Ren, W.; Sun, Y.; Luo, H.; Guizani, M. A Novel Control Plane Optimization Strategy for Important Nodes in SDN-IoT Networks. *IEEE Internet Things J.* **2019**, *6*, 3558–3571. [CrossRef]
9. Ojo, M.; Adami, D.; Giordano, S. A SDN-IoT architecture with NFV implementation. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
10. Ujjan, R.M.A.; Pervez, Z.; Dahal, K. Suspicious Traffic Detection in SDN with Collaborative Techniques of Snort and Deep Neural Networks. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications, Exeter, UK, 28–30 June 2018; pp. 915–920.
11. Wang, L.; Lu, Y. A Survey of Network Measurement in Software-Defined Networking. In *International Conference on Network, Communication, Computer Engineering (NCCE 2018)*; Atlantis Press: Dordrecht, The Netherlands, 2018.
12. Modieginyane, K.M.; Letswamotse, B.B.; Malekian, R.; Abu-Mahfouz, A.M. Software defined wireless sensor networks application opportunities for efficient network management: A survey. *Comput. Electr. Eng.* **2018**, *66*, 274–287. [CrossRef]
13. Megyes, P.; Alessio, B.; Giuseppe, A.; Antonio, P.; Sándor, M. Challenges and solution for measuring available bandwidth in software defined networks. *Comput. Commun.* **2017**, *99*, 48–61. [CrossRef]
14. Kim, H.; Feamster, N. Improving network management with software defined networking. *IEEE Commun. Mag.* **2013**, *51*, 114–119. [CrossRef]
15. Yeganeh, S.H.; Amin, T.; Yashar, G. On scalability of software-defined networking. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [CrossRef]
16. Yang, G.; Bong-yeol, Y.; Wontae, J.; Chuck, Y. FlowVirt: Flow rule virtualization for dynamic scalability of programmable network virtualization. In Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 350–358.
17. Molina Zarca, A.; Garcia-Carrillo, D.; Bernal Bernabe, J.; Ortiz, J.; Marin-Perez, R.; Skarmeta, A. Enabling virtual AAA management in SDN-based IoT networks. *Sensors* **2019**, *19*, 295. [CrossRef]

18. Al-Rubaye, S.; Kadhum, E.; Ni, Q.; Anpalagan, A. Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency. *IEEE Internet Things J.* **2019**, *6*, 267–277. [CrossRef]
19. Chaudhary, R.; Aujla, G.S.; Garg, S.; Kumar, N.; Rodrigues, J.J.P.C. SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment. *IEEE Trans. Ind. Inf.* **2018**, *14*, 2629–2640. [CrossRef]
20. Du, M.; Wang, K. An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things. *IEEE Trans. Ind. Inf.* **2020**, *16*, 648–657. [CrossRef]
21. Hu, T.; Niu, W.; Zhang, X.; Liu, X.; Lu, J.; Liu, Y. An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning. *Secur. Commun. Netw.* **2019**, *2019*, 1–12. [CrossRef]
22. Schueller, Q.; Basu, K.; Younas, M.; Patel, M.; Ball, F. A hierarchical intrusion detection system using support vector machine for SDN network in cloud data center. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018; pp. 1–6.
23. Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Evaluation of Recurrent Neural Network and its Variants for Intrusion Detection System (IDS). *Int. J. Inf. Syst. Model. Des.* **2017**, *8*, 43–63. [CrossRef]
24. Meng, F.; Fu, Y.; Lou, F. A network threat analysis method combined with kernel PCA and LSTM-RNN. In Proceedings of the 2018 Tenth International Conference on Advanced Computational Intelligence (ICACI), Xiamen, China, 29–31 March 2018; pp. 508–513.
25. Li, H.; Wei, F.; Hu, H. Enabling Dynamic Network Access Control with Anomaly-based IDS and SDN. *Secur. Softw. Def. Netw. Funct. Virtual.* **2019**, 13–16. [CrossRef]
26. Oo, M.M.; Kamolphiwong, S.; Kamolphiwong, T. The design of SDN based detection for distributed denial of service (DDoS) attack. In Proceedings of the 2017 21st International Computer Science and Engineering Conference (ICSEC), Bangkok, Thailand, 15–18 November 2017; pp. 1–5.
27. Latah, M.; Toker, L. Artificial intelligence enabled software-defined networking: A comprehensive overview. *IET Netw.* **2019**, *8*, 79–99. [CrossRef]
28. Raiyn, J. A survey of cyber attack detection strategies. *Int. J. Secur. Appl.* **2014**, *8*, 247–256. [CrossRef]
29. Haider, A.; Muhammad, A.K.; Abdur, R.; Muhib, U.R.; Hyung, S.K. A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System. *CMC-Comput. Mater. Cont.* **2021**, *66*, 1785–1798.
30. Liu, T.; Yanan, S.; Yang, L.; Yuhong, G.; Yucheng, Z.; Dai, W.; Chao, S. Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection. *Future Gener. Comput. Syst.* **2015**, *49*, 94–103. [CrossRef]
31. Baek, S.; Kwon, D.; Kim, J.; Suh, S.C.; Kim, H.; Kim, I. Unsupervised Labeling for Supervised Anomaly Detection in Enterprise and Cloud Networks. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 205–210.
32. Huang, C.-H.; Lee, T.-H.; Chang, L.-h.; Lin, J.-R.; Horng, G. Adversarial Attacks on SDN-Based Deep Learning IDS System. *Int. Conf. Mobile Wirel. Technol.* **2019**, *513*, 181–191.
33. Dey, S.K.; Rahman, M.M. In Flow based anomaly detection in software defined networking: A deep learning approach with feature selection method. In Proceedings of the 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), Dhaka, Bangladesh, 13–15 September 2018; pp. 630–635.
34. Fu, Y.; Lou, F.; Meng, F.; Tian, Z.; Zhang, H.; Jiang, F. An Intelligent Network Attack Detection Method Based on RNN. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; pp. 483–489.
35. Dawoud, A.; Shahristani, S.; Raun, C. A Deep Learning Framework to Enhance Software Defined Networks Security. In Proceedings of the 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 16–18 May 2018; pp. 709–714.
36. Arora, K.; Chauhan, R. Improvement in the performance of deep neural network model using learning rate. In Proceedings of the Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 21–22 April 2017; pp. 1–5.
37. Khan, M.; Karim, M.; Kim, Y. A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network. *Symmetry* **2019**, *11*, 583. [CrossRef]
38. Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. *IEEE Access* **2019**, *7*, 31711–31722. [CrossRef]
39. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4724–4734. [CrossRef]
40. Bhatt, P.; Morais, A. HADS: Hybrid anomaly detection system for iot environments. In Proceedings of the International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Hamammet, Tunisia, 20-21 December 2018; pp. 191–196.
41. Alaiz-Moreton, H.; Aveleira-Mata, J.; Ondicol-Garcia, J.; Muñoz-Castañeda, A.L.; García, I.; Benavides, C. Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol. *Complexity* **2019**, *2019*. [CrossRef]
42. Mansour, A.; Azab, M.; Rizk, M.R.; Abdelazim, M. Biologically-inspired SDN-based intrusion detection and prevention mechanism for heterogeneous IoT networks. In Proceedings of the IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1120–1125.

43. Narayanadoss, A.R.; Truong-Huu, T.; Mohan, P.M.; Gurusamy, M. Crossfire attack detection using deep learning in software defined ITS networks. In Proceedings of the 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–6.
44. Meidan, Y.; Bohadana, M.; Shabtai, A.; Ochoa, M.; Tippenhauer, N.O.; Guarnizo, J.D.; Elovici, Y. Detection of unauthorized IoT devices using machine learning techniques. *arXiv* **2017**, arXiv:1709.04647.
45. Bovenzi, G.; Giuseppe, A.; Domenico, C.; Valerio, P.; Antonio, P. A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. 2020. Available online: https://d1wqtxts1xzle7.cloudfront.net/64346615/ADIoT_Globecom2020_1stCR.pdf?1599157007=&response-content-disposition=inline%3B+filename%3DA_Hierarchical_Hybrid_Intrusion_Detectio.pdf&Expires=1617962449&Signature=T8ZhNst7noVjJAoF0glWOLYjrhSfpylOi7O1LcMGOdOn~zVME1Kt~5Ud63wJUShXOOMIw6MDOoDugee5kl0VDjJgNOjUSC32wLTpOhfBDIPt3gQZncME90di~gIaEKNPuK6V-RNY0kWx8dkASV0W3sFPlRT8RrnnVPOS1tDbbtMXUB8Xrp8hIjlpKXa6nFQ~uUtKxNKwKiD9k65LGLCURiRRs1eyBzyea39eJlg6gp-zsTXgu~7xsGt-F2wlOtRiIht4obWbUri5rMTPCc143E1HRYrgGqh6CBFjVLHPgG~G3KH9Ap2D~docmgHWlYL-r-IXp6NCWa~cuV0qNxUang__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed on 9 April 2021).
46. Liaqat, S.; Akhunzada, A.; Shaikh, F.S.; Giannetsos, A.; Jan, M.A. SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). *Comput. Commun.* **2020**, *160*, 697–705. [CrossRef]
47. Tsironi, E.; Barros, P.; Weber, C.; Wermter, S. An analysis of Convolutional Long Short-Term Memory Recurrent Neural Networks for gesture recognition. *Neurocomputing* **2017**, *268*, 76–86. [CrossRef]
48. Müller, M. Optimizing Recurrent Neural Network Language Model GPU Training. 2017. Available online: https://project-archive.inf.ed.ac.uk/msc/20172467/msc_proj.pdf (accessed on 9 April 2021).
49. Acar, G.; Huang, D.Y.; Li, F.; Narayanan, A.; Feamster, N. Web-based attacks to discover and control local iot devices. In Proceedings of the 2018 Workshop on IoT Security and Privacy, San Francisco, CA, USA, 24 May 2018; pp. 29–35.
50. Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–8.
51. 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]
52. Sindian, S.; Samer, S. An Enhanced Deep Autoencoder-based Approach for DDoS Attack Detection. *Wseas Trans. Syst. Control* **2020**, *15*.