IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Towards SDN-enabled, Intelligent Intrusion Detection System for Internet of Things (IoT)

Mohammed Saleh Ali Muthanna[1], Reem Alkanhel[2], Ammar Muthanna[3], Ahsan Rafiq[4], Wadhah Ahmed Muthanna Abdullah[5]

[1]Institute of Computer Technologies and Information Security, Southern Federal University; 344006 Taganrog; Russia
[2]Department of Information Technology/ College of Computer and Information Sciences/ Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia;
[3]Peoples' Friendship University of Russia (RUDN University) 6 Miklukho-Maklaya, 117198 Moscow, Russia;
[4]College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China ;
[5]Department of Mathematics & Mechanics, Saint Petersburg State University, St Petersburg 199178, Russia;

Corresponding author: Mohammed Saleh Ali Muthanna (e-mail: muthanna@mail.ru).

"This work was supported in part by the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia"

ABSTRACT The Internet of Things (IoT) has established itself as a multibillion-dollar business in recent years. Despite its obvious advantages, the widespread nature of IoT renders it insecure and a potential target for cyber-attacks. Furthermore, these devices' broad connectivity and dynamic heterogeneous nature can open up a new surface of attack for refined malware attacks. There is a critical need of protecting the IoT environment from such attacks and malwares. Therefore this research aims to propose an intelligent, SDN-enabled hybrid framework leveraging Cuda Long Short Term Memory Gated Recurrent Unit (cuLSTMGRU) for efficient threat detection in IoT environments. To properly assess the proposed system, a state-of-the-art IoT-based dataset and standard evaluation metrics were used. The proposed model achieved 99.23 % detection accuracy with a low false-positive rate. For further verification, we compare the proposed model results with two of our constructed models (i.e., cuBLSTM and cuGRUDNN) and current benchmark algorithms. The proposed model outclassed the other models regarding speed efficiency, detection accuracy, precision, and other standard evaluation metrics. Finally, the proposed work employed 10-fold cross-validation to ensure that the results were completely unbiased.

INDEX TERMS Deep Learning, Network security, Intrusion detection, software-defined network, IoT.

I. INTRODUCTION

With the development in information technology (IT), the Internet of things (IoT) has significantly evolved over the last two decades. IoT expands the existence of the Internet by connecting smart devices. The increase of user demands and the large data throughput produced by IoT devices have grown to billions of gigabytes. The IoT connects millions of smart devices resulting in smart environments, i.e., smart factories, ecosystems, smart cities, and intelligent health systems [1]. However, the high user demand and the increasing connectivity of these devices result in raising multiple security concerns. In the last several years, there has been a rapid growth in IoT devices along with the data shared by these devices. Due to this, many threats and attacks are also focusing on the networks of IoT [2]. IoT comprises heterogeneous and homogenous networks along with networking devices using different protocols. The dynamic characteristics of these devices make the entire system and IoT devices vulnerable to cyber-attacks, i.e., distributed denial of service (DDoS) attacks, brute force attacks, denial of service (DoS) attacks, etc. [3]. Security operation center analysts monitor the network continuously to identify each threat and vulnerability, but an attacker tries to exploit the system by looking for a single vulnerability. The authors of [4] discussed deception and replay attacks along with the detection techniques and security controls of such attacks on the industrial level. As the IoT devices are heterogeneous in nature and follow different protocols, various security measures need to be followed for these devices due to their seamless nature. A comprehensive strategy has yet to be devised for securing the complete infrastructure of IoT. The security of the IoT environment remains a major challenge and presents a serious need for security.

Software-defined networking (SDN) enabled architecture provides the opportunity to configure and abridge the management of networks and improves the ability of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

heterogeneous and dynamic nature of the IoT devices. Further, the SDN offers a platform for implementing a security solution to detect threats effectively and efficiently without the exhaustion that does not overburden the IoT devices. A network security system contains an antivirus, firewall, and intrusion detection system (IDS). The IDS generates alerts after identifying unusual behavior of the system, i.e., destruction, alteration, and replication. Thus, one of the best methods for SDN surveillance is to integrate IDS in SDN [5]. With the SDN's programmable feature and the feasibility of Artificial Intelligence (AI), Integrating AI-based security solutions with SDN helps boost security levels. The authors of [8] discussed AI-based techniques employed as network traffic algorithms such as Decision Trees, ANN's, and fuzzy logic resulting in ideal results.

Furthermore, Deep Learning (DL) algorithms and SDN have found several interesting applications in the research community. SDN gives better network security compared to traditional systems [6]. For efficient and early detection of new emerging numerous cyber-attacks, we use SDN-based DL architecture in this work, as illustrated in Figure 1. using the algorithms of DL. The experimentation and evaluations are performed on the CICIDS2017 dataset.

A. CONTRIBUTION

The contributions of this research are as follow:

- We propose a hybrid Intelligent, SDN-enabled model for efficient and early threat detection in the IoT environment.
- cuLSTMGRU is used for effective intrusions detection.
- We employ standard evaluation metrics for a thorough evaluation of the proposed model.
- cuBLSTM and cuGRUDNN are exploited on the same dataset for comparison purposes to prove the proposed model's efficiency.
- For further verification, we compare the proposed model with existing literature.
- Finally, we employed 10-fold cross-validation to ensure that the results were completely unbiased.

The remaining part of this paper is organized as follow:

The Background and Related Work are described and discussed in Section II. The methodology is presented in Section III. The results are summarized and discussed in Section IV. This paper's conclusion is presented in Section V.

II. RELATED WORK AND BACKGROUND

A. BACKGROUND

IoT is defined as an environment of physical devices connected in such a manner where these devices become vital members of a business process. These devices include sensors, network devices, health care, and household devices [7]. IoT consists of different kinds of devices connected by different protocols, and it varies from various networks and environments. A unique address is assigned to each device and connected to the Internet together [8]. The IoT is becoming an essential component of any evolving paradigm of networking and computing. This tremendous revolution in IoT, resulting in enormous advancement in terms of automation and monetary benefit. The complex nature of the IoT environment makes it challenging to provide a common solution because these devices are designed for explicit user purposes. Security is the primary objective in this era, and attaining security is not as simple for IoT devices. These devices cannot be fit into a single protocol due to their diverse nature. Scanning IoT devices for threat detection in real time may result in an unavoidable overhead. That is why we introduce SDN to focus on the programmability of the network. SDN comprises an application plane, control plane, data plane, and related south and north-bound APIs layers. The control plane is responsible for all the decision-making for the whole network. The advent of SDNs has led to a new networking paradigm by separating the data plane and control plane. The efficient and effective SDN framework provides a centralized control plane to the entire control logic. Therefore, SDN's capability and efficiency intelligence reside in their centralized controlled architecture [9]. The south-bound protocol elements provide statistics (insight) to the SDN controller [10]. The integration of IoT and SDN provides a precise network inspection approach for detecting suspicious activities, threats, and attacks. Therefore SDN provides the IoT with a promising future.

B. RELATED WORK

Internet of Things (IoT) is an expeditiously evolving cutting-edge technology that aims to ameliorate traditional communication networks. The broader surroundings of IoT applications make it susceptible to an assortment of crucial security concerns that need to be taken into consideration. Literature has witnessed a plethora of scientific contributions in this regard that have been discussed in this article.

The deep learning (DL) methods improve the model's performance over the traditional Machine learning (ML) approaches. DL framework has been used in different fields, i.e., computer vision, voice recognition, image processing, by large organizations such as Youtube, Google, Microsoft, and Facebook. In recent years, different approaches of DL have been used to mitigate cyber-attacks [11]. The authors in [12] proposed a Deep Learning (DL) driven Software Defined Networks (SDN) based intrusion detection mechanism (CNN-LSTM) for resource-constrained IoT supported medical environments. The system is trained on a distinguished dataset-- IoT Malware Dataset that makes it durable to detect the existence of an enormous variety of common security threats in IoT networking scenarios. Attack detection accuracy, confusion matrix, True Positive (TP), False Positive (FP), True Negative (TN), and False Negative

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

Table 1. Existing Literature

Ref	Classifier	Dataset	Methodology	Limitations	Future Work
[12]	LSTM	IoT Malware Dataset	A DL driven SDN based IDS is proposed for medical IoT environments	End-to-End delay increases in results of traffic analysis	Not Defined
[13]	Random Forest	CICIDS2017	A signature-based IDS is designed against cyber attacks	Computational resource consumption to increased	Aiming to design a more lightweight IDS
[14]	Random Forest	USTA-IoT	A security framework is presented to cater DOS attack category	The collected data set is not reliable and needs to address more features.	The authors planned to train the proposed system on more datasets.
[15]	DNN	CICIDoS2019	The security solution is proposed to identify DoS attack	The proposed system required high network resources	This study targets to address more attacks in the future.
[16]	DNN	IoT Network-Traffic	The designed framework can detect isolation attacks and misappropriation attacks in RPL based IoT	The designed solution is not valid for large-scale commercial networks.	Researchers are motivated to expand the applications of the proposed model.
[17]	SVM, MLP, KNN	UNSW-NB15 *ISCX*	DOS attack detection scheme is designed	Not feasible for resource-constrained environments.	Authors are willing to address more relevant attacks.
[18]	SMO, SDPN	NSL-KDD'99	A threat detection system is proposed to prohibit unauthorized access	High computational resources are required in regards.	The research aims to include more classifiers in the future.
[19]	Multiclass CNN Model	BoT-IoT, MQTT-IoT-IDS2020, IoT-23	A cyber threat identification mechanism is presented	The proposed system is not feasible for small-scale networks.	The authors intend to increase the application area of the proposed framework.
[20]	LSTM	CIDDS-001	A security framework is formulated to detect port scanning and Brute-Force attack	The system is not compatible with large scale networks	The study intends to address the medical IoT sector.
[21]	CNN, LSTM	IoTID20	A detection and prevention scheme against cyber threats is presented.	The formulated scheme requires Complex computational resources.	Not defined
[22]	LSTM	CSE-CIC-IDS2018	A security architecture is designed to locate Brute-Force, SYN flooding, and ICMP flooding attacks	The proposed architecture is not compatible with small-scale networks.	Researchers claim to validate it for resource-constrained environments
[23]	ANN	AD	A comprehensive threat identification mechanism is designed	The system is not feasible for home-based IoT scenarios.	The proposed system aims to extract common features from more datasets
[24]	SVM	BOT-IoT	A machine learning-based model is proposed to mitigate malicious network behavior	Communicational latencies have been experienced	Researchers have planned to reduce false-positive rates in the future.
[25]	DT, NB, RF, LR, SVM, SGD	CICIDS2017	The system is capable of analyzing traffic behavior	The proposed system is not feasible for small-scale residential networks.	Researchers intend to work on its compatibility.

(FN) are all used to evaluate the suggested framework's performance. Moreover, a performance comparison is conducted between the designed framework and other relevant solutions, where favorable results with 99.9% attack detection accuracy seem to support CNN-LSTM and endorse it as a secure and decisive choice for IoT-based communication networks. Another security model is elaborated in [13], where authors proposed an IDS to highlight the malicious enterprises enclosing the IoT communication systems. The proposed system is trained on CICIDS2017 set in accomplice with Random Forest (RF) classifier; the performance is analyzed in comparison with some other variants of the same dataset—The Wednesday's release version. The proposed framework seems to beat later datasets with 99.7% attack detection accuracy and proves its effectiveness in terms of convenient configuration, instant communication, and a trustworthy security sphere. RF is acquired as a training pattern in [14] as well, where another IDS is proposed that aims to assure threat-free transmission channels in IoT environments. The authors conducted a legitimate traffic analysis through Wireshark by taking various factors into account, such as normal packets, encapsulated suspicious elements, transmission speed, transmission power, etc. The obtained logs are filtered and categorized in an appropriate dataset labeled as the USTA-IoT dataset that comes with a moderate integration capability with all state-of-the-art classifiers. The designed model is then scrutinized on a scattered performance matrix including a vast range comprising Denial of Service (DOS) attacks such as SYN, UDP Flood, UDP scan, and ping flood. The proposed framework proves its effectiveness by detecting formerly mentioned networks attacks in significantly less time as compared to the benchmarked model with data set BoT-IOT and TON-IoT.

Distributed Denial of Services (DDOS) attacks possess noticeable status among the list of frequently reported security threats in IoT scenarios. Such sort of attacks tends to slow down the overall performance of the network and sometimes result in even more swear outcomes. To countermeasure such security concerns, another solution is proposed in [15], where the core concepts of deep learning are implemented to formulate a threat detection framework. The designed framework, referred to as CyDDoS that comprises of CICIDoS2019 dataset accompanied with a training pattern on a Deep Neural Network (DNN) classifier. A security matrix is composed to compare the performance of the proposed framework and its rival framework. However, CyDDoS remarkably depicts substantial results and becomes a trustworthy threat detection system. DNN classifier is also interconnected with IoT Network-Traffic dataset to forge a disclosure mechanism for cyber-attacks such as the isolation attacks and misappropriation attacks in IoT networks based on the Routing Protocol for Low Power and Lossy Networks (RPL) [16]. [17] presents another excellent approach for dealing with DoS attacks. The proposed model is trained on three distinguished machine learning techniques, i.e., Multilayer Perception (MLP), Support Vector Machine (SVM), and K-nearest Neighbour (KNN). Moreover, the system is interspersed with two different datasets-- the UNSW-NB15 dataset and the ISCX Dataset. IoT networks more often are victimized by another domain of security threats in which the various suspicious attacks are committed to gain unauthorized access upon the crucial network components. The relevant catalog encompasses a User-to-Root attack (U2R), Remote-to-Local (R2L) attack, and probe attack. [18] intensively spotlight such attacks and provide optimal strategies to culprit such malevolent practices within IoT environments. The designed security framework is trained on the NSL-KDD dataset with its more recent version at NSL-KDD'99. Furthermore, some remarkable training algorithms named Stacked Deep Polynomial Network (SDPN) and Spider Monkey Optimization (SMO) are considered. The proposed framework proficiently encounters the mentioned attacks with the detection accuracy of approximately 99.02%, 99.3%, and 99.4%, respectively. In [19], the authors have proposed a comprehensive security framework to detect the existence of threats in IoT infrastructure. Multiple data sets, i.e., BoT-IoT, MQTT-IoT-IDS2020, IoT Network Intrusion, and IoT-23, are incorporated to make the designed framework more splendid and responsive. This formulated solution is later evaluated in terms of attack detection, where incredibly surprising results advocate the proficiencies of this model by witnessing 98.7% detection accuracy against an extensive range of cyber threats. IoT may also be potentially victimized by a diverse range of cyber threats, including port scanning and Brute-Force attacks. Work proposed in [20] comes to safeguard IoT against such conglomeration. The designed mechanism is trained by acquiring Long Short-Term Memory (LSTM) pattern in an acquisition with Coburg Intrusion Detection Dataset (CIDDS-001). The proposed system possesses the capability to remarkably detect the existence of pre-discussed attacks with 99.92% accuracy along with 99.85% precision, which makes it a phenomenal choice to protect IoT working environments. Host Brute-Force attacks, HTTP flooding, and UDP flooding attacks can also be enlisted in the intermittent threats for IoT. [21] formulated a protection mechanism as an antidote to these security threats. Convolution neural networks (CNN) along with LSTM are some well-known classifiers that have been employed to train the proposed framework. Furthermore, Particle Swarm Optimization (PSO) is used to select the best feature among the IoTID20 dataset. Authors have addressed a vast range of cyber-attacks, and their designed framework has validated this claim by successfully detecting these attacks with remarkable accuracy. [22] discussed a relevantly admissible approach to an encounter Brute-Force attack, SYN flooding, and ICMP flooding attacks. The designed security framework is aggregated with CSE-CIC-IDS2018 data set with a training pattern on LSTM and is capable of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

detecting premonition threats in IoT communications. Another ML-based IDS is offered by employing state-of-the-art feature extraction techniques to accumulate their combined features to detect cyber threats in an effectual way [23]. The system is leveraged by Artificial Neural Network (ANN) classifier in interconnection with the AWID dataset, which makes it compatible to investigate the existence of suspicious entities in a miraculous way. Another relevant approach is used in [24], where researchers proposed another id by commemorating the Support Vector Machine (SVM) classifier in coordination with the BOT-IOT dataset. The actual momentum of the proposed system is analyzed under diverse performance matrixes where adjuvant outcomes seem to strengthen the ancillary framework. [25] contains an encyclopedic IDS to substantially detect the perpetuation of cyber threats. Authors have encompassed an acclaimed data set originated by the Canadian Institute of Cyber Security Intrusion Detection System Dataset (CICIDS2017). Additionally, six different classifiers are taken into consideration, namely Decision Tree (DT), Logistic Regression (LR), Naïve Bayes (NB), Random Forest (RF), Stochastic gradient descent (SGD, and Support Vector Machine (SVM). The framework dexterously percolates malicious communicational streams among IoT networks with impressive veracity.

The entire related work is summarized in Table 1.

III. METHODOLOGY

This section provides the entire research methodology of this research work with a thorough explanation of the network model, dataset, detection framework, algorithms, pre-processing, etc.

A. NETWORK MODEL

In the last few years, SDN has emerged as a technology of integrated network design. It consists of three planes: Application, control, and data plane. In SDN, the control and data planes are separated, which allows simplification and flexibility. The whole network is managed by the SDN controller, which is placed in the control plane. The SDN simplifies gathering network statistics by having a global view of central control functions and networks and gives better network security than traditional techniques. In SDN architecture, the south-bound protocol is the most significant protocol, responsible for exchanging information between the networking devices and controller.

The authors propose a DL-driven, SDN-enabled framework for intrusion detection in the IoT environment. The network model is shown in Figure 1. The proposed DL-driven model (cuLSTMGRU) is placed in the control plane. The proposed model is highly cost-effective and centralized. We have placed the proposed model in the control plane for the following reasons: First of all, the SDN control plan is utterly programmable and adjustable. Secondly, the control plane can cover multiple networks on its data plane. Thirdly, it can leverage IoT devices without the exhaustion that does not overburden them, which makes it a suitable revolution for IoT.

Fourthly, it has Open-Flow (OF) switches that provide a solution for heterogeneity between IoT devices and SDN controllers. OF is a prime south-bound protocol identified by an SDN framework's control and data plane. It consists of activities and flows tables that notify the switch how to proceed with these channels and flows; consequently, the switches and controller are connected. The combination of IoT and SDN provides a proper way to inspect network traffic for detecting threats, suspicious events, and attacks. Further, many IoT devices can be added to the data plane of SDN: e.g., sensors, wireless technologies, and smart devices.

B. DATASET

Selecting an appropriate dataset significantly affects the threat detection framework performance. Various datasets have been employed by different authors for intrusion detection in IoT contexts, according to the literature, i.e., the author in [26] used CICDDoS19 for threat detection in IoT. At the same time, some authors used kdd99, NSLKDD, etc., which lacks the supportive features of IoTs. As a result, the proposed research work used the most up-to-date publicly available CICIDS2017 dataset [27]. This dataset has the supporting features of IoTs, i.e., the dataset is flow-based and is multi-class. It comprises more than 80 features with eight categories of attacks such that. The proposed work selected all the features of this dataset, and the total distribution is across five classes, i.e., benign and attacks. Table 2 provides more information about these classes and its instances.

C. PREPROCESSING OD DATASET

The data in the dataset is in various forms, feeding it directly to the algorithm for classification is not reliable. To increase the proposed model's performance and efficiency, we have performed the pre-processing of the dataset. Initially, all the rows having NaN and Infinity values are deleted. Further, all the non-numeric values are converted to numeric values as the algorithms of DL process the numeric data mainly. Finally, we have performed data normalization to improve the dataset's quality by using the MinMaxScalar function.

D. Detection Framework

The authors proposed SDN enabled intelligent framework, i.e., cuLSTMGRU, to combat sophisticated threats in IoT. Gated Recurrent Unit (GRU) is a lately-developed variant of the long short-term memory (LSTM) unit. GRU is informal to adjust and uses the hidden state to allocate information; however, it doesn’t require memory units. Consequently, quicker to train and provide improved performance. Subsequently, LSTM is implemented to attain effectual modeling for longer sequences from the dataset, sustaining

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

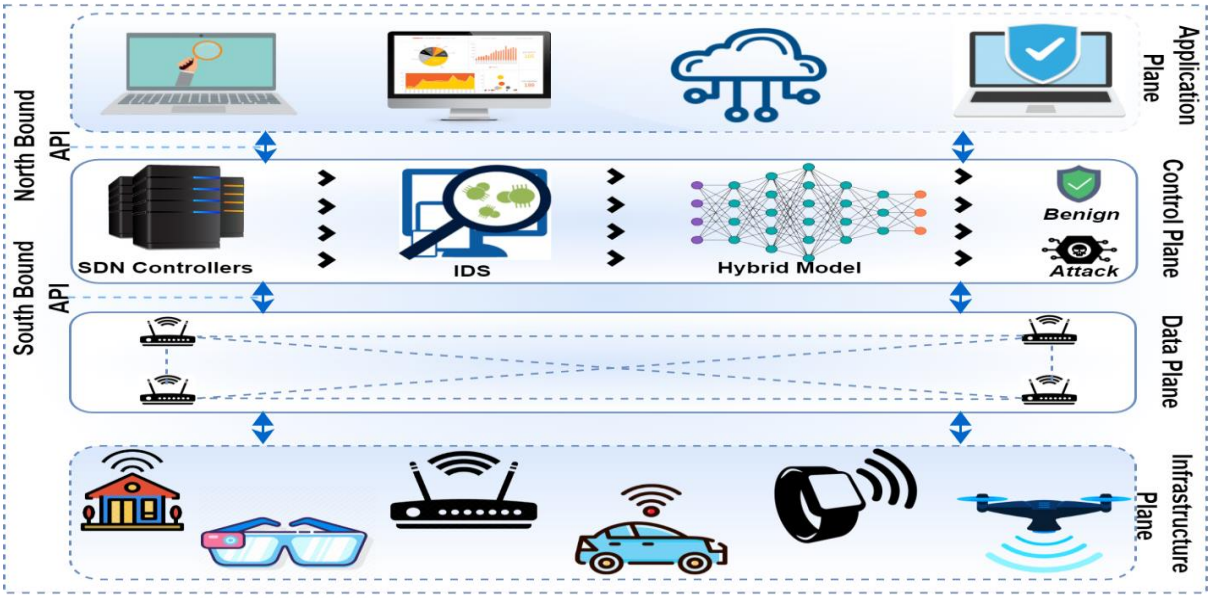

Figure 1. Proposed Network Model

Table 2. Dataset Description

Category	Attack	No of Instances
Benign		8000
Bot	Ares	1876
DDoS	Goldeneye	2149
	Slowloris	2045
Cross-site scripting	XSS	872
Total		**14942**

significantly for preemption of gradient vanishing problem. To entirely get an advantage from the abilities of various DL-classifiers simultaneously, we have used LSTM and GRU for refining complete outcomes in terms of accuracy, recall, precision, speed efficiency, and F1-score. The proposed framework is highly versatile and cost-effective. This framework has been trained and tested on the CICIDS2017 dataset and achieved a better detection accuracy with a very low false-positive rate (FPR). The proposed framework has multiple layers, i.e., LSTM 200 and GRU have 100 neurons in a single layer. The proposed detection framework is depicted in Figure 2. We have used the Relu and softmax functions. For experimental purposes, we have used the Cuda-enabled versions for improved performance. The experimentation has been conducted for five epochs with 32 batch size for achieving efficient results. Further, the proposed work used the Keras framework and the backend of TensorFlow (TF) for python. In addition, we have used two hybrid classifiers to compare their results with our proposed model for an enhanced evaluation, i.e., cuBLSTM and cuGRUDNN are used as comparison classifiers. cuBLSTM consists of one layer of BLSTM with 200 neurons, while cuGRUDNN consists of one layer of GRU with 200 and another layer of DNN with 100 neurons. Table 3 depicts an in-depth description of the proposed scheme along with the comparison classifiers.

E. ALGORITHMS

The proposed work used Cu-LSTM-GRU for affective intrusion detection in IoT environments. The proposed model has been tested and evaluated under the CICIDS2017 dataset. The details of the algorithms are as follow

a. LONG SHORT TERM MEMORY (LSTM)

LSTM belongs to the RNN family proposed in 1997. It has the ability to learn order dependence in problems like sequence predictions. The LSTM uses feedback connections unlikely feed forward standard neural networks. It uses gating mechanisms for the optimization of the flow of info. The LSTM comprises cell, input, output,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

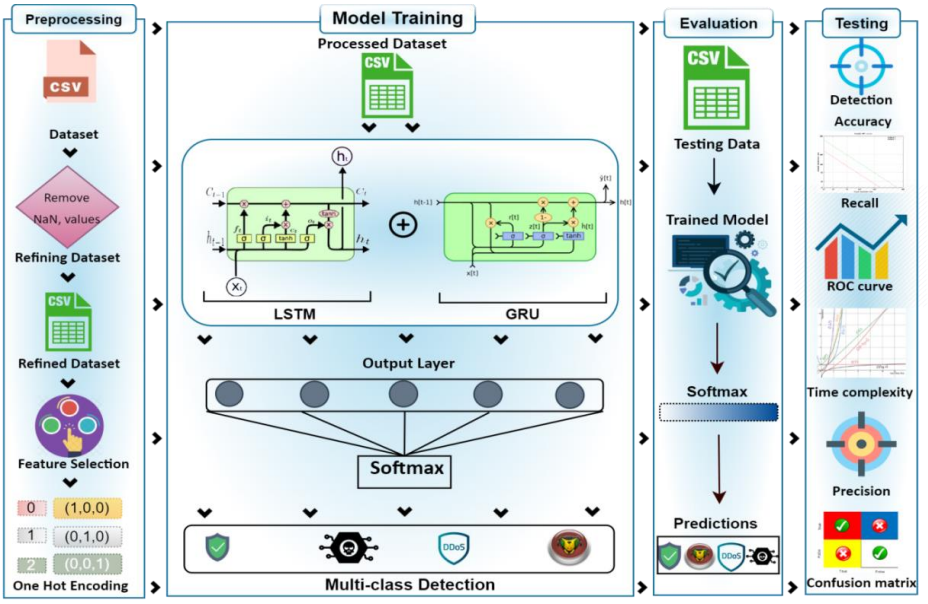

Figure 2. Proposed Detection Framework

Table 3. Hybrid Models Description

Algorithm	*Cu-LSTM-GRU*	*Neurons*	*Cu-BLSTM*	*Neurons*	*Cu-GRU-DNN*	*Neurons*
Layers	Cu-LSTM (1)	(200)	BLSTM (1)	(200)	GRU(1)	(200)
	Cu-GRU (1)	(100)	-	-	DNN (1)	(100)
	Output Layer (1)	(07)	Output Layer (1)	(07)	Output Layer (1)	(07)
	Dense (3)	(200,100,50)	Dense (3)	(200,100,50)	Dense (3)	(200,100,50)
	Dropout	0.3	Dropout	0.3	Dropout	0.3
Activation Function	Relu and Softmax					
Optimizer	Adamax					
Lose Function	CC-E					
Batch-size	32					
Epochs	05					

and forget gate. The cell recalls the values while the three gates control the information flow in and out of the cell.

Each j-th LSTM unit maintains a memory cjt at time t, unlike the recurrent unit, which simply adds up the weighted sums of the input signals and applies a nonlinear function; the recurrent unit adds up the weighted sums of the input signals and applies a nonlinear function. The output hjt , or the activation, of the LSTM unit, is then

$$h^j_t = o^j_t \tanh(c^j_t) \quad (1)$$

The ojt, which is an input gate, controls the amount of memory content exposure. The output gate is determined by the following formula:

$$o^j_t = \alpha\,(W_o X_t + U_o h_{t-1} + V_o c_t)^j \quad (2)$$

Where Vo is a diagonal matrix and — α is a logistic sigmoid function. Cjt is the memory cell that is updated by partially forgetting the present memory and adding a new memory content c~jt :

$$c^j_t = f^j_t\, c^j_{t-1} + i^j_t\, c^{\sim j}_t \quad (3)$$

where the new memory content is

$$c^{\sim j}_t = \tanh(W_c X_t + U_c h_{t-1})^j \quad (4)$$

The degree to which the current memory is forgotten is modulated by a forget gate fjt , and the degree to which the new memory content is added to the memory cell is modulated by an input gate ijt. Gates are computed by

$$f^j_t = \alpha\,(W_f x_t + U_f h_t + V_f\, c_{t-1})^j \quad (5)$$

$$i^j_t = \alpha\,(W_f x_t + U_f h_t + V_f\, c_{t-1})^j \quad (6)$$

b. GATED RECURRENT UNIT (GRU)

GRU belongs to the RNN family and is the improved version of the standard RNN. GRU has the ability to solve the problem of the gradient by using an update and reset gate. They are known as the two vectors and decide what info should be passed to the output. Its specialty is keeping the information from long ago instead of removing the information irrelevant to the prediction. The equations of GRU are as follow:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

$$Z_t=\sigma\ (W^{(Z)}x_t + U^{(z)}h_{t-1}) \quad (7)$$

Equation 07 is used to calculate the update gate.

$$R_t= \sigma\ (W^{(r)}x_t + U^{(r)}h_{t-1}) \quad (8)$$

Equation 08 is used for resetting the gate and for deciding how much past info to forget.

Both of these formulas are the same. The only difference is the gate usage and the weight.

$$H'_t= \tanh(Wx_t + r_t \odot Uht\text{-}1) \quad (9)$$

Rt is a set of reset gates and ⊙ is an element-wise multiplication. The reset gate basically causes the unit to behave as if it is reading the first symbol in an input sequence, allowing it to forget the state it had previously computed. Equation 3 is used for storing the related info from the past.

$$H^t=z_t \odot h_{t-1} + (1\text{-}z_t) \odot h'_t \quad (10)$$

Equation 10 is the final phase, in which the network must calculate the vectors containing the current state's information.

C. PSEUDO CODE

The pseudo code of the proposed model is as follow

Algorithm 1 Hybrid cu-LSTM-GRU detection model

Input:

nth IoT features and malware labels: X_n^{iot}, Y_n^{iot}

cu-GRU layers = M ; cu-LSTM layers = l; k-Folds = k; epochs= e;

Output:

Get the Error E and predictions P.
For all k:=1 to 10 do
  for epochs:=1 to e do
    if select.layer [M] = cuGRU **then**
      Calculate update gate for timestamp t.
      Calculate reset gate to determine how much of past information to forget.
      Starting with the usage of the reset gate, new memory content will use the reset gate to store information.
      Calculating ht-Vector, which holds information of the current position.
    else
      Generate a feature vector.
    end if
    if select.layer[l] = cuLSTM **then**
      Randomly generate the w and b of LSTM;
      Compute the Hidden layers of LSTM;
      Compute the output of Hybrid GRULSTM;
    end if
  end for

IV. EXPERIMENTAL SETUP

We have used Core i7, a seventh-generation Intel processor, and Nvidia Geforce 1060 Graphics Processing Unit (GPU) for experimentation. Complete detail of the experimental setup is shown in Table 4.

Table 4. Experimental Setup

Operating System	Windows 10
Processor	Core i7, 3.33 GHz
Model	7700, 7th generation
RAM	16 GB
GPU	6 GB, Nvidia GeForce 1060
Language	Python 3.8
Libraries	Numpy, Tensorflow, Scikitlearn, Pandas, Keras
IDE	Spyder Anaconda

A. PERFORMANCE EVALUATION METRICS

The proposed work used all of the standard metrics of evaluation, i.e., Accuracy, F1-score, Recall, Precision, etc., to comprehensively assess the proposed framework's performance on the CICIDS2017 dataset. The description of the parameters and the mathematical formulae of these metrics of evaluation are as follow:

B. ACCURACY

The accuracy represents the accurately classified percentage of the records in the dataset.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

C. RECALL

It represents the total number of records that are accurately predicted over all the data available for a specific class.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (12)$$

D. PRECISION

It represents the total number of the records that are predicted accurately over all the predicted records

$$\text{Precision} = \frac{TP}{TP+FP} \quad (13)$$

E. F1-SCORE

For a thorough evaluation of the model, F1-score uses recall and precision and is also known as the mean of recall and precision.

$$\text{F1-score} = \frac{2*TP}{2*TP+FP+FN} \quad (14)$$

Other performance evaluation metrics, such as True Negative Rate (TNR), Matthews Correlation Coefficient (MCC), False Discovery Rate (FDR), False

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

Positive Rate (FPR), True Positive Rate (TPR), False Negative Rate (FNR), and False Omission Rate (FOR), have also been calculated for a better evaluation of our model.

V. RESULTS AND DISCUSSION

The complete results and assessment of the proposed model are presented here. For a comprehensive assessment of the proposed model (cuLSTMGRU), its results are compared with the other two classifiers, i.e., cuBLSTM and cuGRUDNN, which are also trained and tested on the same dataset. All of the three models are evaluated under the same standard metrics of evaluation. For further verification, the output of the proposed model is also compared with the existing literature. The proposed model's performance is assessed using the standard metrics listed below.

A. CROSS-VALIDATION

The ten-fold cross-validation has also been employed for the verification of our results. A complete description of each of the folds is depicted in Table 5. The average results of the ten-fold are presented in different parts of this paper for evaluation metrics.

B. CONFUSION MATRIX ANALYSIS

It is used for the purpose of classification and is extremely important to measure the accuracy, F1-score, and recall. The confusion matrix shows the TNR, TPR, FNR, and FPR. The proposed model (cuLSTMGRU) identified the classes properly, as shown in Figure 3.

C. ROC CURVE ANALYSIS

The Roc is a crucial parameter in any intrusion detection system (IDS). It is used for plotting the visualized performance to compare the false positive rate and true positive rate. Figure 4 depicts the Roc curves of the three models accordingly, proving that the proposed algorithm performs significantly better than the other hybrid DL-driven architectures.

D. ACCURACY, F1-SCORE, PRECISION AND RECALL

For a better assessment, we present the proposed model accuracy. The detection accuracy indicates the performance and efficiency of our proposed model. Figure 5 depicts the results of the proposed model along with the other two models. The proposed model achieved an accuracy of 99.23 %. The detection accuracy has been acquired from the implementation results by applying Cu-LSTM-GRU on the CICIDS2017 dataset. The precision represents the total number of accurately predicted records over all the predicted records. The precision of the model is 99.79 %. Further, the recall signifies the total number of accurately predicted records over the data available for a specific class. The F1-score and recall of the proposed model are 98.57 % and 99.87%, respectively. The results are evident that the proposed model achieves better results than the other two classifiers. However cuBLSTM and cuGRUDNN achieved an accuracy of 97.31 % and 97.02 % with F1-score of 96.88 % and 97.02 % respectively.

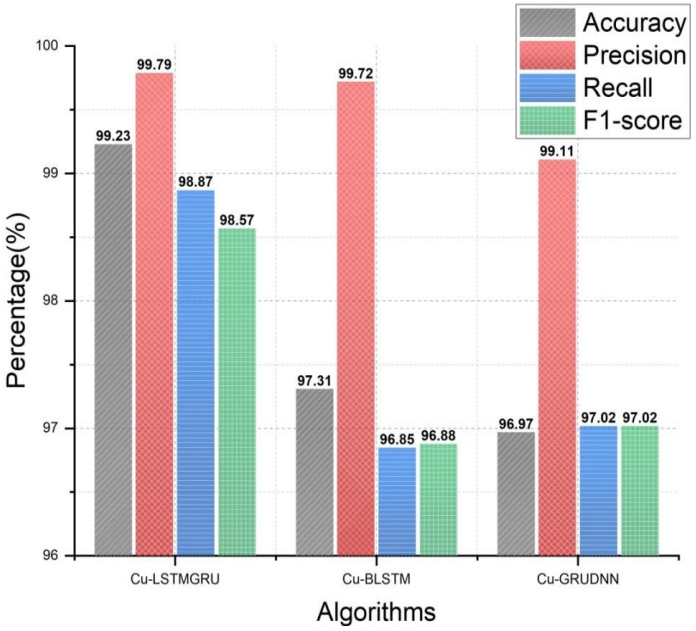

Figure 5. Accuracy, Precision, Recall and F1-score

E. TPR, TNR, AND MCC

In DL, the true positive rate is used for measuring the percentage of actual positives which are identified correctly. The values of TPR, TNR, and MCC are acquired from the uncertainty matrix. Figure 6 depicts the values of these matrices values, which are 98.87 %, 99.11 %, and 94.59 respectively. On the other hand the values of TPR, TNR, and MCC of cuBLSTM are 96.88 %, 98.98 %, and 93.11 %. For cuGRUDNN these values are 97.02 %, 96.82 %, and 92.21 % accordingly.

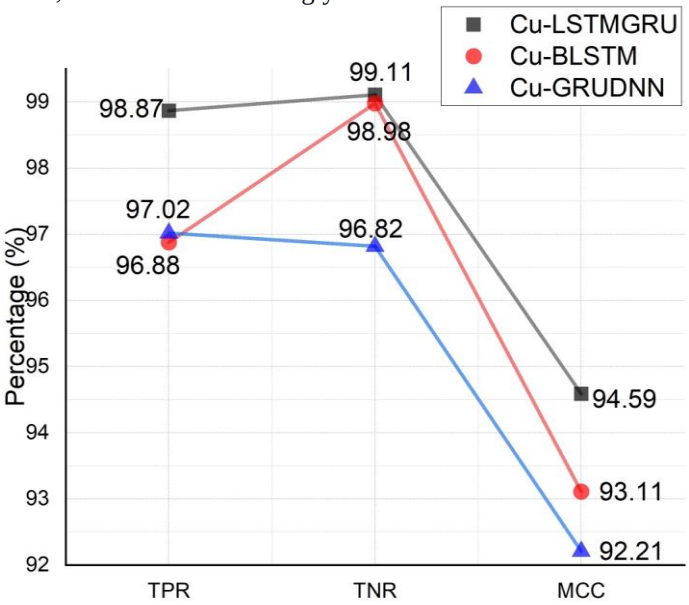

Figure 6. TPR, TNR and MCC

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

Table 5. 10-Folds Result

Folds	Accuracy (%)			Precision (%)			Recall (%)			F1-Score (%)		
	LS-GR	BLSTM	GR-DN	LS-GR	BLSTM	GR-DN	LS-GR	BLSTM	GR-DN	LS-GR	BLSTM	GR-DN
01	99.44	97.38	96.92	99.83	99.78	99.01	98.95	96.91	97.06	98.95	96.91	97.06
02	99.29	97.40	96.80	99.81	99.81	99.81	99.11	96.91	96.18	99.11	96.91	96.18
03	99.16	97.38	97.05	99.71	99.95	99.64	98.71	96.75	96.64	98.71	96.75	96.64
04	99.15	97.38	97.10	99.67	99.90	99.42	98.91	96.80	96.91	98.91	96.80	96.91
05	99.36	97.11	97.03	99.78	99.39	98.98	99.09	96.95	97.22	98.09	96.95	97.22
06	99.19	97.10	97.07	99.83	99.56	99.28	98.85	96.78	97.00	98.85	96.78	97.00
07	99.18	97.36	96.85	99.81	99.59	98.70	98.73	96.78	97.26	98.73	97.07	97.26
08	99.29	97.64	97.22	99.83	99.90	99.14	98.85	96.12	97.32	98.85	97.12	97.32
09	99.31	97.34	96.97	99.82	99.97	98.64	99.16	96.70	97.46	97.16	96.70	97.46
10	98.94	97.04	96.69	99.87	99.40	98.57	98.39	96.84	97.18	98.36	96.84	97.18

LS-GR= Cu-LSTM-GRU, BLSTM= Cu-BLSTM DN-GR= Cu-GRU-DNN

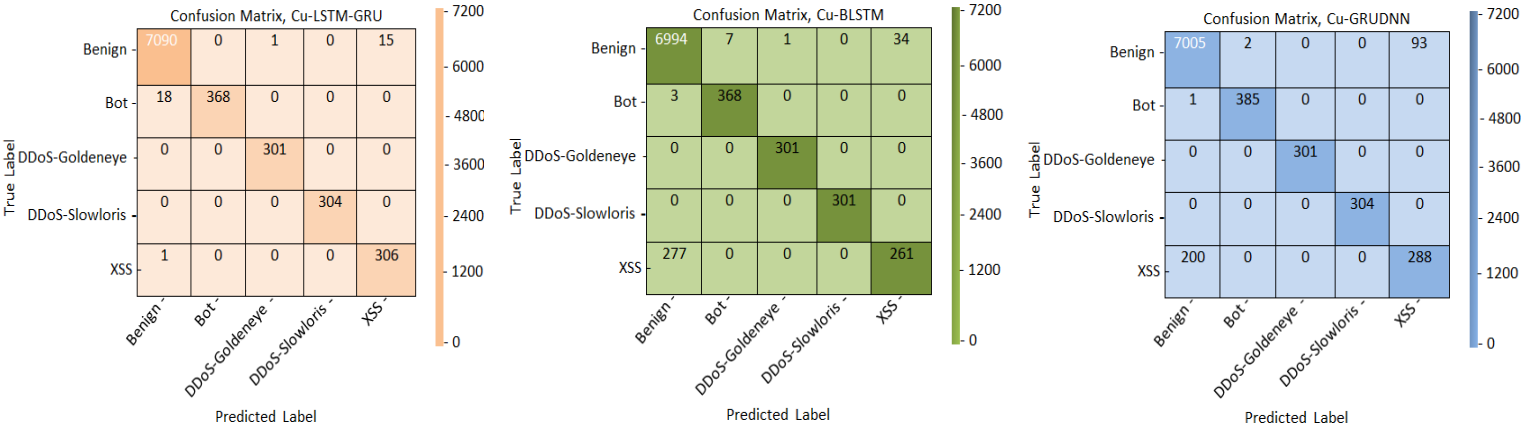

Figure 3. Confusion Matrix of cuLSTMGRU, cuBLSTM, and cuGRUDNN

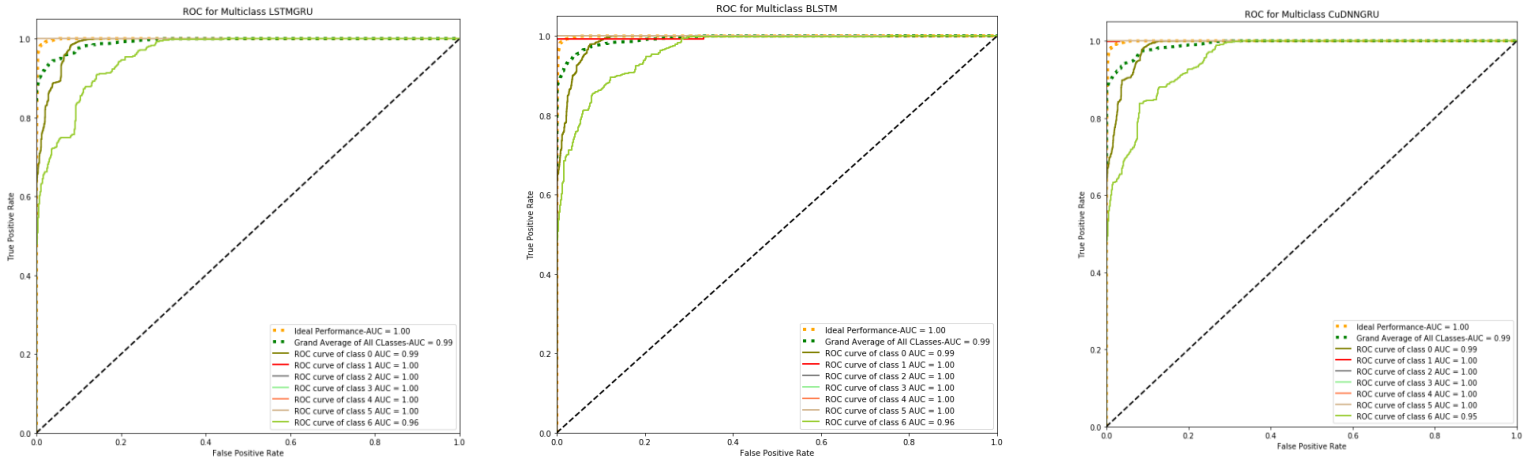

Figure 4. Roc Curves of cuLSTMGRU, cuBLSTM, cuGRUDNN

F. FDR, FPR, FNR AND FOR

This work additionally measures the FDR, FOR, FNR, and FPR for better assessment. Figure 7 demonstrates that the proposed model has an FDR and FOR of only 0.0036 % and 0.0990 %, and FNR and FPR of only 0.0030 % and 0.0066 % only.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

Table 6. Comparison with current Benchmarks

Schemes	Dataset	Algorithm	T.Time	Cu-E	10 Fold	Precision	Accuracy	Recall	F1-score
Proposed	CICIDS2017	LSTMGRU	15.30 ms	✓	✓	99.79 %	99.23 %	99.87 %	98.57 %
[28]	CICIDS2018	CNN	×	×	×	×	91.50 %	×	×
[29]	CICIDS2017	LSTMCNN	296 ms	✓	✓	99.37 %	98.60 %	99.50 %	99.35 %
[30]	CICDDoS2019	EDSA	×	×	×	91 %	98 %	×	×
[31]	NSL-KDD	DNN	×	×	×	×	75.75 %	×	×

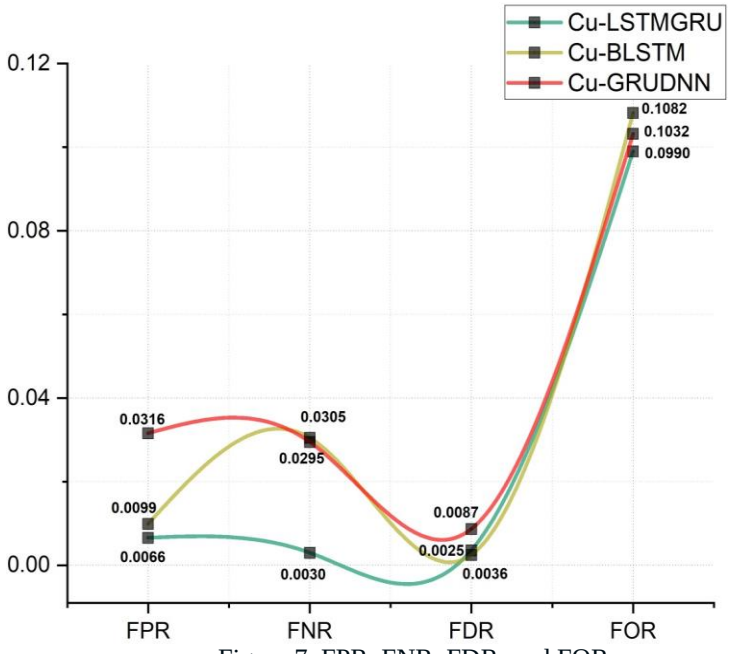

Figure 7. FPR, FNR, FDR, and FOR

G. SPEED AND TIME EFFICIENCY

Training and testing are two phases of analysis. The testing phase is critical since it demonstrates the model's effectiveness. However, the training phase is primarily conducted offline, which is normally overlooked. Figure 8 depicts the proposed model's (cuLSTMGRU) testing time

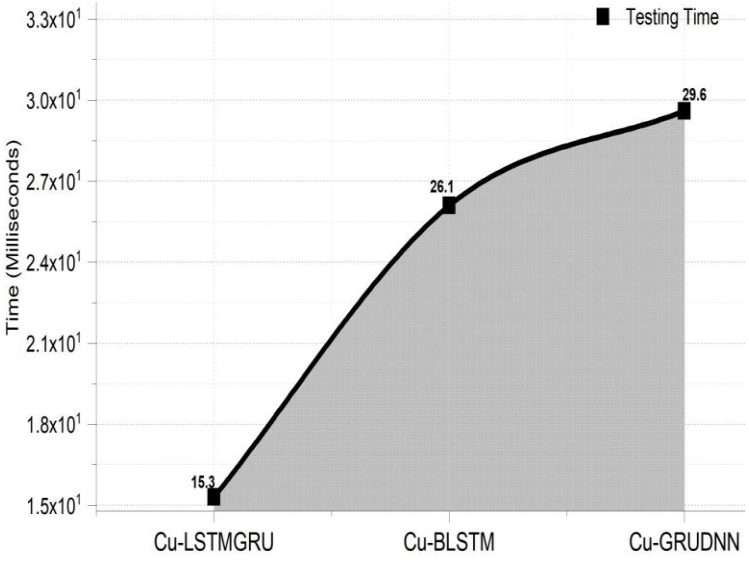

Figure 8. Testing time of the Models

of only 15.3 ms, proving that the model is computationally efficient. However, the speed efficiency of cuBLSTM and cuGRUDNN is 26.1 ms and 29.6 ms.

H. COMPARSION WITH CURRENT BENCHMARK ALGORITHMS

To prove the proposed model's efficiency, we have further compared the proposed model (Cu-LSTMGRU) with our constructed two classifiers, i.e., Cu-BLSTM and Cu-GRU-DNN. These models are trained on the same dataset and evaluated under the same standard evaluation metrics. Furthermore, the model is also compared with current benchmark algorithms for a thorough performance evaluation, as shown in Table 6. In [28], the authors used CNN as a detection model, trained on the CICIDS2018 dataset, and achieved a detection accuracy of 91.50%. However, in [29], a hybrid detection module, i.e., LSTM-CNN, has been used, and the achieved accuracy and precision rates are 98.60% and 99.37%, with a testing time of 296 milliseconds (ms). The authors of [30] used an autoencoder with sigmoid AF (EDSA) as a detection module trained and evaluated under the CICDDoS2019 dataset. The authors achieved an accuracy of 98% with a 91% precision. In [31], Deep Neural Network (DNN) was used as a detection module, but the authors got a very low detection accuracy of only 75.75%. Our proposed model (cuLSTMGRU) outclassed the existing literature in all of the considered standard metrics of evaluation. In addition, cuLSTMGRU has a testing time of only 15.30 ms, reasonably better than cuBLSTM and cuGRUDNN classifiers and existing literature.

V. CONCLUSION

The Internet of Things requires a dependable, dynamic, adaptable, quicker, and secure network architecture. Intrusion detection systems based on deep learning are capable of detecting a wide range of sophisticated threats and attacks. In this paper, the authors introduced SDN-based hybrid DL-driven architecture (i.e., cuLSTMGRU) for efficient threat detection in an IoT environment. The architecture presented is both cost-effective and scalable. The detection accuracy achieved by the proposed model is 99.23 %, with a false-positive rate of only 0.0066 %. A comprehensive evaluation of the model is conducted by comparing it with two of our constructed DL-driven models (i.e., cuBLSTM and cuGRUDNN) and current benchmarks. The proposed model outclassed the other models in terms of all standard metrics of evaluation. The testing time of the proposed model is only 15.30

milliseconds, proving the speed efficiency of the model. In the future, we aim to use blockchain with hybrid models based on DL to develop a more efficient intrusion detection system for IoTs. Furthermore, this hybrid model is expected to be integrated into the NIDS so that it can be used to mitigate sophisticated threats in real-time. Finally, the authors recommend a variety of DL-driven hybrid models for the security of the IoT ecosystem and upcoming computational paradigms.

Acknowledgments:

The work of Mohammed Muthanna was supported by the Southern Federal University.

REFERENCES

[1] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," Sensors (Basel), vol. 20, Jun 28 2020

[2] D. Javeed, T. Gao. M. T. Khan and I.Ahmad, "A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT)". Sensors, 21(14), 4884.

[3] A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems," IEEE Transactions on Communications, vol. 67, pp. 1371-1387, 2019.

[4] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," Neurocomputing, vol. 275, pp. 1674-1683, 2018.

[5] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," Computers in Human Behavior, vol. 48, pp. 51-61, 2015.

[6] A. Wang, Z. Zha, Y. Guo, and S. Chen, "Software-Defined Networking Enhanced Edge Computing: A Network-Centric Survey," Proceedings of the IEEE, vol. 107, pp. 1500-1519, 2019.

[7] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, vol. 03, pp. 164-173, 2015.

[8] W. Ren, Y. Sun, H. Luo, and M. Guizani, "A Novel Control Plane Optimization Strategy for Important Nodes in SDN-IoT Networks," IEEE Internet of Things Journal, vol. 6, pp. 3558-3571, 2019.

[9] R. M. A. Ujjan, Z. Pervez, and K. Dahal, "Suspicious Traffic Detection in SDN with Collaborative Techniques of Snort and Deep Neural Networks," pp. 915-920, 2018.

[10] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN Networks: A Survey of Existing Approaches," IEEE Communications Surveys & Tutorials, vol. 20, pp. 3259-3306, 2018.

[11] I. Ko, D. Chambers, and E. Barrett, "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain," International Journal of Information Security, vol. 19, pp. 53-70, 2019.

[12] S. Khan and A. Akhunzada, "A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)," Computer Communications, vol. 170, pp. 209-216, 2021.

[13] E. M. Zeleke, H. M. Melaku, F. G. Mengistu, and I. Ali, "Efficient Intrusion Detection System for SDN Orchestrated Internet of Things," Journal of Computer Networks and Communications, vol. 2021, pp. 1-14, 2021.

[14] J. Xu, Y. Zhang, Z. Wang, R. Geng, K. K. Choo, J. A. Pérez-Díaz, D. Zhu, "Efficient and Intelligent Attack Detection in Software Defined IoT Networks, ," IEEE International Conference on Embedded Software and Systems (ICESS), , pp. pp. 1-9, 2020.

[15] I. Ortet Lopes, D. Zou, F. A. Ruambo, S. Akbar, B. Yuan, and W. Li, "Towards Effective Detection of Recent DDoS Attacks: A Deep Learning Approach," Security and Communication Networks, vol. 2021, pp. 1-14, 2021.

[16] G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," Sensors (Basel), vol. 19, Apr 27 2019.

[17] J. Ashraf, N. Moustafa, A. D. Bukhshi, and A. Javed, "Intrusion Detection System for SDN-enabled IoT Networks using Machine Learning Techniques," pp. 46-52, 2021.

[18] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," Transactions on Emerging Telecommunications Technologies, 2019.

[19] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," IEEE Access, vol. 9, pp. 103906-103926, 2021.

[20] I. Ullah, B. Raza, S. Ali, I. A. Abbasi, S. Baseer, A. Irshad, and M. Arif, "Software Defined Network Enabled Fog-to-Things Hybrid Deep Learning Driven Cyber Threat Detection System," Security and Communication Networks, vol. 2021, pp. 1-15, 2021.

[21] H. Alkahtani, T. H. H. Aldhyani, and M. I. Uddin, "Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms," Complexity, vol. 2021, pp. 1-18, 2021.

[22] A. Wani, R. S, and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," CAAI Transactions on Intelligence Technology, vol. 6, pp. 281-290, 2021.

[23] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed, and F. Anwar, "Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection," Multimedia Tools and Applications, vol. 80, pp. 31381-31399, 2021.

[24] R. Samdekar, S. M. Ghosh, and K. Srinivas, "Efficiency Enhancement of Intrusion Detection in Iot Based on Machine Learning Through Bioinspire," pp. 383-387, 2021.

[25] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," Arabian Journal for Science and Engineering, 2021.

[26] D. Javeed, T. Gao, and M. T. Khan, "SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT," Electronics, vol. 10, p. 918, 2021.

[27] A. A. Ghorbani, A. Habibi Lashkari, and I. Sharafaldin, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," pp. 108-116, 2018.

[28] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-Based Network Intrusion Detection against Denial-of-Service Attacks," Electronics, vol. 9, p. 916, 2020.

[29] J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN," IEEE Access, vol. 8, pp. 134695-134706, 2020.

[30] S. Sindian and S. Sindian, "An Enhanced Deep Autoencoder-based Approach for DDoS Attack Detection," Wseas Transactions on Systems and Control, vol. 15, pp. 716-724, 2020.

[31] L. M. T. A. Tang, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking, " International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258-263, 2016.

MOHAMMED SALEH ALI MUTHANNA received his M.S. degree from Computer Science Department, Saint Petersburg Electrotechnical University "LETI", Russia, in 2016, and the PhD from Chongqing University of Posts and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3153716, IEEE Access

Telecommunications, Chongqing, China in 2021. Currently, he is a postdoctoral fellow with Institute of Computer Technologies and Information Security, Southern Federal University Russia. His main research interests include mobile edge computing, Software-Defined Networks (SDN), IoT, industrial wireless and sensor networks.

Reem Alkanhel received the B.S. degree in computer sciences from King Saud University, Riyadh, Saudi Arabia, in 1996, the M.S. degree in information technology (computer networks and information security) from Queensland University of Technology, Brisbane, Australia, in 2007, and the PhD degree in information technology (networks and communication systems) from Plymouth University, Plymouth, United Kingdom, in 2019. She has been with Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia since 1997. She is currently a teacher assistant at the college of Computer and Information Sciences. Her current research interests include communication systems, networking, internet of things, information security, information technology, quality of service and experience, software defined network, and deep reinforcement learning.

AMMAR MUTHANNA is an Associate Professor at the Department of Telecommunication networks, Deputy head of Science and Head of SDN Laboratory. He received his B.Sc. (2009), M.Sc. (2011) and as well as Ph.D. (2016) degrees from Saint - Petersburg State University of Telecommunications. 2017-2019 he worked as Postdoctoral Researcher at RUDN University. In 2012 and 2013, he took part in the Erasmus student Program with the Faculty of electrical engineering, University of Ljubljana and in 2014 visitor researcher at Tampere University, Finland.
Ammar is a Member of the IEEE. He has been an Active Member of the Technical Program Committee on many international conferences and journals. He has been an expert at the Judges Panel and Challenge Management board at AI-5G-Challenge, ITU and Russian host organizer. Area of research: wireless communications, 5G/6G cellular systems, IoT applications, Edge computing and software-defined networking.

Ahsan Rafiq received his Master of Computer Science degrees from the National College of Business Administration and Economics, Lahore, Pakistan, in 2016. He is currently pursuing his Ph.D. with the Department of Computer Science, Chongqing University of Posts and Telecommunication, Chongqing, China. His research interests are IIOT to enable smart communication in industries, 6TiSCH networks, and edge and fog computing in industries.

WADHAH AHMED MUTHANNA ABDULLAH received his M.S. degree from Computer Science Department, Kazan National Research Technological University "KNITU", Russia in 2017. He is currently pursuing Ph.D. degree with the department of Mathematics and Mechanics Faculty, St. Petersburg State University, Saint Petersburg, Russia. His research interests include the resources management of the Wireless sensor networks, and the AUV aided underwater sensor networks.