An Intelligent Intrusion Detection System for Smart Consumer Electronics Network

Danish Javeed, Muhammad Shahid Saeed, Ijaz Ahmad, Prabhat Kumar, Alireza Jolfaei, Muhammad Tahir

***Abstract*—The technological advancements of Internet of Things (IoT) has revolutionized traditional Consumer Electronics (CE) into next-generation CE with higher connectivity and intelligence. This connectivity among sensors, actuators, appliances, and other consumer devices enables improved data availability, and provides automatic control in CE network. However, due to the diversity, decentralization, and increase in the number of CE devices the data traffic has increased exponentially. Moreover, the traditional static network infrastructure-based approaches need manual configuration and exclusive management of CE devices. Motivated from the aforementioned challenges, this article presents a novel Software-Defined Networking (SDN)-orchestrated Deep Learning (DL) approach to design an intelligent Intrusion Detection System (IDS) for smart CE network. In this approach, we have first considered SDN architecture as a promising solution that enables reconfiguration over static network infrastructure and handles the distributed architecture of smart CE network by separating the control planes and data planes. Second, an DL-based IDS using Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM) is designed to identify different attack types in the smart CE network. The simulations results based on CICIDS-2018 dataset support the validation of the proposed approach over some recent state-of-the-art security solutions and confirms it a phenomenal choice for next-generation smart CE network.**

***Index Terms*—Consumer Electronics, Cyber-Attacks, Deep learning, Internet of Things, Intrusion Detection System, Software-Defined Networking**

I. Introduction

THE Internet of Things (IoT) is a network of devices embedded with software programs and sensors that utilize the Internet to communicate data. The amalgamation of IoT into traditional Consumer Electronics (CEs) has revolutionized it into next-generation CEs with higher connectivity and intelligence. This improved data availability and automatic control in the CE network are made possible by the connectivity of sensors, actuators, appliances, and other consumer devices [1]. Nevertheless, CE devices connections are now remotely accessed anytime, anywhere in the world with the utilization of computing devices, including laptops, smartphones, and smartwatches, regardless of the network to which they are connected. These smart devices can be used in various fields, including smart homes [2].

The CE devices have significantly evolved in the last decade. According to a recent study, the CE segment might reach 2,873.1m users by 2025 while the Average Revenue Per User (ARPU) is expected to amount to US 317.10 billion [3]. Today, every device may create and share data online, contributing to the CE expansion. The traditional internet architecture is a complex system with a multitude of network components, i.e., routers, middleboxes, switches, and several layers, etc. due to decentralization [4]. Therefore, the traditional network design likewise struggles to adapt to the dynamic nature of modern applications. Moreover, the traditional static network infrastructure-based approaches need manual configuration and exclusive management of CE devices. Potentially, this results in inefficient use of all resources, which exposes systems to a variety of cyber-attacks [5]. However, it is clear from the current literature that smart CE networks are subject to various subtle, cyber threats, including botnets, brute force, Denial-of-Service (DoS), Distributed Denial of Service (DDoS), and web attacks [6]. The DDoS attack is identified as one of the most dangerous attacks on today's Internet. In DDoS, attackers use many compromised hosts to generate a lot of worthless traffic flow toward the target server, which causes servers to overload quickly by consuming their resources and making them unreachable to its user. Although DDoS attacks have been investigated for more than two decades, still it is the most compelling yet common attack approach in recent times [7].

In this regard, Software-Defined Networking (SDN) and Intrusion Detection System (IDS) can be considered the backbone for the next-generation smart CE network. An IDS is designed to detect threats and malicious behavior to defend the network against it [8]. However, for timely detection, the conventional signature-based IDS must continuously be updated and have information tagged as signatures or patterns of prospective threats. Furthermore, it is unable to detect zero-day threats. Hence, Intelligent threat detection techniques should be developed to identify and counteract the most recent cyber threats in smart CE networks, which are constantly expanding with time. However, due to the specific service needs of smart CE (such as low latency, resource limitations, mobility, dispersion, and scalability), attack detection fundamentally differs from conventional approaches in such a network. Therefore, an adaptable, dynamic, well-timed, and cost-effective detection framework against various growing cyber threats is urgently needed for the CE networks [9].

Danish Javeed is with the Software College, Northeastern University, Shenyang 110169, China. Email: 2027016@stu.neu.edu.cn,

Muhammad Shahid Saeed is with Dalian University of Technology, Dalian 116024, China. Email: shahidsaeedrana@gmail.com

Ijaz Ahmad is with Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518000, China. Email: ijaz@siat.ac.cn

Prabhat Kumar is with the Department of Software Engineering, LUT School of Engineering Science, LUT University, 53850 Lappeenranta, Finland. Email: prabhat.kumar@lut.fi.

Alireza Jolfaei is with the College of Science and Engineering, Flinders University, Adelaide, Australia. Email: alireza.jolfaei@flinders.edu.au

Muhammad Tahir is with the Department of Engineering and Computer Science, NUML Faisalabad Campus, Pakistan. Email: engr.tahir1987@gmail.com

SDN provides higher security, scalability, dynamism, efficiency, and reconfiguration. This is made possible by the built-in SDN architecture, in which the control functions are transferred to a central controller rather than being incorporated into the forwarding devices. This enables a controller to oversee and run a CE network from a broad perspective [10]. Motivated by the aforementioned challenges and discussions, this scientific study aims to provide a highly scalable and effective SDN-orchestrated IDS to safeguard the CE networks from severe multi-vector cyber-attacks. Additionally, our proposed detection framework is highly scalable, adaptable, economical, and well-timed while utilising the underlying CE resources without running out of resources. The main contributions of this work are as follows.

- The authors employed SDN and an intelligent Cuda-enabled Bidirectional Long Short-Term Memory (Cu-BLSTM) to quickly and accurately identify threats in CE networks.
- We compared the performance of the proposed Cu-BLSTM model with baseline techniques,i.e., Cuda-enabled Deep neural network (Cu-DNN) and Cuda-enabled Gated recurrent unit (Cu-GRU), to evaluate the proposed model thoroughly. For a fair comparison, all models have been trained and assessed in the same environment.
- A publicly accessible, intrusion dataset namely CICIDS-2018 dataset is employed for model training and evaluation. We also assessed the proposed model performance against the most recent detection models from the current literature and used 10-fold cross-validation technique to show balanced results.

The rest of the article is as follows. Section II presents related work. Section III gives complete details of the network model and proposed Cu-BLSTM-based detection scheme. Section IV presents the experimental setup and evaluation metrics. The results have been discussed in Section IV-A. Finally, the conclusion and future work is provided in Section V.

II. Related work

The CE is characterized by the integration of physical things into a network in a way that makes them active participants in corporate operations. These objects might include everything from network gear to sensors to home and healthcare products. CE is made up of a range of devices that can be wireless or wired and can be used in several places and networks. According to a recent Juniper report, more than 46 billion IoT devices were in operation by 2021. This includes sensors, actuators, and gadgets and represents a 200% growth over 2016 [11]. In any changing computer and network paradigm, IoT becomes an integral part of it. IoT transformation is growing exponentially, leading to significant growth in terms of revenue and automation. Because these devices are created to satisfy the individual demands of users, it is difficult to find a solution that works for everyone [12]. With security being a key concern right now, determining the security of these devices is difficult. These products are too diverse to be compared to a single procedure.

SDN and DL are combined for various benefits, including SDN's capacity to increase IoT's efficacy and Network Traffic Control in Vehicular Cyber-Physical Systems (VCPS) [13]. Application (AP), control (CP), and data planes (DP), as well as associated south- and north-bound APIs are part of an SDN architecture. By separating the DP and CP, the introduction of SDNs has resulted in a new networking paradigm. The AP only offers a thorough implementation of commands given by the other planes and is strategically distinct from the other planes. While the whole network's decision-making is the responsibility of the CP. It has customizable characteristics that effectively connect the DP with other outside communication technologies like the IoT [14]. The CP can allow the dynamic analysis of all data traffic passing across an IoT network. SDN provides bundled services for IoT, including flexibility, scalability, security, and resilience in multi-controller environment [15]. Thus, a precise method of network inspection for identifying suspicious activity, threats, and attacks is made possible by the convergence of IoT with SDN, and this integration offers a bright future for such a network. Significant interest has been shown in Deep Learning (DL) in the last decade, and its applications are being investigated across a wide range of study fields, including healthcare, automobile design, and legal implementation [16]. Additionally, various DL-based intrusion detection strategies have been put forth by researchers recently to defend against malicious threats and attacks in IoT networks. However, SDN-enabled, Intelligent IDS are still in the early stages of a thorough evaluation of diversified attacks in such networks.

The scientific literature has witnessed a plethora of research contributions made to secure IoT against a scattered array of internal and external attacks. The thorough development of DL-driven IDS is addressed in [17], which is primarily designed to detect common security attacks including port-based attacks and the DOS slowloris and DOS Hulk. To accomplish the intended security goals, the CICIDS2017 dataset is used for experimentation. The authors compared their proposed to existing techniques and exhibit a significant superiority in terms of productivity, with an attack detection accuracy of 98%. Another threat detection framework is proposed in [18] that is composed of two renowned classifiers i.e Spider Monkey optimization (SMO), and Stacked Deep Polynomial Network (SDPN). Along with DoS attacks, the designed model is capable to investigate major commonly occurring attacks such as User-to-Root (U2R) attacks, Remote-to-Local (R2L) attacks, probe attacks, etc. The designed framework is trained on the NDL-KDD dataset, and its performance is compared with benchmarked schemes. The model has significantly achieved 99.02% accuracy.

Authors have specifically designed an IDS to carefully detect DDoS attacks in large-scale IoT networks [19]. The system is evaluated on comprehensive performance metrics where it remarkably achieves high attack detection accuracy. The authors of [20] created a threat intelligence technique for industrial environments. The size of the UNSW-NB15 and power system datasets was reduced in this work using Independent Component Analysis. Researchers have combined LSTM with Variational Auto Encoder (VAE) technique to

TABLE I: Literature Review

Ref	Domain	Model	Dataset	Analysis
[17]	NIDS	DNN	CICIDS2017	The proposed model is designed to detect common security attacks including port- based attacks and DOS. The authors achieved 98% detection accuracy.
[18]	IoT	SMO, SDPN	NSL-KDD	A DL-based threat detection framework is proposed to counter DoS, U2R, R2L, and probe attacks. The model has shown 99.02% accuracy.
[19]	IDS	MLP, CNN, LSTM, TCN	BoT-IoT, CICDS2017, N-BaIoT	The designed model is a defensive framework against frequently occurring attacks in IoT. However, it causes significant computational overhead as well.
[20]	IIoT	Beta mixture-Hidden Markov Model (MH-MMs)	UNSW-NB15, Power system	Researchers have proposed a threat intelligence scheme for smart industries, that have achieved 98.45% accuracy on a comparison scale with five other benchmarked schemes.
[21]	IoT	LSTM-VAE	ToN-IoT, IoT-Botnet	The authors proposed a hybrid model to safeguard IoT environments and achieved efficient detection accuracy.
[22]	IoT	GRU, DVAE	ToN-IoT, IoT-Botnet	A blockchain and DL-based secure threat investigation framework is designed that is highly efficient in terms of communication cost and computation cost. The model has achieved 89.99% accuracy.
[23]	IDS	MLP. NLP	Self-generated dataset using Sixgill	The researchers proposed a threat discovery model for the dark web. Authors claim to obtain more than 90% accuracy with MLP.
[24]	IoT	CNN	BoT-IoT	An intrusion detection system for the vehicular network is presented to address frequently occurring IoT attacks and their proposed model has demonstrated 99.25% accuracy.

design another attack detection scheme for IoT. The system is effectively trained on ToN-IoT and IoT-Botnet datasets to enhance the learning experience of the proposed system. The system has proven its efficiency on an analytical performance scale regarding attack detection accuracy, training time, etc [21]. Blockchain and DL-based solutions are also regarded as the best choice for threat detection in IoT. Authors have proposed a threat detection scheme based upon the core concepts of the Gated Recurrent Unit (GRU) and Deep Variational Auto Encoder (DVAE) technique. The proposed actively proves its efficiency against potential adversaries [22]. In [23], the authors used Multi-Layer Perceptron (MLP) and Natural Language Processing (NLP) to discriminate between crucial and non-crucial posts on the dark web. Another intrusion detection approach, capable of detecting the presence of cyber threats in IoT, is presented [24]. The model is based on Convolutional Neural Network (CNN) classifier and is trained on the BoT-IoT dataset. CNN is also employed in another threat detection scheme proposed in [25], The model is specifically designed for botnet attacks, zero-day attacks, and DDoS attacks. The initial training of the proposed model is performed at the MQTT-IoT-IDS2020 dataset, and the run time performance is evaluated in terms of accuracy, precision, and Recall. CNN is integrated to design another anomaly detection framework purely designed to investigate suspicious entities over the network. The model is evaluated in comparison with some relevant security solutions on a performance scale of threat detection accuracy [26]. The authors of [27] designed an ensembled model consist of naïve bayes, QDA, and ID3 classifiers and achieved 95.10% accuracy. Further, in [28], the authors used federated learning based NIDS namely SecFed-NIDS to protect IoT networks from poisoning attacks. The authors achieved detection accuracy of 97.03% under CICIDS-2018 dataset. Another intrusion detection scheme using an ensemble approach consisting of ET, RF, and DNN is proposed in [29] to combat threats in IoT and Fog environments. BoT-IoT, IoTID20, NSL-KDD, and CICIDS-2018 datasets are used for a thorough evaluation of the model. The system

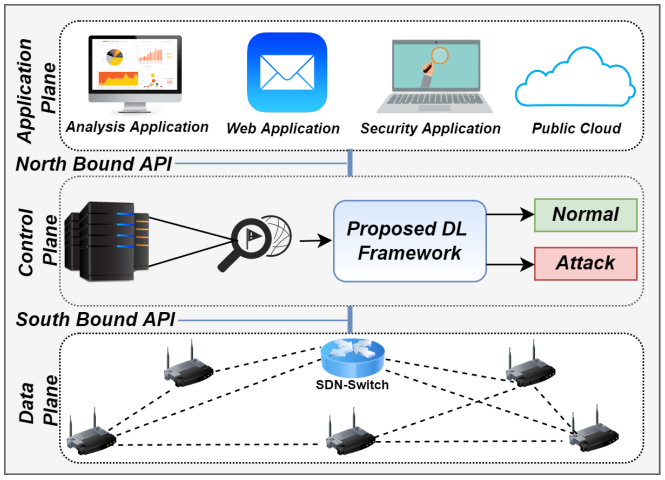

Fig. 1: Network Model.

significantly proves its effectiveness by achieving 98.21% accuracy on CICIDS-2018 dataset. The existing literature is summarized in Table I.

III. Methodology

A. Network Model

SDN is considered as a well-established method for building integrated networks in recent years. Its architecture separates the data planes and control planes, allowing simplicity and flexibility. Furthermore, in traditional networks, each router in the network can only perceive the network's local state. The lack of a full overview of the whole network makes it challenging to construct a potentially powerful defensive mechanism against cyber threats. SDN, on the other hand, provides a global network perspective and centralized control capabilities, making network statistics easier to obtain. In SDN, the control plane manages routing choices, data transfers, and traffic monitoring via application techniques. The data plane incorporates many CE devices, such as intelligent devices,

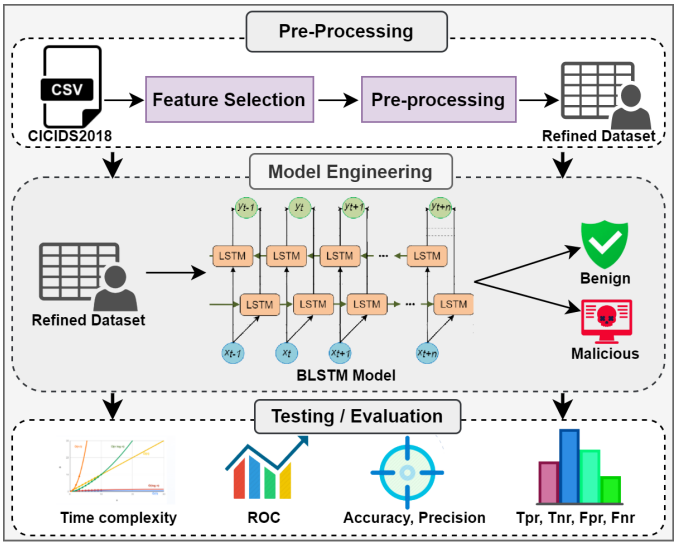

Fig. 2: Proposed Detection Scheme.

sensors, and other wireless technologies. The proposed Cu-BLSTM detection model is placed in the control plane for the following reasons; First and foremost, it is entirely adaptable and therefore capable of changing functionality. Secondly, it may extend numerous networks into its DP and give flexible solutions between linked CE devices and SDN control through an open-flow switch. Thirdly, the control plane has an SDN controller that can govern the whole network as the controller serves as a central decision-maker and a significant source of centralized control intelligence. CE and SDN's combination provides a simple network traffic monitoring solution for detecting assaults and suspicious activities. SDN offers a global network view of all the devices and the network. The combination of SDN with CE proposes a suitable method for monitoring network traffic to detect attacks, threats, and unwanted occurrences. Hence, SDN offers a bright future for the CE network. Fig 1 depicts the network model.

B. Proposed DL-driven BLSTM-based framework

A DL-driven Intelligent framework for threat detection in the CE network is provided, incorporating Cu-BLSTM. A low-cost, versatile, and powerful detection module is designed to detect threats across CE networks. Fig 2 depicts a comprehensive workflow of the proposed acquisition module. Cu-BSLTM consists of two layers with 200 and 100 neurons. In addition, we added one dense layer with 30 neurons. The proposed work utilized Relu as the activation function (AF) for all levels except the output layer. SoftMax, on the other hand, is employed in the output layer. The Categorical Crossentropy (CC-E) is used as a loss function (LF). Tests are run up to 10 epochs with 64 batch sizes to acquire effective findings. We utilized Cuda-enabled versions for GPU processing for an enhanced performance. Furthermore, the authors used the Keras framework, which is the foundation for Python TensorFlow. Cuda is a GPU-enhanced library that enables repeated readings, resulting in quicker multiplication of matrices. Moreover, we have used Cu-DNN and Cu-GRU as comparison models that have been trained and evaluated in the same environment. Cu-DNN consists of four dense layers with 100, 75, 50 and 30 neurons, respectively. Further, Cu-GRU comprises four layers of GRU with neurons of 500, 400, 300, and 100, respectively, with one dense layer of 03 neurons.

C. Cu-BLSTM

The proposed work used the Cu-BLSTM model for effective and timely threat detection in smart CE networks. An Artificial Neural Network (ANN) type called Recurrent Neural Networks (RNN) offers much promise for learning from earlier time steps [12]. RNN utilizes Back Propagation Through Time to constantly learn from previous timesteps. Standard RNN cannot perform better when timesteps overlap. The RNN employs feedback loops and links hidden units to preserve information over time. It can take consecutive inputs of any length and produce fixed-length outputs because of such features. The back-propagation causes error signals to disappear or explode, causing weights to fluctuate, resulting in poor system performance and gradient vanishing problems. Analysts focused on Long-Short-Term Memory (LSTM), as LSTM blocks can save information for a long time. RNN with LSTM blocks was designed to solve this issue. However, to address the shortcomings of the LSTM model, researchers improved it and is known as BLSTM. By traversing time steps both forward and backward, BLSTM makes the best use of the data. To generate two layers side by side, the architecture copies the first recurrent network. The input is sent to the first layer in its original form, while the second layer receives a copy that has been reversed. Complete detail of the BLSTM is given by the authors in [30]. The following are the transition functions for Cu-BLSTM gates:

$$\overrightarrow{\mathbb{M}_t} = \alpha(\overrightarrow{\mathbb{W}_m} * [\overrightarrow{\mathbb{H}_{t-1}}, \overrightarrow{\mathbb{Y}_t}] + \overrightarrow{\mathbb{B}_m}) \tag{1}$$

$$\overrightarrow{\mathbb{R}_t} = \alpha(\overrightarrow{\mathbb{W}_r} * [\overrightarrow{\mathbb{H}_{t-1}}, \overrightarrow{\mathbb{Y}_r}] + \overrightarrow{\mathbb{B}_r}) \tag{2}$$

$$\overrightarrow{\mathbb{C}_t} = \overrightarrow{\mathbb{R}_t} * \overrightarrow{\mathbb{C}_{t-1}} + \overrightarrow{\mathbb{M}_t} * \overrightarrow{\tilde{\mathbb{c}}_t} \tag{3}$$

$$\overrightarrow{\mathbb{N}_t} = \alpha(\overrightarrow{\mathbb{W}_n} * [\overrightarrow{\mathbb{H}_{t-1}}, \overrightarrow{\mathbb{Y}_t}] + \overrightarrow{\mathbb{B}_n}) \tag{4}$$

$$\overrightarrow{\mathbb{H}_t} = \overrightarrow{\mathbb{N}_t} * \tanh(\overrightarrow{\mathbb{C}_t}) \tag{5}$$

Where $\overrightarrow{\mathbb{M}_t}$, $\overrightarrow{\mathbb{R}_t}$, $\overrightarrow{\mathbb{C}_t}$, $\overrightarrow{\mathbb{N}_t}$, and $\overrightarrow{\mathbb{H}_t}$ are the input gate, reset gate, candidate cell, output gate, and the final state for forward process.However, $\overleftarrow{\mathbb{M}_t}$, $\overleftarrow{\mathbb{R}_t}$, $\overleftarrow{\mathbb{C}_t}$, $\overleftarrow{\mathbb{N}_t}$, and $\overleftarrow{\mathbb{H}_t}$ are for the backward process. $\overrightarrow{\mathbb{W}_m}$, $\overrightarrow{\mathbb{W}_r}$, $\overrightarrow{\mathbb{W}_n}$ and $\overleftarrow{\mathbb{W}_m}$, $\overleftarrow{\mathbb{W}_r}$, $\overleftarrow{\mathbb{W}_n}$ are the weight matrix for the input $\overrightarrow{\mathbb{Y}_t}$ and $\overleftarrow{\mathbb{Y}_t}$ respectively. $\overrightarrow{\mathbb{H}_{t-1}}$, $\overleftarrow{\mathbb{H}_{t-1}}$ are the hidden states of the previous block, while $\overrightarrow{\mathbb{B}_m}$, $\overrightarrow{\mathbb{B}_r}$, $\overrightarrow{\mathbb{B}_n}$ and $\overleftarrow{\mathbb{B}_m}$, $\overleftarrow{\mathbb{B}_r}$, $\overleftarrow{\mathbb{B}_n}$ are the biases. Further, $\overrightarrow{\mathbb{C}_{t-1}}$, $\overleftarrow{\mathbb{C}_{t-1}}$ are the previous states of the candidate cell.

$$\overleftarrow{\mathbb{M}_t} = \alpha(\overleftarrow{\mathbb{W}_m} * [\overleftarrow{\mathbb{H}_{t-1}}, \overleftarrow{\mathbb{Y}_t}] + \overleftarrow{\mathbb{B}_m}) \tag{6}$$

$$\overleftarrow{\mathbb{R}_t} = \alpha(\overleftarrow{\mathbb{W}_f} * [\overleftarrow{\mathbb{H}_{t-1}}, \overleftarrow{\mathbb{Y}_t}] + \overleftarrow{\mathbb{B}_r}) \tag{7}$$

$$\overleftarrow{\mathbb{C}_t} = \overleftarrow{\mathbb{R}_t} * \overleftarrow{\mathbb{C}_{t-1}} + \overleftarrow{\mathbb{M}_t} * \overleftarrow{\tilde{\mathbb{c}}_t} \tag{8}$$

$$\overleftarrow{\mathbb{N}_t} = \alpha(\overleftarrow{\mathbb{W}_n} * [\overleftarrow{\mathbb{H}_{t-1}}, \overleftarrow{\mathbb{Y}_t}] + \overleftarrow{\mathbb{B}_n}) \tag{9}$$

$$\overleftarrow{\mathbb{H}_t} = \overleftarrow{\mathbb{N}_t} * \tanh(\overleftarrow{\mathbb{C}_t}) \tag{10}$$

Algorithm 1 Cu-BLSTM detection framework

Input: Dataset= DT
Output: $Normal \rightarrow 0$, $Attack1 \rightarrow 1$, $Attack2 \rightarrow 2$, and so on.
Split DT in to DT_{train} and DT_{test}
for `each layer of BLSTM` **do**
    DT'_{train} = DT_{train} pre-proceessing
    $BLSTM_{Tmodel}$ = Train BLSTM model using DT'_{train}
end for
DT'_{test} = DT_{test} pre-processing
while True **do**
    $Predictattacktype \rightarrow BLSTM_{Tmodel}(DT'_{test})$
    if predict value = 0 **then**
        Return Normal
    else
        Return attack type
    end if
end while

As we used the softmax function in the output layer for multi-class classification. It is calculated by using equation 11. Further, the working of the proposed detection framework is shown in Algorithm 1.

$$J = \frac{e^{J}}{\sum_{j=1}^{K} e^{z_j}} \tag{11}$$

IV. Experimental Setup and Evaluation Metrics

The proposed model is trained using the Python version "Python 3.8" and using Keras. In addition, to enable comparable processing, the PC server is coupled with TensorFlow and the GPU-based package. The test was carried out using an Intel Core i7-7700 HQ CPU with a 2.80 GHz processor, along with a RAM 0f 16 GB, and a 6 GB, 1060 GPU. The proposed IDS is evaluated using CICIDS-2018 [31]. The dataset consist of one benign class along with various classes of attacks, i.e., Brute-force (XSS), DDoS, DoS, SSH, etc. However, in this work, we used seven classes of the dataset. Further, we pre-processed the dataset by using various techniques. First, we deleted all lines with empty values and non-numerics since they may have an impact on the performance of the test model. Since DL algorithms primarily handle numerical data, we used the label encoder, i.e., sklearn, to transform any non-numerical values into numerical values. Furthermore, one hot encoding is done on the output label since segment order may affect model performance, resulting in unforeseen effects. Data normalization is also carried out to improve model performance. For this purpose, we utilized the MinMax scalar function. Finally, we divided the dataset into 70% training and 30% testing data. The proposed model performance is evaluated using standard evaluation metrics such as accuracy (ACC), precision (PN), recall (RL), and F1-Score (FS). Furthermore, confusion matrix is used to obtain values for real positive (TP), true negative (TN), false positive (FP), Matthew's correlation coefficient (MCC), false negative (FN), and true negative transaction (TN) (FOR). The mathematical formulas are: $ACC = \frac{TP+TN}{TP+TN+FP+FN)}$; $RL = \frac{TP}{TP+FN}$; $PN = \frac{TP}{TP+FP}$; $FS = \frac{2(TP)}{2(TP+FP+FN)}$.

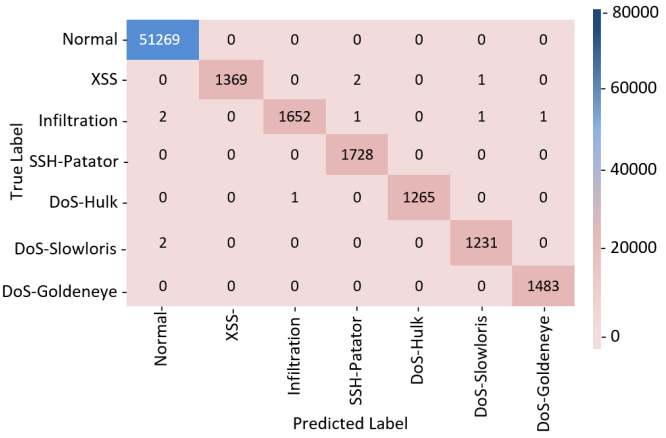

Fig. 3: Confusion matrix of Cu-BLSTM

A. Results and Discussion

This scientific study employed 10-fold cross-validation, and the findings are displayed in Table II to explicitly demonstrate unbiased outcomes. For a better understanding, each fold's results are shown in this section. The confusion matrix depicts the model's performance in the test data set. Data that is binary or multi-category. It is advantageous to assess the receiver's operational element's accuracy, precision, memory, and curve (ROC). The confusion matrix of the proposed model is depicted in Fig 3. The figure is evident that the proposed model identifies all five classes properly.

Further, the ROC curve corrects the given data so that positive and negative positive values may be compared. The extent of segregation is mostly determined by the success of various class division issues, as demonstrated by the ROC. The ROC curve structure is located between the TP and FP levels. Fig 4 depicts the ROC of the proposed Cu-BLSTM model, demonstrating the efficiency of the proposed model. The authors further provided the ACC, PN, RL, and FS of the CU-BLSTM model along with the baseline techniques. The detection accuracy reveals the Cu-BLSTM efficiency and performance. Fig 5 depicts the ACC, PN, RL, and FS of all three models. The proposed model achieved 99.57% ACC with 99.62% PN. Further, the proposed model is having FS and RL of 99.23% and 99.39% respectively. The figure is evident that the proposed Cu-BLSTM model outclassed the baseline models. We have further provided the per-class accuracy of all three models in Table III respectively. Other performance assessment methodologies, such as FP rate, FO rate, FD rate, and FN rate are also studied to properly evaluate the proposed model. Fig 6 demonstrates that our proposed model has values of 0.0033, 0.0022, 0.0033, and 0.0029 percent for the FP rate, FN rate, FD rate, and FO rate. Furthermore, Cu-GRU outperforms Cu-DNN in terms of such metrics. For a thorough assessment, we have further calculated the TPR, TNR, and MCC. These values are obtained using the uncertainty matrix

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2023.3277856

TABLE II: 10-Fold Results

Parameter	Models	1	2	3	4	5	6	7	8	9	10
ACC (%)	BLSTM	99.43	99.41	99.63	99.52	99.74	99.67	99.80	99.46	99.49	99.56
	DNN	98.59	98.53	98.90	99.21	98.81	99.1	98.81	99.42	99.23	98.86
	GRU	98.59	98.81	99.10	99.42	99.26	99.29	99.12	98.89	98.82	98.33
RL (%)	BLSTM	99.90	99.89	99.21	99.18	99.23	99.85	99.12	99.14	99.10	99.16
	DNN	98.59	98.52	98.43	98.52	98.21	98.30	99.14	99.65	99.14	99.16
	GRU	98.94	99.25	99.03	99.17	99.15	98.99	99.21	98.96	98.90	97.56
PN (%)	BLSTM	99.82	99.65	99.51	99.62	99.23	99.46	99.69	99.83	99.89	99.91
	DNN	98.95	99.25	98.31	98.23	98.29	98.56	98.64	98.79	99.25	99.65
	GRU	98.89	99.05	98.59	99.10	99.21	99.35	99.26	99.19	99.14	99.29
FS (%)	BLSTM	99.20	99.28	99.15	98.81	99.14	99.29	99.05	99.56	99.21	99.69
	DNN	98.69	98.51	98.56	98.86	99.12	98.87	98.64	98.93	99.12	98.71
	GRU	98.72	98.83	98.97	99.15	99.49	99.11	98.98	98.96	98.89	98.34

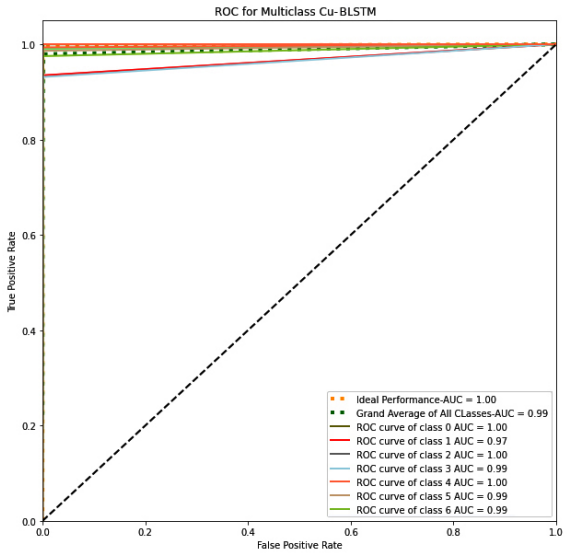

Fig. 4: ROC of Cu-BLSTM

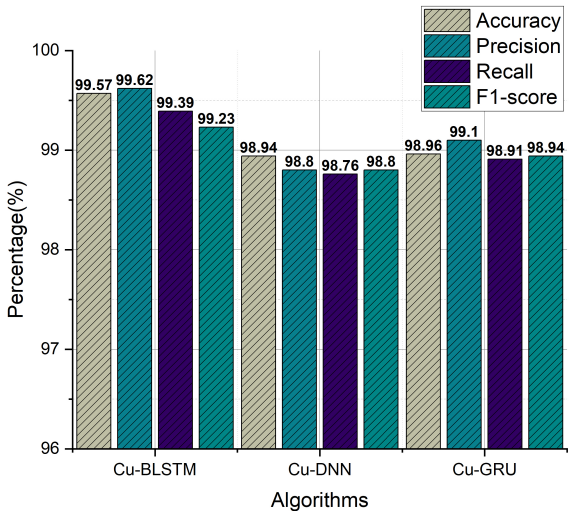

Fig. 5: Overall comparison of Cu-BLSTM against baseline models

TABLE III: Per-class ACC of Cu-BLSTM against baseline models

Models	BLSTM (%)	DNN (%)	GRU(%)
Normal	100	100	100
XSS	99.87	99.13	98.65
Infiltration	99.26	98.76	99.12
SSH-Patator	99.65	98.16	98.36
DoS-Hulk	99.10	98.65	98.70
DoS-Slowloris	99.68	98.73	98.71
DoS-Goldeneye	99.49	98.21	98.46

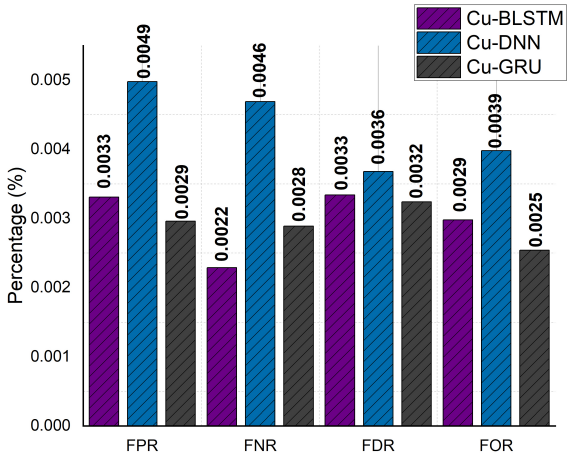

Fig. 6: Overall FPR, FNR, FDR, and FOR of Cu-BLSTM against baseline models

for comprehensive analysis. The proposed model, i.e., Cu-BLSTM yielded improved outcomes than Cu-DNN and Cu-GRU. Fig 7 depicts the performance of these models, where it is clear that the proposed model achieved values of 99.15, 99.34, and 99.31 percent respectively, thus proving the efficacy of the proposed model. Furthermore, we have provided the testing time of the proposed model in Fig 8. We did not considered the training time as it is mostly done offline. Fig 8 depicts the speed efficiency of the Cu-BLSTM and baseline models. The Cu-BLSTM model achieved a testing time of only 17.40 ms. On the other hand, Cu-DNN is having a better testing time of 25.2 ms than Cu-GRU. Finally, the performance of the proposed Cu-BSLTM model is compared with recent threat detection techniques from existing literature [27], [28], and [29], to validate its efficiency. The comparison is made in terms of ACC and the details are provided in Table IV. The table is evident that the proposed model outperformed the existing detection techniques, hence proving its efficiency.

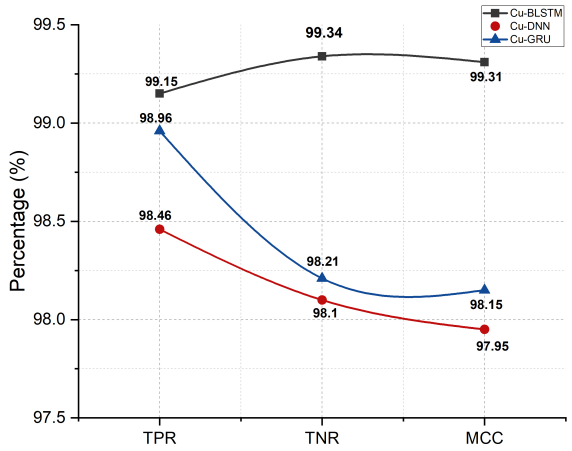

Fig. 7: Overall TPR, TNR and MCC of Cu-BLSTM against baseline models

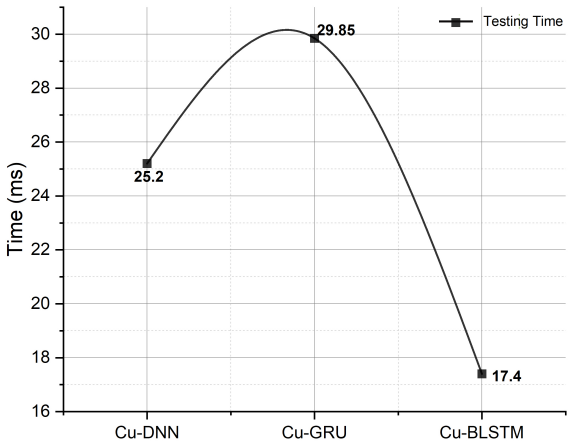

Fig. 8: Overall Speed Efficiency of Cu-BLSTM against baseline models

TABLE IV: Comparison of Cu-BLSTM with existing literature

Ref	Year	Model	Dataset	ACC (%)
Prop	2022	Cu-BLSTM	CICIDS-2018	99.57
[27]	2022	Ensembled model	CICIDS-2018	95.10
[28]	2022	SecFedNIDS	CICIDS-2018	97.03
[29]	2022	Ensemble approach	CICIDS-2018	98.21

V. Conclusion

In this article, to protect consumer electronics network, we proposed an intelligent intrusion detection system based on software-defined networking-orchestrated deep learning approach. Specifically, software-defined networking architecture was integrated with consumer electronics network to handle its distributed architecture and heterogeneous consumer electronic devices. Then, an IDS based on cuda-enabled bidirectional long short-term memory was proposed and deployed at control plane to enhance threat detection mechanism. We proved the effectiveness of the proposed IDS in terms of accuracy, precision and speed efficiency through experimental evaluation on the CICIDS-2018 dataset. We also compared the performance of the proposed IDS against some recent state-of-the-art technique. In the future we aim to train the model on different datasets to further improve intrusion detection in such networks. Finally, we endorse DL-based Intelligent models for efficient threat detection in next-generation smart consumer electronic networks.

References

[1] C. K. Wu, C. -T. Cheng, Y. Uwate, G. Chen, S. Mumtaz and K. F. Tsang (2022), "State-of-the-Art and Research Opportunities for Next-Generation Consumer Electronics," in *IEEE Transactions on Consumer Electronics*, doi: 10.1109/TCE.2022.3232478.

[2] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches, *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 32593306, 4th Quart., 2018.

[3] Statista. (2022, July 28). Consumer Electronics. In Statista, Electronics. Retrieved 14:57, July 28, 2022, from https://www.statista.com/outlook/dmo/ecommerce/electronics/consumer-electronics/worldwide

[4] Al Razib, M., Javeed, D., Khan, M. T., Alkanhel, R., & Muthanna, M. S. A. (2022). Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework. *IEEE Access*, 10, 53015-53026.

[5] Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K., & Kato, Y. (2020). Anomaly detection in smart home operation from user behaviors and home conditions. *IEEE Transactions on Consumer Electronics*, 66(2), 183-192.

[6] Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. *Electronics*, 10(8), 918.

[7] K. Kalkan, G. Gur, and F. Alagoz, "Defense mechanisms against ddos attacks in sdn environment", *IEEE Communications Magazine*, vol. 55, no. 9, pp. 175–179, 2017.

[8] L. N. Tidjon, M. Frappier, and A. Mammar, "Intrusion detection systems: A cross-domain overview," *IEEE Communications Surveys & Tutorials*, 2019.

[9] Prabhakar, G. A., Basel, B., Dutta, A., & Rao, C. V. R. (2023). Multi-channel CNN-BLSTM Architecture for Speech Emotion Recognition System by Fusion of Magnitude and Phase Spectral Features using DCCA for Consumer Applications. *IEEE Transactions on Consumer Electronics*.

[10] R. Kumar, P. Kumar, A. Kumar, A. A. Franklin and A. Jolfaei, "Blockchain and Deep Learning for Cyber Threat-Hunting in Software-Defined Industrial IoT," 2022 IEEE International Conference on Communications Workshops (ICC Workshops), 2022, pp. 776-781, doi: 10.1109/ICCWorkshops53468.2022.9814706.

[11] Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). *Sensors*, 21(14), 4884

[12] Saurabh, Kumar, et al. "LBDMIDS: LSTM Based Deep Learning Model for Intrusion Detection Systems for IoT Networks." 2022 IEEE World AI IoT Congress (AIIoT). IEEE, 2022.

[13] Jindal, Anish, et al. "SeDaTiVe: SDN-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems." IEEE network 32.6 (2018): 66-73.

[14] S. Khorsandroo, A. G. Sánchez, A. S. Tosun, J. Arco, and R. Doriguzzi-Corin, "Hybrid SDN evolution: A comprehensive survey of the state-of-the-art," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 107981.

[15] Ren, Xiaodong, et al. "Adaptive recovery mechanism for SDN controllers in Edge-Cloud supported FinTech applications." IEEE Internet of Things Journal (2021).

[16] J. Cui, M. Wang, Y. Luo, and H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," *Future Gener. Comput. Syst.*, vol. 97, pp. 275283, Aug. 2019.

[17] X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh and K.-H. Le, "Realguard: A lightweight network intrusion detection system for IoT gateways", Sensors, vol. 22, no. 2, pp. 432, Jan. 2022.

[18] Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 33(3), e3803.

[19] R. Ahmad, I. Alsmadi, W. Alhamdani et al., "A comprehensive deep learning benchmark for IoT IDS," vol. 114, pp. 102588, 2022.

[20] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," IEEE Access, vol. 6, pp. 32910–32924, 2018.
[21] M. A. Almaiah, A. Ali, F. Hajjej et al., "A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things," vol. 22, no. 6, pp. 2112, 2022.
[22] Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., & Srivastava, G. (2022). P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot. *IEEE Transactions on Industrial Informatics*, 18(9), 6358-6367.
[23] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, "Exploring the dark web for cyber threat intelligence using machine leaning," in Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), Jul. 2019, pp. 200–202.
[24] L. Yang, and A. J. a. p. a. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," 2022.
[25] I. Ullah, and Q. H. J. I. A. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," vol. 9, pp. 103906-103926, 2021.
[26] A. Anand, S. Rani, D. Anand et al., "An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications," vol. 21, no. 19, pp. 6346, 2021.
[27] Lalduhsaka, R., Nilutpol Bora, and Ajoy Kumar Khan. "Anomaly-Based Intrusion Detection Using Machine Learning: An Ensemble Approach." International Journal of Information Security and Privacy (IJISP) 16.1 (2022): 1-15.
[28] Zhang, Zhao, et al. "SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system." Future Generation Computer Systems 134 (2022): 154-169.
[29] de Souza, Cristiano Antonio, Carlos Becker Westphall, and Renato Bobsin Machado. "Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments." Computers & Electrical Engineering 98 (2022): 107694.
[30] Javeed, D., Gao, T., Khan, M. T., & Shoukat, D. (2022). A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22(4), 1582.
[31] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116.

Danish Javeed is currently pursuing the Ph.D. degree in Software Engineering, specializing in Information Security with the Software College, Northeastern University, China under the prestigious fellowship of Ministry of Education funded by the Government of China. He got his M.E degree in Computer Applied Technology from Changchun University of Science and Technology, China, under the same fellowship in 2020. He is also working on various research projects with researchers from LUT School of Engineering Science, LUT University, Lappeenranta, Finland. He has many research contributions in the area of Deep Learning, Cybersecurity, Intrusion Detection and Prevention System, the Internet of Things, Software-defined Networking and Edge Computing. He has authored or coauthored over 10+ publications in high-ranked journals and conferences. He is also an IEEE Student Member.

Muhammad Shahid Saeed is currently pursuing the Ph.D. degree in Software Engineering, with Dalian University of Technology, PR China, under the prestigious fellowship of Ministry of Education funded by the Government of China. He is also working on various projects in collaboration with researchers from Northeastern University, China and LUT University, Lappeenranta, Finland. He has many research contributions in the area of the Internet of Things, Industry 4.0, and Intrusion Detection System.

Ijaz Ahmad is currently pursuing the Ph.D. at China's Shenzhen Institute of Advanced Technology (Siat) on pattern recognition and intelligent systems, under the ANSO Scholarship. He has over 15 publications in highly ranked journals and conferences. His research interests include Intrusion Detection and Prevention in the Internet of Things and Deep Learning.

Prabhat Kumar received his Ph.D. degree in Information Technology, National Institute of Technology Raipur, Raipur, India, under the prestigious fellowship of Ministry of Human Resource and Development (MHRD) funded by the Government of India in 2022. Thereafter, he worked with Indian Institute of Technology Hyderabad, India as a Post-Doctoral Researcher under project "Development of Indian Telecommunication Security Assurance Requirements for IoT devices". He is currently working as Post-Doctoral Researcher with the Department of Software Engineering, LUT School of Engineering Science, LUT University, Lappeenranta, Finland. He has many research contributions in the area of Machine Learning, Deep Learning, Federated Learning, Big Data Analytics, Cybersecurity, Blockchain, Cloud Computing, Internet of Things and Software Defined Networking. He has authored or coauthored over 35+ publications in high-ranked journals and conferences, including 13+ IEEE TRANSACTIONS paper. One of his Ph.D. publication was recognized as a top cited article by WILEY in 2020-21. He is IEEE Consumer Technology Society (CTSoc) Technical Committee member in Machine learning, Deep learning, and AI in Consumer Electronics. He is also an IEEE Member.

Alireza Jolfaei is an Associate Professor of Networking and Cyber Security in the College of Science and Engineering at Flinders University, Adelaide, Australia. He is a Senior Member of the IEEE and a Distinguished Speaker of the ACM. His main research interest is in Cyber-Physical Systems Security. He has published over 100 papers, which appeared in peer-reviewed journals, conference proceedings, and books. Before Flinders University, he has been a faculty member with Macquarie University, Federation University, and Temple University in Philadelphia, PA, USA. He received the prestigious IEEE Australian council award for his research paper published in the IEEE Transactions on Information Forensics and Security. Dr. Jolfaei is the IEEE Consumer Technology Publication Board member and the Editor-in-Chief of the Consumer Technology Society World Newsletter. He has served as the Regional Chair of the IEEE Technology and Engineering Management Society's Membership Development and Activities for Australia. He has served as a program coChair, a track Chair, a session Chair, and a Technical Program Committee member, for major conferences, including IEEE TrustCom and IEEE ICCCN.

Muhammad Tahir is currently working as an Assistant Professor in the Department of Engineering & Computer Science, NUML (Faisalabad Campus), Pakistan. He received his Ph.D. in Information & Communication Engineering from Changchun University of Science and Technology, PR China. His research interests include the Internet of Things, Information and Signal Processing, Underwater Wireless Communication using EM waves and Energy Optimization in WSNs.