IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 21, 2022, accepted April 30, 2022, date of publication May 3, 2022, date of current version May 23, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3172304

Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework

MOHAMMAD AL RAZIB[1], DANISH JAVEED[2], MUHAMMAD TAIMOOR KHAN[3], REEM ALKANHEL[4], (Member, IEEE), AND MOHAMMED SALEH ALI MUTHANNA[5]

[1]School of Computer Science, Changchun University of Science and Technology, Changchun 130022, China
[2]Software College, Northeastern University, Shenyang 110169, China
[3]Riphah Institute of Science and Engineering, Islamabad 44000, Pakistan
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[5]Institute of Computer Technologies and Information Security, Southern Federal University, 347922 Taganrog, Russia

Corresponding author: Reem Alkanhel (rialkanhal@pnu.edu.sa)

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

ABSTRACT Internet of Things (IoT) is an instantly exacerbated communication technology that is manifesting miraculous effectuation to revolutionize conventional means of network communication. The applications of IoT are compendiously encompassing our prevalent lifestyle and the integration of IoT with other technologies makes this application spectrum even more latitudinous. However, this admissibility also introduces IoT with a pervasive array of imperative security hazards that demands noteworthy solutions to be swamped. In this scientific study, we proposed Deep Learning (DL) driven Software Defined Networking (SDN) enabled Intrusion Detection System (IDS) to combat emerging cyber threats in IoT. Our proposed model (DNNLSTM) is capable to encounter a tremendous class of common as well as less frequently occurring cyber threats in IoT communications. The proposed model is trained on CICIDS 2018 dataset, and its performance is evaluated on several decisive parameters i.e Accuracy, Precision, Recall, and F1-Score. Furthermore, the designed framework is analytically compared with relevant classifiers, i.e., DNNGRU, and BLSTM for appropriate validation. An exhaustive performance comparison is also conducted between the proposed system and a few preeminent solutions from the literature. The proposed design has circumvented the existing literature with unprecedented performance repercussions such as 99.55% accuracy, 99.36% precision, 99.44% recall, and 99.42% F1-score.

INDEX TERMS Deep learning (DL), Internet of Things (IoT), intrusion detection system (IDS), distributed denial of service (DDoS), software-defined networking (SDN).

I. INTRODUCTION

The current century has witnessed an evolutionary growth in information and communication technologies that intend to transform traditional patterns of network communication. Internet of Things (IoT) is such a formidable network communication technology that is revealing marvels in every aspect of our lives by acquainting contemporary concepts of data transmission over networks. The anecdote starts with the unified architecture of IoT that contains a variety of heterogeneous intelligent devices mutually connected with the integration of smart sensors [1]. These interconnected devices can communicate with one another without any human interaction yielding an entirely automated environment [2]. There exist a divergent assortment of communication protocols that comes to govern this automated communication. The expanding circle of IoT applications directly projects its effectiveness and appropriateness. These applications subsist every outskirt of our routing life such as smart homes, transport, health care, education, industrial manufacturing, supply chain management and many more [3]. Along with numerous benefits, the heterogeneous and prevalent nature of IoT also makes it susceptible to a variety of crucial security threats e.g. Denial of Services (DoS) attacks, data sniffing,

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

spoofing, and network resource occupancy, etc [4], [5]. All these phenomena urge a vigorous need for vital security countermeasures to address such sort of potential security concerns. The involvement of the internet in large scale IoT environments encourages cyber security solutions to overcome these dynamic threat metrics. So a plethora of cutting edge technologies are rubbing shoulders together to ensure security around IoT environments against internal and external security threats [6]. Software-Defined Networks (SDN) based solutions are considered to be more prominent to obtain these desired security objectives [7]. Artificial Intelligence (AI), and Machine Learning (ML) are some other significantly prominent technologies that are progressively functioning to obtain the same goals [8]. These technologies can be interlaced together and this amalgamation can provide an aggregated response to counter a diverse variety of security threats in IoT. Over the past decade, the conglomeration of ML with SDN based approaches has flourished as a prominent tool to detect the presence of security threats in IoT communication [9]. SDN based approaches legislatively contribute towards the identification of anonymous activities whereas ML-based approaches provide supportive strength towards the durability of detection mechanism [10], [11]. The programmable features of SDN propound ample room for AI as well, where AI-based algorithms in acquaintance with SDN based frameworks are contemplated as an exquisite solution to overwhelming security threats in IoT [12], [13]. A conventional SDN framework can be majorly classified into three planes referred to as control plane, data plane and application plane [14]. The control plane is entirely configurable and can possess the potential capabilities to integrate interloper networks such as IoT with the data plane. The data plane then ensures a smooth flow of data across both participants under the regulations of the control plane [15]. The control plane in other words is capable to control the inner communicational infrastructure of IoT by taking a pilot control over the assemblage system. All the heterogeneous nodes in the IoT network are dynamically supervised through the control plane where surveillance of cyber threats can be performed in an acclaimed fashion [16], [17]. The DL-based approach offers extensive strengths in the analysis of traffic patterns. The classic deep learning-based framework is initially trained on a comprehensive dataset where it matriculates through a vast range of exclusive security threats. Then the system is deployed in the actual communication environment where it can momentously identify the existence of relevant malicious entities in the concerned communicational network [18]. All these consequential impressions are the core motivation that prodigiously fascinated us to propose a deep learning-driven, SDN-based, intrusion detection system for IoT based communication environments.

A. CONTRIBUTION

Our major contributions in the under contention research study are enlisted as follows:

- We contemplated a deep learning-inspired, SDN-enabled intrusion detection system labelled as Cu-DNNLSTM to interrogate the presence of emerging cyber threats in IoT environments.
- CICIDS2018 dataset is used to train and enhance the threats detection capabilities of the proposed model.
- The constituted framework encircles a consolidated sequence of Cu-DNNGRU and Cu-BLSTM classifiers that are acquired as a comparison to the same dataset.
- The performance of the designed model is evaluated on a comparative scale with existing solutions in the same regard.
- Simulation results insinuate to strengthen the proposed model in terms of efficient threat detection, high accuracy, significant precision, low resource consumption, and less computational overhead.
- Finally, 10 fold cross validation is conducted to show unbiased results.

B. ORGANIZATION

This scientific study is organized in a systematic order in which, Section 2 discloses detailed background along with relevant scientific literature. Section 3 contains the proposed methodology accompanied by the elaboration of the dataset, and algorithms. Section 4 spotlights the performance evaluation setup used to validate the performance of the proposed model. The obtained results are discussed in Section 5, and finally, the study is concluded in Section 6 of this paper.

II. BACKGROUND AND RELATED WORK

A. IOT AND SDN

IoT is an instantly evolving communication technology that comes to transmute the long-established mediums of communication. The synchronized and automated connectivity among various heterogeneous devices is the core strength of IoT [19]. The applications of IoT canvasing every facet of our lives, and the utility circle of IoT is still expanding. IoT also possesses the capability to be assimilated with other states of the art technologies to share the harmonized objectives [20]. The catalogue of such technologies encloses machine learning, SDN, fog computing, etc. Moreover, cloud sharing, big data analysis, blockchain spectrum etc are some other third party consolidated technologies that can be actively synchronized with IoT [21].

SDN is desegregated with IoT for bounteous reasons as SDN is capable to enhance the effectiveness of IoT in the manifold. SDN comprises three basic layers that transparently govern its communication architecture. These layers are widely categorized as the control plane, data plane and the application plane [22], [23]. The application plane is strategically different from the rest of the planes and it only provides a comprehensive implementation of commands made by the other planes [24]. The control plane comes with programmable features that adequately interlinked the aspiring outsider communication technologies such as IoT within the

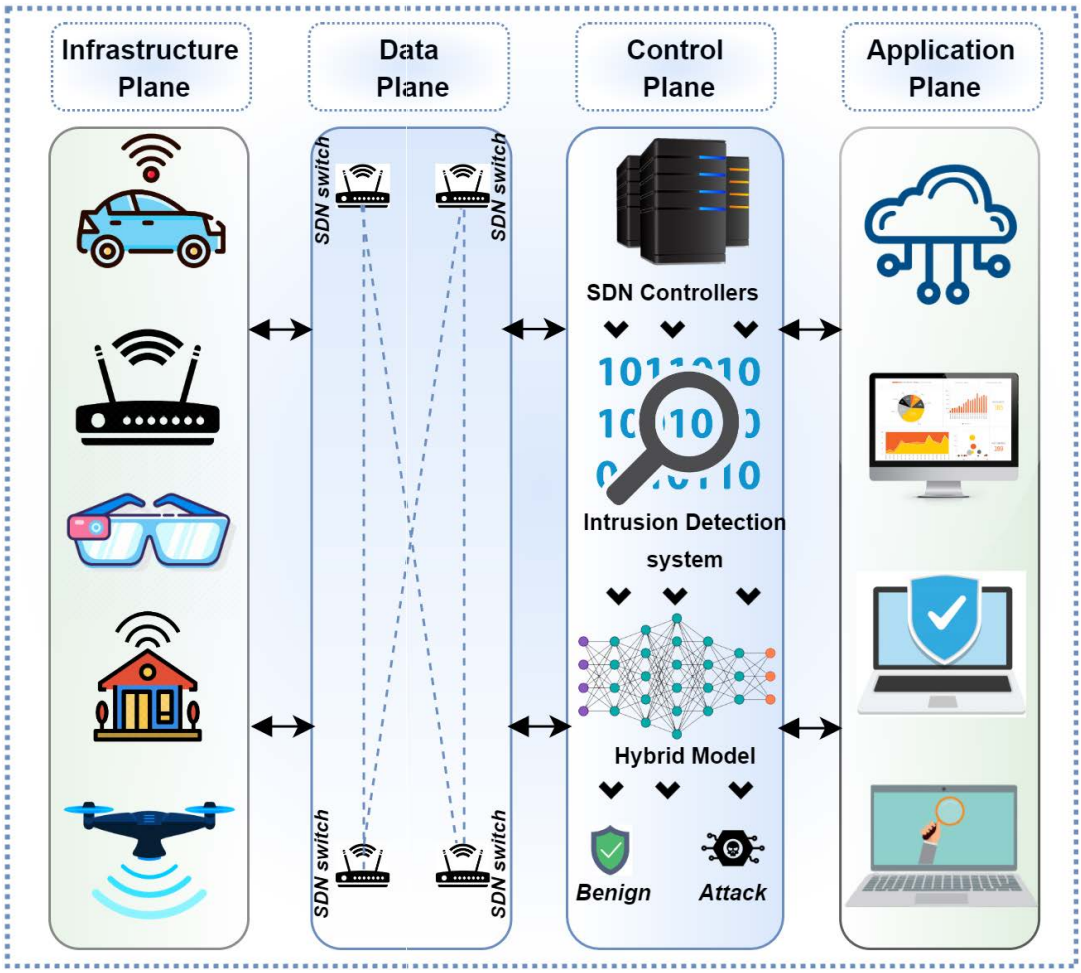

FIGURE 1. Proposed network framework.

data plane [25]. The control plane can further take conclusive control upon the communication nodes of IoT. All the data traffic transmitting over an IoT network can be dynamically analysed through the SDN control plane. In this way, SDN offers conglomerated services, i.e., customization, scalability, and security in IoT [26].

B. RELATED WORK

The aggrandised range of IoT applications makes it influenceable against a multifariousness of security threats that need to be encountered. SN based solutions are considered as an optimal choice to ensure secure, and reliable communication in IoT environments. A plethora of scientific attempts have been made in this regard, and we have included some of such meaningful contributions in this study.

Researchers proposed a Long-Short Term Memory (LSTM) approach to detect the presence of security threats in IoT. The whole traffic stream is analysed, and the suspicious entities are predicted to mitigate the chances of security breaches. Various datasets i.e CIDCC-15, UNSW-NB15, and NSL-KDD are amassed to evaluate the training matrix. A Bio-inspired Firefly Swarm Optimization (FSO) is further integrated with the proposed system to reduce the computational overhead [27]. A comprehensive feature set containing abnormal traffic patterns acts as an essential component to investigate the anonymous behaviour of malicious entries. The same sort of attempt is made in [28], where authors proposed an Intrusion Detection System (IDS) that withholds the ideal feature set used for threat detection. LightGBM is used for feature screening, where, PPO2 and ReLU are used to strengthen the threat detection mechanism. [29] addresses the detailed elaboration of deep learning-driven IDS mainly designed to investigate common security attacks such as DOS slowloris, DOS Hulk, and port scanning based attacks. The system is integrated with the CICIDS2017 dataset to achieve the desired security objectives. The designed model is then evaluated with existing solutions and shows significant productive superiority with an attack detection accuracy of 98%. Another DL inspired intrusion detection scheme is presented in [30], which is purely inspired by Convolutional Neural Networks (CNN). Authors claim to investigate and further categorize the existence of crucial security threats in IoT. CICIDS2017 and UNSW-NB15 are integrated to enhance the attack detection compatibilities of the proposed system. However, significantly high resource consumption is noticed which makes this scheme not

appropriate for resource-constrained networks. Another DL-driven intrusion detection scheme is designed in [31]. Binary classifier and multiclass classifier are employed in accompanying with BOT-IoT dataset. The designed scheme is capable to identify abnormal traffic with appreciable accuracy of 99%. Text-CNN and Gated Recurrent Unit (GRU) classifiers are categorized as the optimal choice for sequential data extraction as a language model. This pattern enhances the selection possibilities of best features, which typically tends to enhance the F1 score. Authors employed these classifiers in integration with KDD99, ADFA-LD datasets to effectively monitor abnormal activities in an IoT communication environment with 98% precision [32]. CNN is employed to another anomaly detection mechanism in an affix with BOT-IoT, and MQTT-IoT-IDS2020 datasets. The core purpose is to evaluate traffic patterns to discover suspicious events in large scale networks [33]. A hybrid feature selection model is acquired to fetch mostly commonly used features for attack detection by segmenting TCP/IP packets. NSL-KDD and UNSW-NB15 are further interlinked to strengthen the proposed system. The performance is evaluated in terms of industrial scenario where the proposed model seems to beat existing solutions with an admirable security matrix containing 97% accurate precision [34]. A combination of Single-hidden Layer Feed-forward Neural Network (SLFN) and LSTM classifier is considered as an effectively practicable choice to clip healthy features with more probabilities of being used in threat detection. Authors have adopted these two classifiers to initiate a multi-layer threats classification approach. The IoT-ID20 dataset is procured for training purposes [35]. The proposed framework produces momentous consequences for threat detection and classification. However, the system seems to consume voluminous resources of the network. Deep learning affected malicious packet filtering approach is proposed for SDN-based IoT communication scenarios [36], Mirari data set and a manually formulated data set the video injection dataset are subsisted together to achieve the desired filtration target. DNN classifier is embedded to control the entire processing infrastructure. The proposed system is only capable to deal with DDoS attacks, and port scan attacks. A multi-CNN based approach is adopted with an alliance of the NSL-KDD dataset [37]. The authors aim to interrogate adversaries in industrial IoT. Simulation results prove the compatibility of the designed framework, however, a notable complexity is also experienced in large-scale networks. DoS attacks are responsible to slow down the overall performance of the system by casting aggregating impacts on central resources. Researchers aim to design a competent detection mechanism to examine the compromised nodes that are dedicated to creating DoS and DDoS attacks [38]. The DoS attacks are catered in a hierarchical pattern by using the approach presented in [39]. To fulfil the claim, researchers have incorporated three generic classifiers that are best known by their competencies to symmetrical categorize the traffic streams. CICIDS2017 and BOT-IoT datasets are used for training purposes. The designed framework exhibits its strength towards DoS attack detection with 99% accuracy and notable precision. Another DL-driven IDS is presented in [40], which is trained on a customised dataset by the researchers. Decision Tree (DT), Multilayer Perceptron (MLP), and LSTM are the classifiers employed to boost the detection potential of the proposed framework. Adversaries are discovered with higher comparatively higher accuracy of 98%. Keylogging attacks, and Data exfiltration attacks are gaining conspicuous popularity in SDN-based IoT communication networks. Authors have constructed a robust IDS to diagnose these attacks in IoT. C5 and SVM classifier are retrieved to design this framework and BoT-IoT is interlinked for the appropriate learning process. The proposed system pays high accuracy of 99% for attack detection, however, communication delays are experienced while evaluating the designed model [41]. User-to-Root (U2R) attacks, Probe attacks, and Remote-to-Local (R2L) attacks are categorized as detrimental security concerns towards the integrity of a communication system. Researchers have acquired Spider Monkey Optimization (SMO) algorithm, and Stacked Deep Polynomial Network (SDPN) algorithm to design a detection mechanism for such security concerns. NSL-KDD is inter-bounded to train the system and on an evaluation scale, the proposed model have shown 97% accuracy for attack detection with a precision of 95% [42]. Man in the Middle (MITM) attack, Reconnaissance, and spoofing attack can also be classified into major security threats for IoT. Researchers have designed an IDS with the integration of SVM, Naïve Bayes, and MLP classifiers. The system is trained on the NSL-KDD dataset, and the performance is evaluated in a scalable virtual simulation environment. The proposed system shows 98% accuracy towards attack detection with a distinguished extensive precision [43]. In [62] the authors used a novel approach ''CANintelliIDS'' for intrusion detection on Controller Area Network (CAN). The authors used a combination of CNN and GRU and claimed that the combination of these two models increases the performance of detection. The authors achieved an F1-score of 93.79 %, 93.69 % precision, and 93.91 % recall. The authors in [63] used a temporal weighted averaging algorithm for asynchronous federated learning (AFL) to simulate an intrusion detection environment. The authors trained and tested the proposed model on the NSL-KDD dataset and achieved an accuracy of 99.50 % respectively. The authors of [64] proposed a Principal Component Analysis (PCA), Grey-Wolf Optimizer (GWO) hybrid model based on DNN for efficient and effective threat detection in the Internet of Medical Things (IoMT) environment. The authors claimed that their proposed model outclassed the existing ML techniques with a 15 % increase in detection accuracy and a 32 % decrease in time complexity. The related work is summarized in Table 1.

III. METHODOLOGY

A. PROPOSED NETWORK MODEL

SDN is acknowledged as a granted solution to boost the paramount potential of a dynamic heterogeneous

TABLE 1. Existing literature.

Ref	Year	Proposed Work	Classifier	Dataset	Limitations
[27]	2022	A hybrid traffic analysis mechanism is proposed to predict security threats in IoT	LSTM	CCC-15, UNSW-NB15, NSL-KDD	A considerable increase in Latency
[28]	2022	An IDS is designed to detect and classify malicious security concerns.	PPO2,ReLU	Dataset published by Oakridge Lab	The proposed system demands high computational resources.
[29]	2022	A DNN based IDS is formulated to analyze common security attacks	DNN	CICDS2017	The designed model is complex to adopt.
[30]	2022	An attack prevention scheme is proposed for IoT	CNN	UNSW-NB15, CICDS2017	Highly resource consumption is experienced.
[31]	2021	An IDS is designed to analyze abnormal traffic	Binary, Multiclass	BOT-IoT	Extensive communication delays.
[32]	2021	A traffic monitoring framework is presented.	Text-CNN,GRU	KDD99, ADFA-LD	Not feasible for large scale networks.
[33]	2021	An anomaly detection mechanism is designed for IoT networks	CNN	BOT-IoT, IoT-IDS2020	Computational overhead increases.
[34]	2021	An IDS is proposed for industrial IoT	DNN	NSL-KDD, UNSW-NB15	Communication breakage experiences.
[35]	2021	A multilayer threat detection and classification model is presented	SLFN, LSTM	IoT-ID20	Extensive computational resources required.
[36]	2020	A malicious packet filtering mechanism is presented.	DNN	Mirari dataset	Not suitable for resource-constrained environments.
[37]	2020	An efficient and robust IDS is designed for industrial IoT	Multi CNN	NSL-KDD	Complexity increases in large scale networks.
[38]	2020	DoS attack detection mechanism is proposed	DNN	NSL-KDD	The system experiences higher latencies.
[39]	2020	Researchers proposed a hierarchical IDS to overcome DoS attacks	REP Tree, Forest PS	CICIDS2017, BOT-IoT	Not compatible for network extension.
[40]	2020	A comprehensive anomaly detection framework is proposed	DT, RF, GBT,MLP, SVM, LSTM	Customised dataset	Extensive computational resources required.
[41]	2019	Researchers have designed an intrusion detection scheme to diagnose Keylogging attacks, and Data exfiltration attacks	C5, SVM	BOT-IoT	Notable communication delays occur.
[42]	2019	A threat detection model is proposed to identify U2R, R2L attacks	SMO, SDPN	NSL-KDD	Not convenient for dynamic networks.
[43]	2019	An IDS is proposed for MITM, Reconnaissance, and Replay attacks	Naïve Bayes, SVM, MLP, RF	NSL-KDD	Significant computational overhead is examined.

network [44]. Moreover, scalability, heterogeneous connectivity, customizable communication, surveillance, and security are some other ascendancy characteristics of SDN that must need to be discussed over here [45], [46]. The core charisma lies in the core architecture of SDN as it compasses two processing layers and one interface layer. The interface layer is only responsible to implement, and reflecting the decisions made by the processing layers [47]. However, processing layers included the control plane and data plane, that actively participate in the decision making as well as facilitate other integrated technologies. The control plane introduces an entirely programmable architecture that provides a customizable administrative experience over the network [48]. It further can authorize the IoT devices into the data plane. We proposed a DNNLSTM model to overcome the emanated cyber threats in the industrial IoT. The designed model is embedded with the control plane of SDN because of multitudinous reasons. The control plane of SDN is acquainted with an integral programmable interaction that further helps to control the fundamental operations of IoT. Hence it regularizes the communication mechanism in IoT networks and provides heterogeneous connectivity, dynamic scalability, and dominant governance. The data plane comprising of prevalent IoT devices that are transmitting data across the network and this data is interlinked with the control plane through open flow switches. Hence, the control plane becomes capable to expedite the IoT devices into its data plane that opens doors for data filtering, traffic monitoring, and general inspection of communication streams. Thus, by integrating SDN with IoT, the emerging cyber threats along with the presence

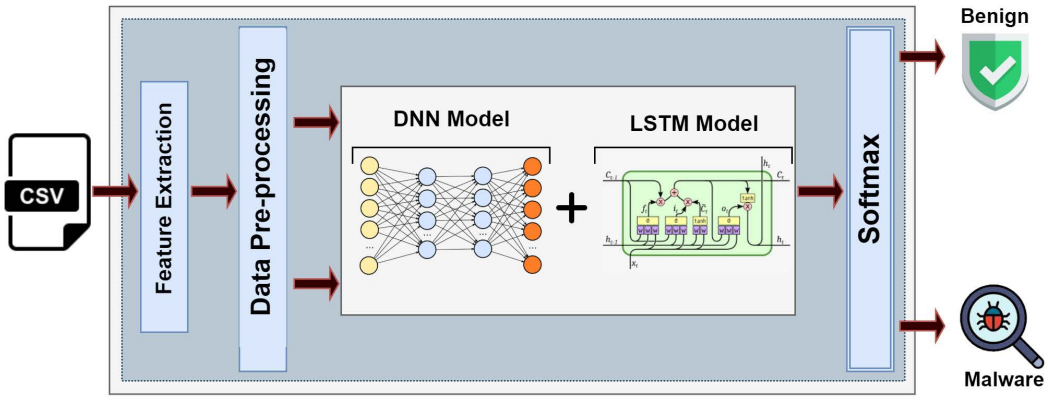

FIGURE 2. Proposed hybrid detection framework.

TABLE 2. Details of hybrid models.

Algorithm	Layers	Neurons/kernel	AF/LF	Epochs	Optimizer	Batch-Size
Cu-DNNLSTM	Cu-DNN (2) Cu-LSTM (1) Dropout Dense (3) Output Layer	500, 300 200 – 200,100,50 02	Relu/CC-E Relu/CC-E – – Softmax	10	Adamax	32
Cu-DNNGRU	DNN Layer (2) GRU Layer (1) Dropout Dense (3) Output Layer	500,300 200 – 200,100,50 02	Relu/CC-E Relu/CC-E – – Softmax	10	Adamax	32
Cu-BLSTM	BLSTM Layer (3) Dropout Dense (3) Output Layer	500,300,200 – 200,100,50 02	Relu/CC-E – – Softmax	10	Adamax	32

of other suspicious antagonists can be efficaciously overthrown. Figure 1 is projecting the proposed architecture.

B. PROPOSED HYBRID DETECTION SCHEME

A DL driven hybrid approach for intrusion detection in IoT is proposed, i.e., Cu-DNNLSTM. The systematic architecture of the proposed model can be witnessed in Figure 2. We have further used Cu-LSTMGRU and Cu-BLSTM to compare their performance with our proposed model. The designed model is comprised of various layers holding a discernible functionality. The Cu-DNNLSTM comes with an asymmetric layer model in which Cu-DNN possess 500 and 300 neurons, however, Cu-LSTM occupies only 200 neurons. Softmax is used as an Active Function (AF) in consanguinity with Adam optimizer. The performance of the purposed model is evaluated under diverse performance metrics, and the simulations are performed until 10 epochs with a batch size of 32. To obtain empirical objectives, we used Cuda-enabled versions with GPU processing to obtain the desired performance. Additionally, the proposed model made use of the Keras framework in conjunction with the Tensor Flow for Python at the backend.

For a thorough performance evaluation, a comparison is conducted with two meticulously identical classifiers i.e DNNGRU classifier and BLSTM classifier. The DNNGRU classifiers hold one layer of DNN with 500 and 300 neurons respectively, and one layer of GRU with 200 neurons. Moving forward, the BLSTM classifier engrossed a BLSTM layer with 500, 300 and 200 neurons respectively. Table 2 conscripts detailed information of the proposed model and other classifiers.

C. DATASET DESCRIPTION

Dataset is an integral component of every DL driven intrusion detection scheme. The selection of an adequate and commensurate dataset actively reinforce the threat detection scheme [49]. There exist a diverse variety of auxiliary datasets that comes to conspire these intrusion detection schemes. UNSW-NB15 [50], NSL-KDD [51], BOT-IoT [52], ADFA-LD [53] are some of these commonly endorsed dataset. However, along with numerous benefits, some prejudices have also

TABLE 3. CICIDS2018 dataset details.

Classes	Instances
Benign	51,956
Brute Force	2795
Bot	2698
DDoS-Hoic	3065
DDoS-Loic-UDP	2854
Infiltration	3156
Total	**66,524**

adhered to these datasets. Lack of appropriate features for IoT, use of malevolent scripts for attack detection, and susceptibility to external cyber malfunctions are some of such enmities [54]. We have adopted the CICIDS2018 dataset which is remarkably known for its spacious range of features towards IoT communications [55], [56]. This dataset implicates seven useful categories with up to 14 contemporary cyber threats (e.g brute force, heartleech attack, DDoS, infiltration attack, and port scanning attacks) [57]. More than 80 traffic scenarios are embedded in this dataset. [58]. In our proposed work, we have included all features of the CICIDS2018 dataset and its classes details along with instances are inducted in Table 3.

D. DATASET PREPROCESSING

CICIDS2018 dataset brings forth the acquiescent data in divergent forms. Using this raw data to classify an algorithm cannot retain substantive results. And hence, it needs to be sorted out before actually bringing it to perform. The first step was to remove any data that contained blank or NAN-values,as they can impact the quality of the data and the evaluation model. We used the label encoder, sklearn, to convert all non-numeric values to numeric values because DL algorithms primarily analyse numeric input. Additionally, the output label has been encoded as a one-hot encoding because the category ordering can have a negative impact while validating the performance of a proposed model.

E. DATA NORMALIZATION

When it comes to numeric columns in a dataset, normalisation refers to the act of translating their values to a similar scale without manipulating the value ranges. For machine learning, each dataset does not require normalisation. It is necessary only when features have a diverse range of values. To normalise CICIDS2018, we have used the Min-Max Scalar function. In this approach, the data is normally scaled to a fixed range that is usually between 0 and 1. A normalized dataset leads towards the effectiveness of the proposed model and yields productive outcomes.

IV. EXPERIMENTAL SETUP AND DISCUSSION

A. EXPERIMENTAL SETUP

The performance validation of our proposed framework is carried out through analytical simulations, where an Intel processor, Core i7-7700 accompanied by a Graphical Processing Unit (GPU) is used. During the experimentation process, we have considered various comprehensive libraries such as Numpy, Tensor Flow, Pandas and Keras. However, the proposed model is concurrently trained on Keras with the 3.8 version of Python.

B. EVALUATION METRICS

To validate the performance of an intrusion detection framework, the evaluation matrix should be generic and it should indulge all possible attributes of a targeted framework. Although there is no standardized scale to classify a performance matrix, however, the matrix that included Accuracy, Recall, Precision, and F-1 score is quite frequently used. We have captivated this performance matrix to examine our proposed DNNLSTM framework. The accuracy of a model is purely dependently calculated by various crucial indicators such as True Positive Rate (TPR) and True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR). The summation of True Positives (TP) and True Negative (TN) is compiled on a ratio scale with the aggregated summation of TP, TN along with False Positives (FP), and False Negatives (FN) as stated in equation 1.

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

The recall is considered as a nucleus parameter to determine the performance of an IDS. It indicates the total number of results correctly determined by an algorithm. It is the ratio of TP to the accumulative aggregation of TP and FN as engraved in Equation 2.

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

The term precision confusion overlapped with recall in some cases as it expresses the total number of relevant results declared by the system. Equation 3 numerically represents precision which is the ratio of TP to the TP and FP.

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

However, when the TP is multiplied with 2, and its ratio is implied to the two multiples of TP and summation of FP and FN yields us an F1-score. The equation can be used to calculate this score.

$$F1 - score = \frac{2 * TP}{2 * TP + FP + FN} \tag{4}$$

V. RESULTS AND DISCUSSION

This chapter comprises a detailed discussion regarding the outcomes obtained after a systematic performance evaluation of our proposed framework. For a complete performance comparison, the proposed scheme (DNNLSTM) is compared with two distinguished classifiers DNNGRU, and BLSTM along with existing Literature in Table 5.

A. DISCUSSION

We used cuDNNLSTM model for effective and efficient threat detection in IoT environment. The proposed

TABLE 4. 10 folds performance comparison of DNNLSTM, DNNGRU, and BLSTM.

Parameter	Models	1	2	3	4	5	6	7	8	9	10
Accuracy (%)	cu-DNNLSTM	99.45	98.96	98.93	99.68	99.34	99.74	99.85	99.87	99.88	99.89
	cu-DNNGRU	98.85	98.83	98.69	97.96	97.56	98.65	98.96	99.65	98.85	98.85
	cu-BLSTM	99.69	99.86	99.86	98.75	98.64	98.65	98.92	98.26	98.21	98.21
Recall (%)	cu-DNNLSTM	98.97	99.65	99.45	99.25	99.61	99.9	99.92	98.91	98.9	99.89
	cu-DNNGRU	98.69	98.84	98.65	98.45	98.96	98.76	98.25	98.86	98.99	98.99
	cu-BLSTM	98.98	98.65	98.45	98.99	98.98	98.64	98.26	98.6	98.90	98.67
F1-score (%)	cu-DNNLSTM	99.56	99.81	99.62	99.54	99.64	99.15	99.85	99.62	98.89	98.54
	cu-DNNGRU	98.98	98.98	99.65	98.56	98.65	98.52	98.85	98.99	98.89	99.65
	cu-BLSTM	98.92	98.96	98.64	98.64	98.65	98.64	98.68	99.64	98.84	98.65
Precision (%)	cu-DNNLSTM	98.79	99.51	99.54	99.36	99.71	99.25	99.54	98.88	99.65	99.45
	cu-DNNGRU	98.96	98.85	98.81	98.89	98.68	98.96	98.99	99.18	99.86	98.54
	cu-BLSTM	98.65	98.85	98.98	98.90	98.62	98.15	98.34	98.96	98.25	98.76

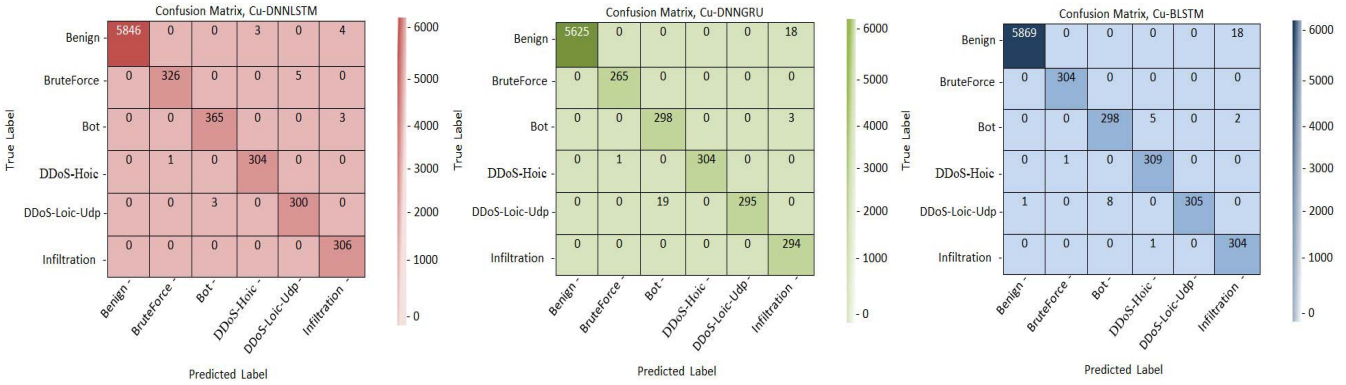

FIGURE 3. Confusion matrix of DNNLSTM, DNNGRU and BLSTM.

model (cuDNNLSYM) can detect brute-force, bot, infiltration, and DDoS attacks and is trained and evaluated under CICIDS2018 dataset having 500, and 300 neurons of DNN and LSTM comprises only 200 neurons. As IoT devices are heterogeneous and resource-constrained devices, and are designed to meet the requirement of the specific user purposes, so it is hard to come up with a common solution for all of them. The proposed work used SDN-based threat detection framework for IoT because SDN efficiently adapts with network heterogeneity. Therefore, the integration between SDN and IoT provides accurate guidelines for monitoring network traffic to detect suspicious activities. The proposed model is easy to implement and deploy in IoT environments to detect sophisticated threats. However the proposed model is vulnerable to insider threats. A complete discussion on the results are provided in the following sections.

B. CROSS-VALIDATION

Every DL based IDS comes with the conceivable potential to overcome malicious entities. However, cross-validation is an ideal phenomenon to determine the fertility of a system. Our proposed system is validated through 10 fold cross-validation under a diversified bracket of performance parameters such as Accuracy, Precision, Recall, and F-1 score. Significantly supportive results were obtained towards our proposed model as compared to existing solutions embraced for this comparison. While considering accuracy, the DNNLSTM accomplish high accuracy of 99.45% at the first fold. The number trounces the milestone achieved by other competitors DNNGRU and BLSTM, and the sequence goes with the same pattern until the 10th fold. The same manoeuvre can be observed for Recall, where the proposed scheme enacts 98.97% of certainty by beating the results achieved by other schemes. The same productive flow s examined till the final round. Furthermore, DNNLSTM conspicuously procures a prominent number of 99.56% for F1-Score at the 1st fold, and 98.54% at the 10th fold where other schemes experience less F1-score. When it comes to Precision, DNNLSTM again pageant dignitary triumph upon competitors scheme throughout the 10 fold evaluation. The complete analysis of the 10 fold cross-validation is encapsulated in Table 4.

C. CONFUSION MATRIX ANALYSIS

A confusion matrix is a performance measurement technique for the performance evaluation of DL-based IDS. Our proposed model is evaluated on this performance monitoring scale as well and is further compared with DNNGRU and BLSTM. Figure 3 exhibits the fact that the proposed DNNLSTM have shown superior performance than DNNGRU, and BLSTM.

D. ROC CURVE ANALYSIS

The Receiver Operating Characteristic (ROC) Curve possess significant importance while validating a security

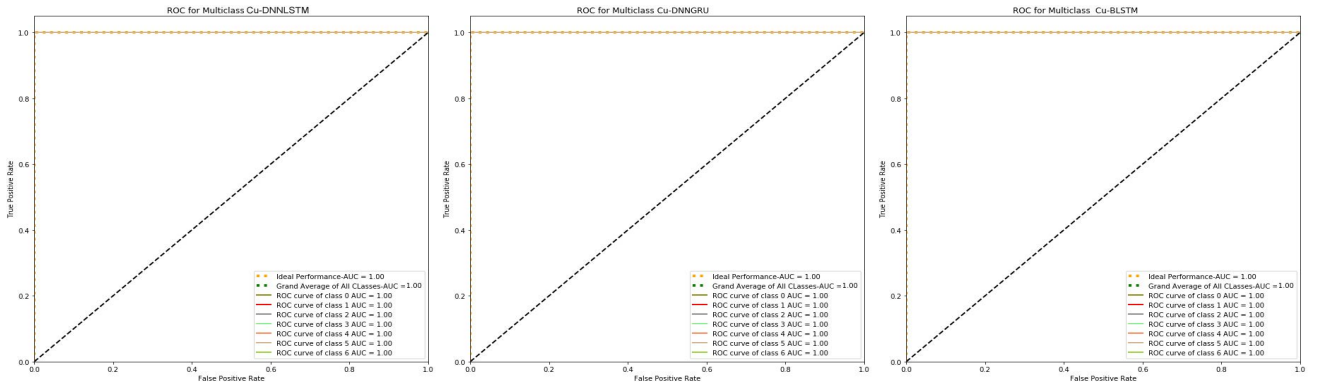

FIGURE 4. Roc-curve of DNNLSTM, DNNGRU and BLSTM.

mechanism. The True Positive Rate (TPR), also known as sensitivity or recall, is a metric used in machine learning to quantify the percentage of correctly detected positive events. Conversely, a True Negative Rate (TNR) is an outcome where the model correctly predicts the negative events. ROC curve shows a deliberated analysis of TPR and TNR, hence, the effectivity of an IDS is truly evaluated. Proposed DNNLSTM possess miraculous performance on the ROC curve as compared to DNNGRU, and BLSTM as can be witnessed in Figure 4.

E. ACCURACY, PRECISION, RECALL AND F1-SCORE

Accuracy is an essential component that spectacle the actual assessment regarding the performance of a specific classifier. The precision determines the degree of accuracy that is measured based on real-time predicted events. The term ''Recall'' can be interchangeably used with TPR, and it determines the investigated attacking scenarios. F1 score is a rational parameter to expose the strength of an intrusion detection framework. The proposed DNNLSTM is classified on all the above-mentioned performance indicators. A phenomenal performance shown by DNNLSTM in comparison with DNNGRU, and BLSTM makes it a marvellous choice to overcome cyber threats in IIoT. The proposed model achieved an accuracy of 99.55% with precision, recall, and F1-score of 99.36%, 99.44%, and 99.42% respectively. The whole performance analysis is engraved in Figure 5.

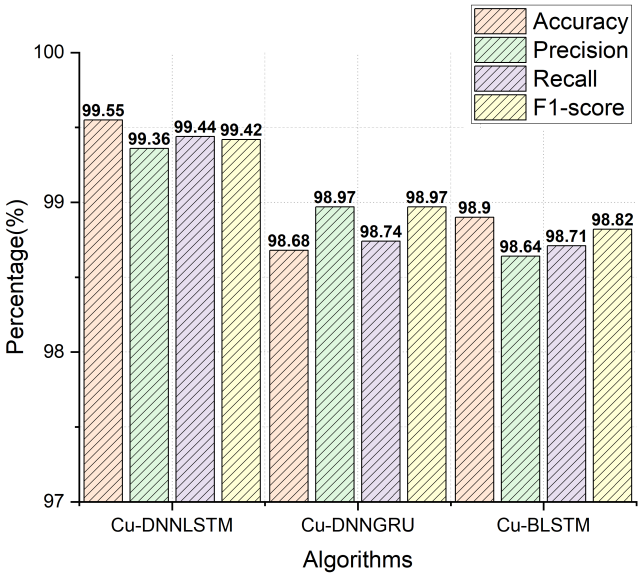

FIGURE 5. Performance evaluation of DNNLSTM, DNNGRU and BLSTM.

F. FPR, FDR, FNR AND FOR ANALYSIS

Our proposed intrusion detection mechanism is further investigated on an extensive performance measurement scale comprising FPR, FNR, False Detection Rate (FDR), and False Omission Rate (FOR). DNNLSTM shows dominant performance as compared to DNNGRU and BLSTM with 0.0032% FPR, 0.0010 FNR, 0.0011% FDR and 0.0021% FOR as exhibited in Figure 6.

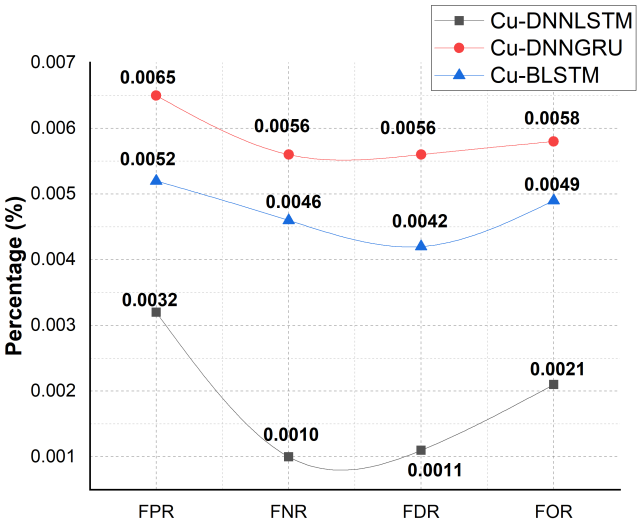

FIGURE 6. FPR, FDR, FNR and FOR analysis.

G. TPR, TNR, MCC ANALYSIS

On the hierarchal performance evaluation matrix, TPR, TNR and MCC maintain vital attention. We have compared DNNLSTM with DNNGRU, and BLSTM against these parameters where DNNLSTM seems to outperform other intrusion detection schemes with marvellous consummation. The proposed model achieved a TPR of 99.66%, TNR of

TABLE 5. Comparison with current benchmarks.

Ref	Model	Dataset	10 Fold	Accuracy	Testing Time	Recall	F1-score	Precision
Proposed	cu-DNNLSTM	CICIDS2018	Yes	99.55%	14.39 ms	99.44%	99.42%	99.36%
[59]	GRU-LSTM	NSL-KDD	No	87.90%	-	77.90%	80.60%	83.50%
[60]	GRU-RNN	CICIDS2017	No	89.00%	-	99.00%	99.00%	99.00%
[61]	Generalized Suffix Tree	NSL-KDD	No	98.70%	24 ms	98.60%	98.20%	98.90%

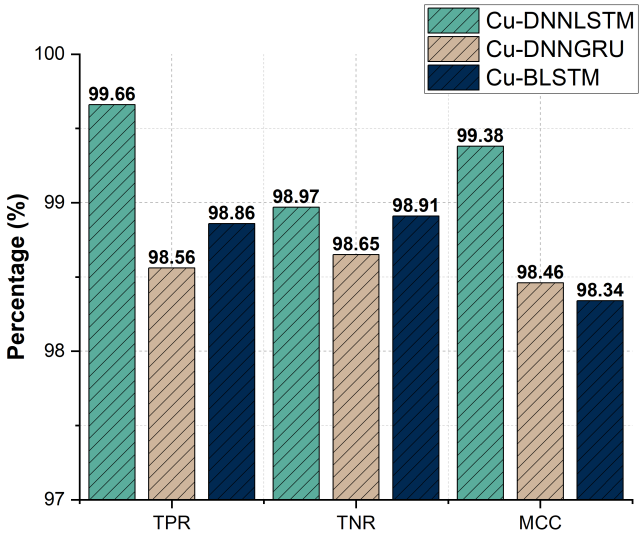

FIGURE 7. TPR, TNR and MCC analysis.

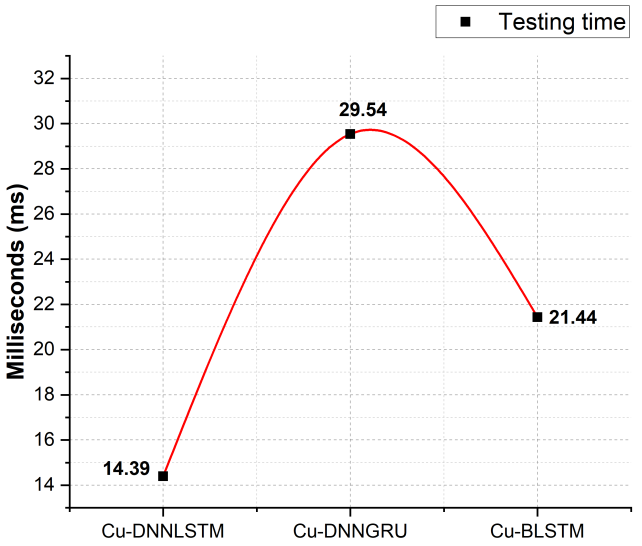

FIGURE 8. Testing time of the models.

98.97%, and MCC of 99.38% respectively. The paradox is luminary stated in Figure 7.

H. TIME EFFICIENCY

The time that a system takes to acquire the internal sustainability of its absolute features is referred to as the training time, and it is considered an indispensable scale to check the performance of a system. The proposed DNNLSTM imprison a training time of 14.39ms, which is comparatively low with DNNGRU, and BLSTM with a training time of 29.54ms and 21.44ms respectively as projected in Figure 8.

I. PERFORMANCE COMPARISON OF THE PROPOSED MODEL WITH EXISTING DL ALGORITHMS

To validate the performance of the proposed DNNLSTM, we have correlated and compared it with some phenomenal benchmark algorithms i.e DNNGRU, and BLSTM. The evaluation is drawn on Accuracy, precision, Recall, and F1-score. All of these algorithms are analysed in terms of these parameters, however, the DNNLSTM envisage prodigious performance. A 10 fold performance evaluation approach is conducted to achieve more analytical and interpretive consequences. Our proposed model reveals monumental performance on a comparison scale with other benchmark algorithms. This comparison is elaborately enlisted in Table 4. To expand the validation spectrum of DNNLSTM, a comprehensive performance comparison is further drawn between the proposed model and some state of the art existing frameworks from the literature. On all the above-mentioned performance parameters, DNNLSTM has accomplished an astounding performance by drubbing the existing literature in an impressive way. An inquisitive comparison can be overviewed in Table 5.

VI. CONCLUSION

This study is drafted about intrusion detection in IoT, where we have proposed a DL based SDN enabled intrusion detection mechanism to combat emerging cyber threats in IoT. The proposed system (DNNLSTM) provides commensurate strength to encounter an assimilated range of potential security threats including DOS, DDOS, MITM, botnet attacks, infiltration attacks, brute force attacks, port scanning attacks etc. The performance of the proposed model is evaluated on a diverse performance matrix where several indispensable parameters i.e accuracy, precision, recall, F1-score are taken into consideration. For validation perspective, the designed framework is compared with two benchmark classifiers, i.e., DNNGRU, and BLSTM. For more comprehensive and analytical scalability, the DNNLSTM is also compared with state-of-the-art intrusion detection schemes focusing on the same domain. The proposed framework has outclassed the existing literature with eloquent performance towards efficient attack detection. 99.55% accuracy, 99.36% precision, 99.44% recall, and 99.42% F1-score are the perceptible achievements of our proposed framework that

makes it an ideal choice to investigate malicious entities in IoT environments.

ACKNOWLEDGMENT

The authors express their gratitude to Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] J. Mocnej, A. Pekar, W. K. G. Seah, P. Papcun, E. Kajati, D. Cupkova, J. Koziorek, and I. Zolotova, "Quality-enabled decentralized IoT architecture with efficient resources utilization," *Robot. Comput.-Integr. Manuf.*, vol. 67, Feb. 2021, Art. no. 102001.

[2] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–188, 2021.

[3] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108040.

[4] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, Jun. 2021.

[5] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, 2020.

[6] D. Javeed, T. Gao, M. T. Khan, and D. Shoukat, "A hybrid intelligent framework to combat sophisticated threats in secure industries," *Sensors*, vol. 22, no. 4, p. 1582, Feb. 2022.

[7] A. Rahman *et al.*, "SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic," *Cluster Comput.*, 2021, doi: 10.1007/s10586-021-03367-4.

[8] Z. Lv, L. Qiao, A. K. Singh, and Q. Wang, "AI-empowered IoT security for smart cities," *ACM Trans. Internet Technol.*, vol. 21, no. 4, pp. 1–21, Jul. 2021.

[9] Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, "A topical review on machine learning, software defined networking, Internet of Things applications: Research limitations and challenges," *Electronics*, vol. 10, no. 8, p. 880, Apr. 2021.

[10] S. Prabakaran, R. Ramar, I. Hussain, B. P. Kavin, S. S. Alshamrani, A. S. AlGhamdi, and A. Alshehri, "Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network," *Sensors*, vol. 22, no. 3, p. 709, Jan. 2022.

[11] E. M. Zeleke, H. M. Melaku, and F. G. Mengistu, "Efficient intrusion detection system for SDN orchestrated Internet of Things," *J. Comput. Netw. Commun.*, vol. 2021, pp. 1–14, Nov. 2021.

[12] S. Wang, L. Nie, G. Li, Y. Wu, and Z. Ning, "A multi-task learning-based network traffic prediction approach for SDN-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, early access, Jan. 11, 2022, doi: 10.1109/TII.2022.3141743.

[13] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "BDEdge: Blockchain and deep-learning for secure edge-envisioned green CAVs," *IEEE Trans. Green Commun. Netw.*, early access, Apr. 7, 2022, doi: 10.1109/TGCN.2022.3165692.

[14] S. A. Latif, F. B. X. Wen, C. Iwendi, L.-L.-F. Wang, S. M. Mohsin, Z. Han, and S. S. Band, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, Jan. 2022.

[15] J.-H. Moon and Y.-T. Shine, "A study of distributed SDN controller based on apache kafka," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2020, pp. 44–47.

[16] M. Arif, G. Wang, V. E. Balas, O. Geman, A. Castiglione, and J. Chen, "SDN based communications privacy-preserving architecture for VANETs using fog computing," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100265.

[17] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K.-R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 625–638, Jul. 2020.

[18] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Comput. Secur.*, vol. 104, May 2021, Art. no. 102221.

[19] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on deep learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100389.

[20] I. Idrissi, M. Azizi, and O. Moussaoui, "IoT security with deep learning-based intrusion detection systems: A systematic literature review," in *Proc. 4th Int. Conf. Intell. Comput. Data Sci. (ICDS)*, Oct. 2020, pp. 1–10.

[21] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics," *J. Ind. Integr. Manage.*, vol. 5, no. 1, pp. 165–180, Mar. 2020.

[22] V. Balasubramanian, M. Aloqaily, and M. Reisslein, "An SDN architecture for time sensitive industrial IoT," *Comput. Netw.*, vol. 186, Feb. 2021, Art. no. 107739.

[23] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido, and A. Cardenas, "A survey of the main security issues and solutions for the SDN architecture," *IEEE Access*, vol. 9, pp. 122016–122038, 2021.

[24] S. K. Keshari, V. Kansal, and S. Kumar, "A systematic review of quality of services (QoS) in software defined networking (SDN)," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 2593–2614, Feb. 2021.

[25] 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.

[26] Y. Maleh *et al.*, "A comprehensive survey on SDN security: Threats, mitigations, and future directions," *J. Reliable Intell. Environ.*, 2022, doi: 10.1007/s40860-022-00171-8.

[27] A. S. Alqahtani, "FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks," *J. Supercomput.*, vol. 78, pp. 9438–9455, 2022.

[28] S. Tharewal, M. W. Ashfaque, S. S. Banu, P. Uma, S. M. Hassen, and M. Shabaz, "Intrusion detection system for industrial Internet of Things based on deep reinforcement learning," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–8, Mar. 2022.

[29] 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, p. 432, Jan. 2022.

[30] K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, "IMIDS: An intelligent intrusion detection system against cyber threats in IoT," *Electronics*, vol. 11, no. 4, p. 524, Feb. 2022.

[31] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.

[32] M. Zhong, Y. Zhou, and G. Chen, "Sequential model based intrusion detection system for IoT servers using deep learning methods," *Sensors*, vol. 21, no. 4, p. 1113, Feb. 2021.

[33] 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.

[34] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in industrial Internet of Things network-based on deep learning model with rule-based feature selection," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–17, Sep. 2021.

[35] R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in IoT networks based on deep learning," *Sensors*, vol. 21, no. 9, p. 2987, Apr. 2021.

[36] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial attacks against network intrusion detection in IoT systems," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10327–10335, Jul. 2021.

[37] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, Mar. 2020, Art. no. 107450.

[38] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam, M. Zamani, S. Kavianpour, and N. B. Idris, "Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems," *Electronics*, vol. 9, no. 7, p. 1120, Jul. 2020.

[39] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," *Future Internet*, vol. 12, no. 3, p. 44, Mar. 2020.

[40] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of Things," *J. Cloud Comput.*, vol. 9, no. 1, pp. 1–16, Dec. 2020.

[41] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting Internet of Things attacks," *Electronics*, vol. 8, no. 11, p. 1210, Oct. 2019.

[42] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning–based intrusion detection framework for securing IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3803, 2019.

[43] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019.
[44] A. Ashraf *et al.*, "Scalable offloading using machine learning methods for distributed multi-controller architecture of SDN networks," *J. Supercomput.*, vol. 78, pp. 10191–10210, 2022.
[45] A. Galal, X. Hesselbach, W. Tavernier, and D. Colle, "SDN-based gateway architecture for electromagnetic nano-networks," *Comput. Commun.*, vol. 184, pp. 160–173, Feb. 2022.
[46] 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, no. 8, p. 918, Apr. 2021.
[47] B. Rudra and S. Thanmayee, "Architecture and deployment models-SDN protocols, APIs, and layers, applications and implementations," in *Software Defined Internet of Everything* (Internet of Things), S. G. Aujla, S. Garg, K. Kaur, and B. Sikdar, Eds. Cham, Switzerland: Springer, 2022.
[48] Z. Zeng, X. Zhang, and Z. Xia, "Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–10, Feb. 2022.
[49] L. J. Muhammad, I. Badi, A. A. Haruna, I. A. Mohammed, and O. S. Dada, "Deep learning models for classification of brain tumor with magnetic resonance imaging images dataset," in *Computational Intelligence in Oncology* (Studies in Computational Intelligence), vol. 1016, K. Raza, Ed. Singapore: Springer, 2022, doi: 10.1007/978-981-16-9221-5_9.
[50] P. G. V. S. Kumar and S. Akthar, "Execution improvement of intrusion detection system through dimensionality reduction for UNSW-NB15 information," in *Mobile Computing and Sustainable Informatics* (Lecture Notes on Data Engineering and Communications Technologies), vol. 68, S. Shakya, R. Bestak, R. Palanisamy, and K. A. Kamel, Eds. Singapore: Springer, 2022, doi: 10.1007/978-981-16-1866-6_28.
[51] I. F. Kilincer, F. Ertam, and A. Sengur, "A comprehensive intrusion detection framework using boosting algorithms," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107869.
[52] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107810.
[53] S. Rawat, A. Srinivasan, V. Ravi, and U. Ghosh, "Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network," *Internet Technol. Lett.*, vol. 5, no. 1, p. e232, Jan. 2022.
[54] Y.-D. Lin, Z.-Q. Liu, R.-H. Hwang, V.-L. Nguyen, P.-C. Lin, and Y.-C. Lai, "Machine learning with variational AutoEncoder for imbalanced datasets in intrusion detection," *IEEE Access*, vol. 10, pp. 15247–15260, 2022.
[55] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 16, 2021, doi: 10.1109/TITS.2021.3122368.
[56] 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*, vol. 21, no. 14, p. 4884, Jul. 2021.
[57] B. Lahasan and H. Samma, "Optimized deep autoencoder model for Internet of Things intruder detection," *IEEE Access*, vol. 10, pp. 8434–8448, 2022.
[58] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, and H. Han, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Comput. Secur.*, vol. 116, May 2022, Art. no. 102675.
[59] S. K. Dey and M. M. Rahman, "Flow based anomaly detection in software defined networking: A deep learning approach with feature selection method," in *Proc. 4th Int. Conf. Electr. Eng. Inf. Commun. Technol. (iCEEiCT)*, Dhaka, Bangladesh, Sep. 2018, pp. 630–635.
[60] T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, "Intrusion detection in SDN-based networks: Deep recurrent neural network approach," in *Deep Learning Applications for Cyber Security* (Advanced Sciences and Technologies for Security Applications), M. Alazab and M. Tang, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-13057-2_8.
[61] Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the Internet of Things," *J. Netw. Syst. Manage.*, vol. 29, no. 3, pp. 1–26, Jul. 2021.
[62] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and T. Reddy, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021.
[63] S. Agrawal, A. Chowdhuri, S. Sarkar, R. Selvanambi, and T. R. Gadekallu, "Temporal weighted averaging for asynchronous federated intrusion detection systems," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–10, Dec. 2021.
[64] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020.

MOHAMMAD AL RAZIB graduated in computer science and technology from the Changchun University of Science and Technology, China, in 2020. He is currently working as a Cyber Security Analyst. He has several research projects in deep learning and IoT. His research interests include deep learning, cyber security, network security, the Internet of Things, and artificial intelligence.

DANISH JAVEED received the M.E. degree in computer applied technology from the Changchun University of Science and Technology, China, in 2020. He is currently pursuing the Ph.D. degree in software engineering, specializing in information security with the Software College, Northeastern University, China. He has several research publications to his credit as a primary author and coauthor. His research interests include information security, network security, the Internet of Things, deep learning, software-defined networking, intrusion detection, and prevention systems.

MUHAMMAD TAIMOOR KHAN received the B.S. degree in computer science from Abdul Wali Khan University Mardan, Pakistan, and the M.S. degree in information security from the Riphah Institute of Science and Engineering, Pakistan, in 2021. His research interests include cyber security, deep learning, intrusion detection, and prevention systems.

REEM ALKANHEL (Member, IEEE) 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 the Queensland University of Technology, Brisbane, QLG, Australia, in 2007, and the Ph.D. degree in information technology (networks and communication systems) from the University of Plymouth, Plymouth, U.K., in 2019. Since 1997, she has been with Princess Nourah bint Abdulrahman University, Riyadh, where she is currently a Teacher Assistant at the College of Computer and Information Sciences. Her current research interests include communication systems, networking, the Internet of Things, information security, information technology, quality of service and experience, software-defined networks, and deep reinforcement learning.

MOHAMMED SALEH ALI MUTHANNA received the M.S. degree from the Department of Computer Science, Saint Petersburg Electrotechnical University "LETI," Russia, in 2016, and the Ph.D. degree from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2021. He is currently a Postdoctoral Fellow with the Institute of Computer Technologies and Information Security, Southern Federal University Russia. His main research interests include mobile edge computing, software-defined networks (SDN), the IoT, industrial wireless, and sensor networks.