

Received 30 December 2022, accepted 11 January 2023, date of publication 20 January 2023, date of current version 31 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3238664

## RESEARCH ARTICLE

# Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures

IRFAN ALI KANDHRO<sup>1</sup>, SULTAN M. ALANAZI<sup>ID2</sup>, FAYYAZ ALI<sup>3</sup>, ASADULLAH KEHAR<sup>4</sup>, KANWAL FATIMA<sup>1</sup>, MUEEN UDDIN<sup>ID5</sup>, AND SHANKAR KARUPPAYAH<sup>ID6</sup>, (Member, IEEE)

<sup>1</sup>Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Pakistan

<sup>2</sup>Department of Computer Science, Northern Border University, Arar 91431, Saudi Arabia

<sup>3</sup>Department of Software Engineering, Sir Syed University of Engineering and Technology, Karachi Sindh 75300, Pakistan

<sup>4</sup>Institute of Computer Science, Shah Abdul Latif University, Khairpur, Karachi Sindh 66111, Pakistan

<sup>5</sup>College of Computing and Information Technology, University of Doha For Science and Technology, Doha, Qatar

<sup>6</sup>National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia, Gelugor, Penang 11800, Malaysia

Corresponding author: Shankar Karuppayah (kshankar@usm.my)

This work was supported in part by Universiti Sains Malaysia (USM) through Short Term Grant Research under Grant 04/PNAV/6315576.

**ABSTRACT** Computer viruses, malicious, and other hostile attacks can affect a computer network. Intrusion detection is a key component of network security as an active defence technology. Traditional intrusion detection systems struggle with issues like poor accuracy, ineffective detection, a high percentage of false positives, and an inability to handle new types of intrusions. To address these issues, we propose a deep learning-based novel method to detect cybersecurity vulnerabilities and breaches in cyber-physical systems. The proposed framework contrasts the unsupervised and deep learning-based discriminative approaches. This paper presents a generative adversarial network to detect cyber threats in IoT-driven IICs networks. The results demonstrate a performance increase of approximately 95% to 97% in terms of accuracy, reliability, and efficiency in detecting all types of attacks with a dropout value of 0.2 and an epoch value of 25. The output of well-known state-of-the-art DL classifiers achieved the highest true rate (TNR) and highest detection rate (HDR) when detecting the following attacks: (BruteForceXXS, BruteForceWEB, DoS\_Hulk\_Attack, and DOS\_LOIC\_HTTP\_Attack) on the NSL-KDD, KDDCup99, and UNSW-NB15 datasets. It also maintained the confidentiality and integrity of users' and systems' sensitive information during the training and testing phases.

**INDEX TERMS** Cybersecurity, Internet of Things, intrusion detection system (IDS), anomaly detection, security attacks, deep learning.

## I. INTRODUCTION

Deep learning (DL) methods are used with different operators, which become beneficial for distinct mechanisms, especially the artificial neural network (ANN). It comprises three layers: input, output, and hidden [2], [3]. However, in DL, each layer is in a nonlinear fashion, which sent responses based on the data provided through input layers. Recently, DL approaches have been frequently used to discover graphic recognition, image processing, signal processing, and voice and audio recognition. Substantially, DL learning approaches

The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino<sup>ID</sup>.

are widely used in medicine for genomics and diseases [4]. The structure and functionality of the DL methods use complex data organization (such as images, text, and numbers hierarchy) and illustrate how to manage big data with forward, and back backpropagation methods focused. In addition, the other question raises how devices change the values and hyperparameters with dimensions to compute the Size of samples rendering the different layers. Successful methods make a minor difference between testing and training presentation and representation. The outdated wisdom characteristics result from a minor deviation from the family's usual quality and structural approaches to training [5]. Due to the reasons assumed and adopted DL methods in many areas,

privacy and security concerns are critical. In DL methods, the key issue is data movement, where data is transferred between encrypted forms in training, testing, and interface modules. In addition, the DL prevailing in all models for the training part relies on enormous data, confidential and sensitive data for the user, primarily training data [6].

Intrusion detection systems (IDS) are part of a system's subsequent protection line. [7]. IDS is an observing system that detects suspicious activities and produces alerts when they are detected and implemented in conjunction with security concerns and procedures such as authentication, security system and encryption approaches to strengthen security against cyber-attacks. Employing a variety of benign traffic/normal flow patterns and precise attack-specific rules, IDS can distinguish between harmful and non-malicious activity [8]. Data mining is used to describe and deploy IDSs with robust behaviour with higher accuracy than traditional IDS that may impact modern, sophisticated cyber-attacks. [9]. Businesses are growing increasingly worried about securing critical infrastructure (CI), especially Internet Industrial Control Systems (IICs), as the number of devices used in IIoT-based setups is continuously rising [4]. Industrial Control Systems (ICS) are a collection of hardware, software, operators, and links that are used to manage essential control functions and accomplish complex tasks. In the literature, several intrusion detection systems (IDS) have been developed to identify online attacks on IICs networks. However, there are some significant flaws in the methodologies and evaluation metrics of the majority of the current IDSs. To address the issues of poor detection rate and high false positive rates (FPR), this work provides an effective IDS for IIoT-powered IICs utilising deep-autoencoder-based LSTM model/method.

The DL methods must not reveal essential or secret information. An intrusion detection device is frequently a software application utility or a physical device that watches for intrusions by arriving and departing community visitors for signs of malicious activity or violations of security standards. Intrusion detection systems and IDS products are sometimes compared to intruder alarms, alerting administrators of any activity that might damage data or network infrastructures. IDS tools search for unusual behaviour or indicators of a capability compromise by examining the packets that move through your community and the network visitor styles to detect any irregularities. Intrusion detection structures are primarily passive, albeit a few intrusion detection structures can intervene when they identify harmful conduct. Overall, they're mainly intended to acquire real-time visibility during times of capacity community compromises. Numerous IDS products will respond differently depending on the type of intrusion detection equipment that has been deployed. For instance, a network intrusion detection system, also known as NIDS [10], will strategically put sensors throughout the network. These sensors will then detect community visits without causing performance issues or blockages. Host-based

complete intrusion detection systems (HIDS) operate on specific gadgets and servers that are only helpful in tracking visits to those specific gadgets and hosts [7].

However, each generation selects a set of different deep learning pre-trained methods such as RNN, CNN, and DL MLP. The framework used discriminative architecture, which includes convolutional neural networks (CNN), recurrent neural networks (RNN), and deep neural networks (DNN), a set of items that are included in IDS independently. As a result, one individual item indicates a possible combination of many systems that will be used to build more profound and more relevant aspects. Deep learning algorithms are trained to evaluate the model's effectiveness by simply concatenating the in-depth features. The deep feature representations are then destroyed, and the final classification results are made with a network that was made by itself and had several dense, hidden layers.

The proposed framework assessed three separate datasets (NSL-KDD, KDDCup99, and UNSW-NB15). The experimental outcomes show that the proposed framework is superior to several strong strategies, which makes it easier to deploy it in actual IICs networks. And also, compared the outcomes of the suggested state-of-the-art methods/models. The following are the key objectives and contributions of this paper:

1. Developed a novel comprehensive framework to detect cyber and malicious attacks which can collaboratively train the system on multiple data with deeper traffic analysis.
2. A proposed AI-enabled deep intrusion detection framework that employs multi-layer perceptrons (MLP), recurrent neural networks (RNN), and deep neural networks (DNN) methods to detect cyberattacks and malicious intent to capture latent data that can support effective IDS design.
3. Tests the performance of the proposed efficient IDS framework on IIoT IICs and exterior networks on the NSL-KDD, KDDCup99, and UNSW-NB15 datasets.

The rest of this paper is structured as follows: Section II examines and analyses various related works and identifies research gaps. Section III highlights the proposed methodology. Section IV elaborates results and discussion. Section V concludes the paper with future scope.

## II. RELATED WORK

The deep learning methods brought a big revolution in computer science with additional powerful subfields and various fields, including Natural Language Processing (NLP), machine learning, computer vision, and speech/audio processing. In visual data analytics, Convolutional Neural Networks (CNNs) have exhibited substantial gains in picture categorization, object identification, and video motion monitoring. A CNN contains a sequence of linear and nonlinear layers called a hierarchical structure, with a direct connection and shared weights. It was first proposed for simple picture

recognition. LeNet-5 CNNs have two convolutional layers, each followed by a sub-sampling layer and, eventually, a convolution for class prediction. It was later widely employed in various scientific and real-world applications as hardware technology (e.g., GPUs) progressed [2], [11], [12], [13], [14], [15], [16], [17].

A study of intrusion detection datasets was recently published [16]. The research includes 34 datasets and 15 features for each of them. The traits of these are divided into five categories: (1) well-known data, (2) assessment, (3) recording environment, (4) recording volume, (5) recording type, and well-known, relevant data [8], [17], [18], [19], [20] researched intrusion detection systems' machine learning methodologies. The datasets were divided into three categories: The first category is packet-level data, then the second one is network packet data, and the last category is accessible datasets. The computational cost was also analyzed in the study (running time) of each malware detection approach that employs extraction and machine learning technology. On the interconnected internet of things (IoT), [20], [21], [22], [23], [24], [25], [26] conducted a comparative analysis of intrusion detection techniques on the IoT. The study used the detection approach, IDS placement strategy, and security threat to classify IDSs for IoT [18]. The study analyzed current systems for each primary assessment factor, including workloads, metrics, and approaches, to give common practices in cyber security intrusion detection. Deep learning algorithms for cyber security intrusion detection are the topic of our research and four other papers [23, 28-31]. On the other hand, these publications do not provide a comparison of deep learning algorithms on the datasets. Our research is the first to investigate an in-depth examination of deep learning for IDS, including methodologies, datasets, and comparative analysis, according to our awareness [30], [31], [32], [33].

Table 1 represented the comparison of related work in 2021 and 2022 of machine learning and deep learning for detecting intrusion and cyber security attacks. This survey has discussed the minimal work of deep learning and machine learning. The studies focused on the issues, challenges, and shortcomings of ML and DL techniques for detecting ICS anomalies and the current ICS-to-cloud infrastructure. ML methods secure ICT on the network and physical levels by managing the information through packets and controlling anomalies [66]. The research on ML-AIDS identifies and efficiently implements the effective and efficient anomalies of networks and computers [70]. Recently, many researchers have been dedicated to developing ML with NIDs [41], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70]. The IDS faced challenges in accuracy by reducing false alarm rates. For that reason, the DL with an IDS system was deployed as a potential solution to identify intrusion attacks [69]. Beyond that, binary and multiclass experiments were performed on the CSECIC-IDS2018 and the Bot-IoT datasets [70], [71], [72], [73], [74].

**TABLE 1.** Comparison table from 2021 to 2022.

Reference	Year of Publication	Similarities/Differences
[67]	2022	<ul style="list-style-type: none"> <li>The author of this paper presented a solution on swarm intelligence for cyber-attacks inspired by an intrusion detection system (IDS).</li> </ul>
[68]	2022	<ul style="list-style-type: none"> <li>The author of this paper proposed an efficient methods and discussion on a driven approach based intelligent intrusion system (IDS) with control Anomalies</li> </ul>
[69]	2022	<ul style="list-style-type: none"> <li>This paper focuses on Deep learning methods for evaluation, metrics, strategies for IoT and different types of attacks.</li> </ul>
[70]	2021	<ul style="list-style-type: none"> <li>The paper presented on data-driven approaches to NID minority attacks</li> </ul>
[71]	2021	<ul style="list-style-type: none"> <li>The author of this paper demonstrated a comprehensive analysis (tabular strctrurized) on machine learning approaches for intrusion detection, no used DL methods.</li> </ul>
[72]	2021	<ul style="list-style-type: none"> <li>In this paper, the main focus of the author is on ICS and Cloud-based deep belief network intrusion detection and related operations.</li> </ul>
[73]	2021	<ul style="list-style-type: none"> <li>This paper presented the role of IoT, and their application in the cloud environment and proposed a third-party collaborative approach for prevention from the attacks.</li> </ul>
[74]	2021	<ul style="list-style-type: none"> <li>It focuses on performances and future detections involvinf in the domain of Intrusion detection</li> </ul>
[66]	2021	<ul style="list-style-type: none"> <li>The use of ML for categorizing list of attacks and prevention</li> </ul>

**TABLE 1.** (Continued.) Comparison table from 2021 to 2022.

[65]	2022	<ul style="list-style-type: none"> <li>The author of this paper focused of this paper to analysis the advanced persistent threats in industrial internet of things (I-IoT).</li> </ul>
[67]	2022	<ul style="list-style-type: none"> <li>This work involves IoT Multi-Vector Cyberattack Detection and compromised with IoT network.</li> </ul>
[68]	2021	<ul style="list-style-type: none"> <li>The paper presented the role IoT security challenges and state-of-the-art malware detection methods with a focus on AIS.</li> </ul>

### III. RESEARCH METHODOLOGY

The proposed framework depicts the complete process of a working operations that includes IDS and the revolutionary process, as illustrated in Fig 1. Precisely, the designed framework consists of five levels, which shows the novelty such as 1) the initial stage of datasets under study; 2) Data preprocessing; 3) learning component; and finally, 4) results of diverse cyberattacks and malicious detection.

#### 1. Dataset used:

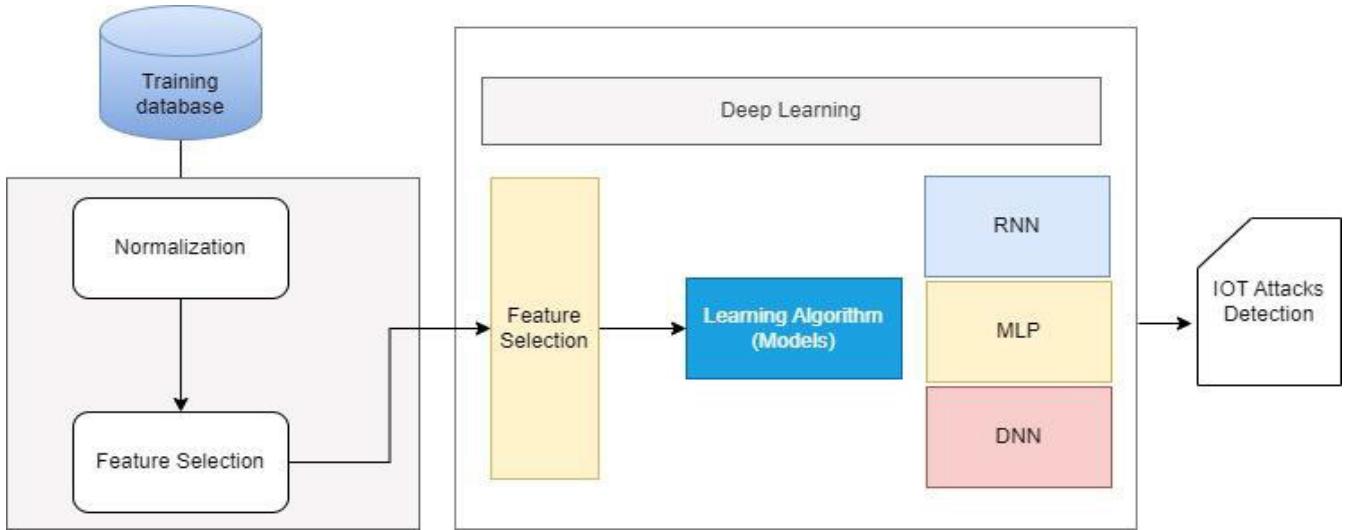
KDDCup99, NSL-KDD and UNSW-NB15 are the most popular and widely used datasets in academic research to evaluate the different malicious activities and detect diverse attacks. The NSL-KDD dataset is the extension of KDD99, it reduces the shortcomings of the old version dataset, precisely, it not only focuses to reduce the redundant data from training and testing but also sets the number of records in training and testing sets. The dataset has 42 features and is divided into 3 categories, traffic features, content features and content features. The KDDCup 99 dataset is one of the popular datasets in IoT with cybersecurity [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47]. This dataset provides labelled and unlabeled training and testing data, and it originated from the evaluation program DARPA98 IDS with corresponds to seven and two weeks [33], [41], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74]. The UNSW-NB15 dataset was created by perfectStorm (IXIA) in collaboration with the UNSW Cyber Range Lab to generate moderately aggressive activities and attacks. In dataset, each record in the collection has 47 features, divided into 10 types, including Backdoors, DoS, Analysis, Exploits, Generic, Reconnaissance, Fuzzers for Abnormal Activity, Shellcode, and Worms.

**TABLE 2.** Related work with evaluation metrics.

NETWORK	REF	DATABASE	Evaluation Metrics
DL(RNN)	[34]	NSLKDD Database	ACC, Detection rate, FAR Detection
	[35]	CICIDS2017 dataset	ACC, Detection Rate and FAR
DL(CNN)	[36]	IEEE-118 and 30 (Bus)	Feature score, accuracy
	[37]	Credit card details (Transaction)	Accuracy, Detection Rate, F1-Score
	[38]	Information of online transaction	ACC, Recall and Precision
	[39]	KDDCup1999 database	ACC, Recall and Precision
	[40]	NSLKDD database	A.C.C.
DL(RBM)	[41]	KDDCup1999 database	FAR Detect, ACC, and Detection Rate.
	[42]	NSLKDD database	Precision, F1-Score
	[43]	Real online network traffic	ACC, Detection rate, FAR Detection
	[33]	KDDCup1999 database	Accuracy, detection rate, FNR ROC F1-score Curve,
	[44]	NSLKDD database	Precision, Recall, F1-Score.
DL(DNN)	[45]	NSLKDD database	A.C.C.
	[46]	Vehicular network communication	ROC, Detection rate and FAR
	[47]	KDD Cup 1999 database	CC, Precision, Recall and F1-score
	[39]	DOS, R21, U2R AND PROBIN	ACC, TPR, FPR.
	[48]	KDDCup1999 database	ACC, Recall and Precision, F1-score
	[49]	KDDCup1999 database	ACC, Detection rate, False Alarms
	[33]	The database vehicles attacks	Detection rate, False and True positive and time per msg

#### 2. Data Preprocessing:

Data preprocessing is collecting and manipulating electronic data and transforming data values of a certain dataset. It is the modification of information detected by the observer, aiming to optimize the information acquisition. Generally, there is a very large difference between the minimum and maximum values in the dataset. The normalization process reduces the complexity of the algorithm and data allows an adequate benefit for the classification of algorithms related to neural networks. The basic method of normalization is data scaling, it consists of minimum and maximum algorithms. The data converting into current range typically  $(-1, 1)$  and  $(0, 1)$  interval. In addition to this, the standardization function is also used for normalizing data in advance, whereas the z-score function is used to normalize the features of the dataset with the standard distribution, as shown in Figure 1.



**FIGURE 1.** Proposed framework for intrusion detection in the IoT environment.

#### A. DEEP DISCRIMINATE MODELS (DDM)

In the designed framework, a deep neural network (DNN) working with multiple input and output layers. The DNN is used as a multilayer perceptron due to its properties. In a network, the multilayer features are brought advantage to represent the complex and unique methods with given parameters. The DNN network supports feature extraction and representation learning. Fundamentally, the DNN method chains three categories of layers: The first layer is made up of input layers, a concealed layer, and a convolution layer. The proposed DNN model provides a solution to network security problems for flow-based anomaly detection and analysis [50]. The simple DNN method is initially applied for network security results, with a single input layer, three hidden levels, and a final layer at the end. A few experiments are compiled on the NLS-KDD database, where the proposed model shows outstanding results for identifying zero-day attacks and outperforms the competition and conventional techniques.

Moreover, to enhance the performance of the DNN model, they developed a novel network structure named Hash-Tran D.N.N. to categorize the OS Android malware [51]. Fig 2 depicts the simple structure to observe the most innovative points in converting input samples to satisfy locality characteristics using hash functions. The Hash-Tran DNN AE is used to accomplish quantization tasks. The Hash-Tran D.N.N. classifier achieved good results in the potential space by obtaining locality information. DNN is a multilayer perceptron (MLP) with more than three layers. Fig 2 presents the structure of MLP, It employs a kind of feed-forward ANN network by n layers that make up and surpass one another.

DM (aM, M, nM) denotes layer M [1, N] and the DNN network. The number of inputs is given by aM N. middle and outer layers containing neurons where RaM denotes the linear

transformation. Described by the matrix WM and the vector bM. nM: RaM RaM is layer M's transference purpose and the vector bM. M: RaM1 RaM is the affine transformation defined by the matrix WM. The VM matrix is also known as the weight matrix since it computes the weight between M-1 and M layers. The bias vector of layer M is the vector bM. as defined in Algorithm 1 below:

---

#### Algorithm 1 Pseudocode for Attack Detection Using Deep Learning Method Based on MLP

---

*The input Training R(t), S(t)*

*h(t)=r(t)  $\forall t \in [1, tf]$ ;*

*Normalize (Di) values between (0,1)*

*The window size (tw, Di)*

*loop k = 1 to Size of samples do*

*gM = nM(hM-1) = WM  $\times$  hM-1 plus(+) bM;*

*hM =  $\alpha M(gM)$*

*Run Predictions using L*

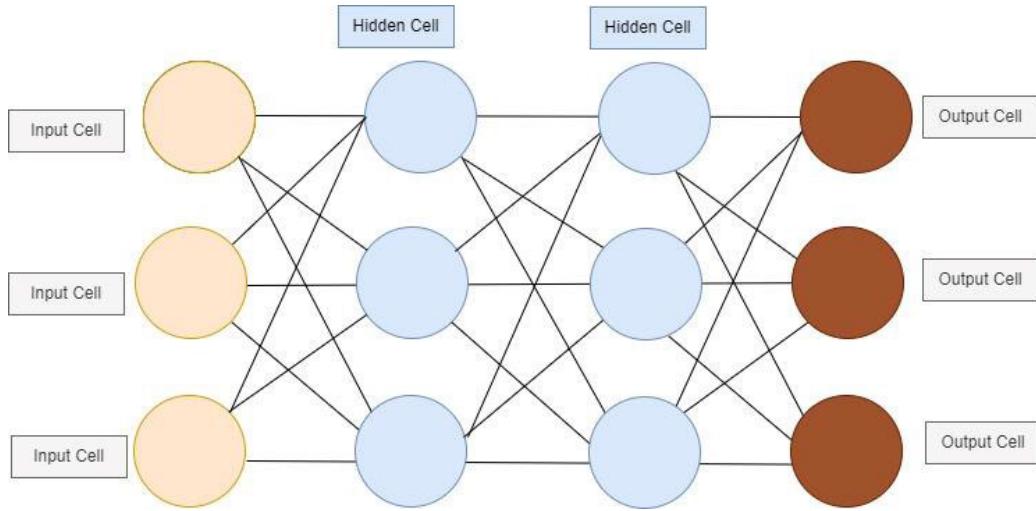
*End Inner Loop*

*End Outer Loop*

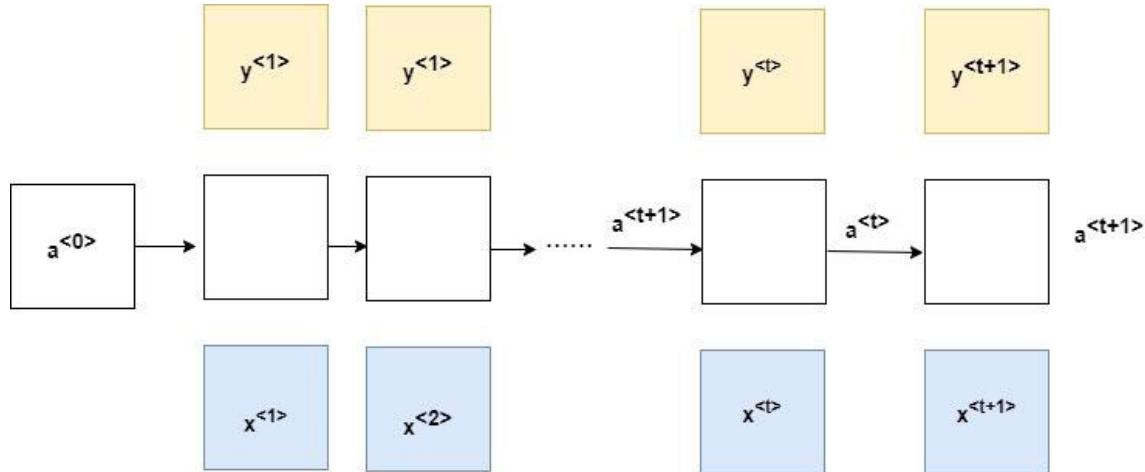
---

#### B. RECURRENT NEURAL NETWORK (RNN)

RNNs (recurrent neural networks) are a set of neural networks that allow prior outputs to be used as inputs while having hidden states, as shown in Figure 2. So, the output of CNN and DNN simply represents the current inputs' effect without considering past and future information. RNNs may achieve notable performance in recognition and classification without temporally erratic characteristics. With the help of time-dependent data, the RNN focuses on a special package for a neural network for memory function to manage the previous content. However, there are several challenges in the construction and design of RNN with intensity explosion



**FIGURE 2.** The architecture of a traditional MLP.



**FIGURE 3.** Working of traditional RNN.

and extinction. The RNN does quite well with time-series information, such as design features that coincide with the notion that human cognition is founded on memories and experience [52], [53], as shown in Figure 3. Due to the time series, RNNs cause forgetfulness or long-term reliance. Thus, the researchers created the LSTM and GRU with design gates and memory cells, which have a long-term association. and the flow of information from gate to gate. At each timestep  $t_1$ , the activation  $a(t)$  and the output  $y(t)$  is expressed as follows in equation 1 and 2:

$$a(t) = g1(Waaa^{t-1}) + g1(Waax^{t-1}) + b_a \quad (1)$$

$$y(t) = g2(Wya^{t-1}) + b_y \quad (2)$$

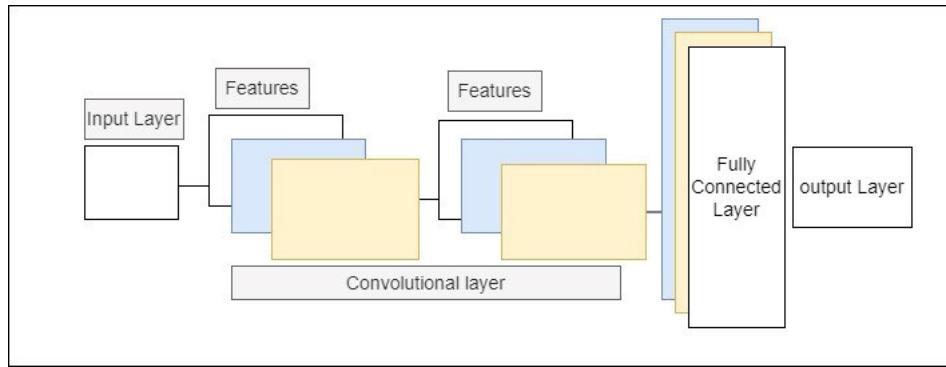
where  $W_{ax}$ ,  $W_{aa}$ ,  $W_{ya}$ ,  $b_a$ , and  $b_y$  are coefficients that are shared temporally and  $g1$  and  $g2$  are activation functions.

The RNN is described by introducing an interconnection matrix  $V.W.M$ . RaMaM to layer M [1, N] to produce a layer

M of the recurrent community conversation to decide in fig. 3 and grade by grade are defined in pseudocode as a set of rules in algorithm 2.

### C. CONVOLUTIONAL NEURAL NETWORKS (CNNs)

The CNN is also termed as ConvNet. The CNN contains a deep and hierarchical structure, and it encompasses high computation for processing complex data, which is normally represented in the deep learning domain in the form of cascading linear and nonlinear fashion. The CNN used independent features and less preprocessing to contain prior knowledge. [54] The ConvNet layers are the basic building blocks of a convolutional neural network, and these layers take the computation burden and carry the data from one layer to another, as shown Figure 4. CNN uses a modified design of multilayer perceptron for minimal processing with local connectivity and weight sharing. For self-learning, the CNN layers take the dot product of data in matrix form [55]. The



**FIGURE 4.** The architecture of a traditional CNN.

---

**Algorithm 2** RNN Pseudocode for Number of Attacks Detection

---

*The input Training  $R(t)$ ,  $S(t)$*   
 $h(t)=r(t) \forall t \in [1, tf]$ ;  
*Normalize the dataset ( $D_i$ ) between (0,1)*  
*Select training ( $T_w$  and  $D_i$ )*  
*Outer loop  $k=1$  to Size of samples do*  
  *Inner loop  $t=1$  to  $tf$  do*  
     $Gm(t) = WM * HM-1(t)$   
    *(Therefore: WM = Weight Matrix and HM = Hidden Matrix)*  
    *plus VWMX HM (t1-1)+ Bm.*  
     $hM(t)=\alpha M(gM(t))$ ;  
    *Run Predictions using L*  
  *End Inner Loop*  
*End Outer Loop*

---

learning is based on learnable parameters and various kernels. Structure-wise, the CNN network has three layers: 1) input, 2) hidden, and 3) output. The hidden layer uses different filters such as kernel, max, and min pooling, and a complete connection layer, as shown in fig 4, in network data passes through each step either backward or forwards. The kernel slides with a certain height and width in each network layer and representation are shown in the receptive region. In one more step, CNN produces a 2-dimensional vector of image known as the activation layer, which response to the kernel at each position. Each sliding layer is also called a striding. The equations 3 show the Wout computation:

$$W_{out} = \frac{W - F + 2P}{S} + 1 \quad (3)$$

The output extent of length is  $W_{out} \times W_{out} \times D_{out}$ . If we have an entry of length  $W \times W \times D$  and  $D_{out}$  wide variety of kernels with a spatial length of  $F$  with aspect  $S$  and a quantity of padding  $p$ , then the dimensions of the output extent may be determined.

#### IV. EXPERIMENTS AND RESULTS

With the rapid growth of applications and network uses, security has become a significant concern for network systems. Numerous IoT devices rely on the self-created system, which is susceptible to diverse attacks. The network layer issues denial of service (DoS) assaults, gateway attacks, sniffers and illegal access. IDS are improved along with the emergence of large-scale, high-dimension IoT and computer networks. However, in this section, we evaluated the results of the proposed framework. To elaborate on the effectiveness of a Deep learning-based approach for enterprise network environment solutions for edge IoT device security.

Table 3 shows the results of Deep Learning discriminative methods for various attacks and the type and nature of attacks and benign. It is shown that deep neural networks give outstanding results on the performance metrics of true negative rate (TNR) (attack) with an accuracy of 96.915%. The recurrent neural networks and their variants archive good results on seven different models and attacks. Specifically, Brute\_ForceWEB (95.22%), BruteForceXXS (95.62%), DoS\_Hulk\_Attack (96.88%), DOS\_GoldEyes\_Attack (97.55%), DoS\_SlowHTTPTest\_Attack (92.10%), Infiltration (96.15%).and DoS\_SlowLoris\_Attack (97.90%). The convolutional neural network (CNN) provides superior performance when compared to other techniques and kinds of attacks. The CNN gives high detection on four attacks, such as Botnet (97.90%), DOS\_LOIC\_UDP\_Attack (95.00%), DOS\_LOIC\_HTTP\_Attack (97.74%), and DOS\_HOIC\_Attack (95.11%). The performance of unsupervised and generated models is comparable to the various types of attacks and benign ones. The deep belief network (DBN) has the greatest true negative rate (98.212%) and the highest accuracy rate for four attackers. i.e., DOS\_LOIC\_HTTP\_Attack (95.48%), Brute\_ForceWEB (94.84%), BruteForceXXS (95.14%), and DoS\_Hulk\_Attack (96.83%). The deep autoencoder (DA) is comparatively better than others. The detection rate is quite high on three different attacks, such as Infiltration (93.77%), Brute\_ForceWEB (95.11%), and DoS\_SlowLoris\_Attack (95.03%). The Deep Boltzmann machines (DBM) learn

**TABLE 3.** System performance for diverse attacks.

State-of-the-Art Attacks	DNN	RNN	CNN	RBN	DBN	DBM	DA
Brute_ForceXXS	94.50%	<b>95.62%</b>	93.66%	90.129%	<b>95.14%</b>	91.40%	92.90%
Brute_ForceWEB	<b>94.50%</b>	<b>95.22%</b>	92.66%	90.33%	<b>94.84%</b>	93.20%	<b>95.11%</b>
DoS HTTP	93.03%	92.75%	91.13%	91.01%	90.51%	92.42%	92.23%
DoS UDP	92.40%	93.78%	91.79%	82.38%	91.21%	91.543%	91.54%
DoS TCP	90.50%	93.14%	93.99%	90.98%	92.10%	92.19%	92.70%
DDoS HTTP	91.46%	91.55%	89.12%	92.33%	89.65%	90.86%	90.87%
OS Server scanning	92.12%	92.33%	92.66%	90.22%	92.93%	89.77%	91.22%
OS Fingerprinting	93.51%	90.16%	91.21%	90.41%	91.42%	92.20%	93.77%
Infiltration	94.11%	96.15%	97.22%	92.10%	92.81%	92.90%	92.11%
Botnet	93.50%	93.55%	97.80%	91.14%	92.30%	95.09%	92.74%
DOS_LOIC_HTTP_Attack	92.30%	94.63%	97.73%	94.51%	95.48%	93.56%	94.59%
DOS_GoldEyes_Attack	96.44%	97.55%	95.234	90.877%	90.55%	96.63%	91.72%
DOS_HOIC_Attack	93.22%	93.10%	95.14%	94.25%	93.23%	94.93%	90.20%
DOS_LOIC_UDP_Attack	92.22%	93.10%	95.00%	92.25%	92.23%	94.93%	90.20%
DoS_SlowLoris_Attack	97.09%	97.90%	92.55%	91.90%	93.10%	92.02%	95.03%
DoS_SlowHTTPTest_Attack	94.50%	92.10%	91.33%	90.75%	90.46%	95.03%	90.45%
DoS_Hulk_Attack	<b>95.30%</b>	96.88%	92.90%	92.72%	<b>96.83%</b>	<b>96.02%</b>	91.95%

**TABLE 4.** Comparison results for the UNSW-NB15 dataset (%).

Comparison With Other State-of-the-Art Attacks	DNN	RNN	CNN	RBN	DBN	DBM	DA
Normal	88.22%	87.00%	83.01%	95.00%	88.13%	94.93%	90.20%
DoS	87.09%	88.00%	89.55%	85.90%	86.11%	89.02%	88.01%
Analysis	94.50%	92.10%	91.33%	90.75%	90.46%	95.03%	90.45%
Exploits	89.22%	90.88%	88.61%	88.92%	87.13%	88.02%	89.00%
Generic	96.99%	92.33%	92.09%	92.30%	96.02%	92.00%	90.13%

good generative models. The DBM gives the highest accuracy and detection rate on five different types of attacks, such as DoS DOS\_GoldEyes\_Attack (94.63%), DOS\_LOIC\_UDP\_Attack (94.93%), and Botnet (95.09%), DoS Attacks-Hulk (96.02%), DoS attacks-SlowHTTPTest and (95.03%).

Table 4 shows that the UNSW-NB15 database helps to achieve the best overall performance compared to the other seven well-known models, except for the overall recall rate with five different attacks (DNN (in generic attack) performs slightly higher as compared to others, such as 96.99%, whereas CNN in Normal Attack performs lower than 83.01%). UNSW-NB15 reaches the highest detection rate on the Normal, Generic, DoS, Analysis, and Exploits.

In this section, we explained metrics and performance measurement (07) equations such as ACC (Attack), Precision (attack), true positive attack TPR (attack), true negative rate TNR(attack), recall RE(attack), false positive rate FPR (attack), F1 Score (attack), we express various substances where positive FP (attack) are false and true positive TP (attack) are related to attack data appropriately or incorrectly, the measurement true positive TP (attack) and false-positive FP (attack) is used to classify the normal data, and attacks. Subsequently, the performance measurement equations (01-07) are defined as:

The ACC (attack) is a classical metric for evaluating the accuracy of classification models, in which ACC denotes the fraction of the total number of assaults accurately

**TABLE 5.** Evaluation results of various attacks.

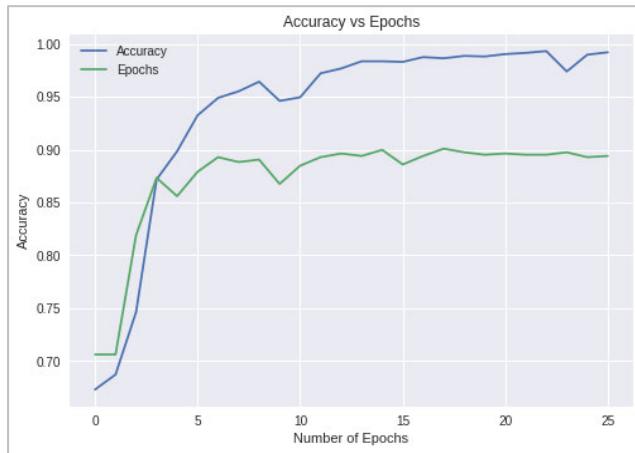
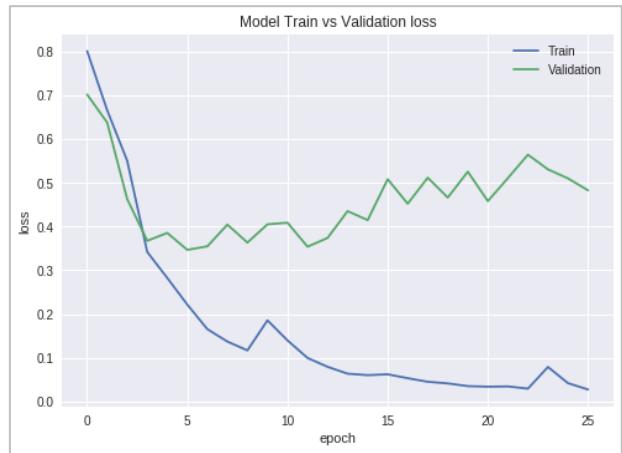
Other State-of-the-Art Methods of Deep Learning	Reference	System	Database	Accuracy	ACC (PR.)	ACC (PR.)	FS.
Dynamic AE Sparse System	[58]	ID system	NDLKDD	92.39	91.33	Nil	0.92
Automated AE.	[41]	ID. System	NSLKDD	92.22	93.22	Nil	0.91
Deep Belief Network	[59]	ID. System	KDDCup99	92.22	91.22	0.76	Nil
Convolutional AE CNN-AE	[60]	ID. System	CTUUNB	Nil	96.02	Nil	0.96
Autoencoder (AE)	[61]	MD, ID System	NSLKDD	82.23	Nil	Nil	Nil
	[41]	ID. System	NSLKDD	92.02	90.22	Nil	0.944
	[62]	ID. System	KDDCup99	95.77	97.03	2.00	0.97.90
	[62]	ID System	NSLKDD	89.22	92.97	10.78	0.910
AE Sparse System	[63]	ID. System	KDDCup99	93.71	94.53	0.42	Nil
Autoencoder (AE.)	[64]	ID. System	KDDCup99	79.88	80.00	Nil	Nil
AE Sparse System	[65]	ID. System	NSLKDD	97.40	Nil	Nil	0.990
Proposed framework	None	ID. System	NSL-KDD	96.90	95.21	94.50	95.03
		ID. System	KDDCup99	90.01	85.11	89.23	87.22
		ID. System	UNSW-NB15 Databased	95.90	94.20	91.41	90.18

categorized. Fig 5 depicts that each epoch processes the actual data from the system, either backwards or forward. The RE (attack) or TPR (attack) measurement focuses on the proportion of predicated attacks from the entire attack data, the PR (Attack) is only interested to determine the fraction of attack data accurately categorized from all data, indicating how many assaults are genuinely predicated as actual attacks. Maximizing PE (attack) will minimize the number of FP, whereas maximizing RE (attack) will minimize the number of FN FNR (attack) and estimates the percentage of the number of attacks and the number of miscounted average data from the entire sample. The second name of FPR (attack) is a FAR (attack) measure, and it is based on the fraction of innocuous incidents that are mistakenly categorized as attacks. TNR (attack) may be predicted as the fraction of attack samples in the total samples. The F1-Measure, or F1-score (attack), The F1 score is a cumulative total of PR and RE, which equally represents the precision and recall, the variant most often used when imbalanced data and exemplifies accuracy both in recognition rate.

The stats in Table 5 provide thorough information on attack detection on deep learning methods such as RNN, CNN, and DNN, as explained in the methodology section. Of the listed methods, most of them work on malware detection and intrusion detection. In this paper, we emphasize imbalances in results between researchers and dataset-wise. The different authors adopt distinct databases, settings, and measures. In this paper, we used quality measurements to analyze the results and compare and contrast the accuracy of listed methods such as RNN, CNN, and DNN with the help of measurement metrics such as F1 score, accuracy, precision, and FPR.

Furthermore, Table 2 also roughly summarizes and highlights the deep learning methods for detecting different types of attacks. Figures 5 and 6 depict the proposed framework accuracy and loss with 25 epochs, in graphs representing the system's performance drastically changing at specific points and with distinct hyperparameters. As shown in Table 4, the advised performances of numerous types of assault detection structures are different from each other. According to the authors, all four (CNN, AE, DBN, and LSTM) provide the best overall identification accuracy in the order of decreasing. The hybrid approaches are inconsistent, as their performances show that they are linked with classifiers in groups.

In addition, DBN is the top performer because of its intrinsic characteristics of more than one layer in processing large amounts of unlabeled data. In addition, LSTM, by utilizing connected temporal assets for more detailed simulation, may outperform in terms of results compared to CNN. AE can also be plagued by a large amount of unlabeled data that lacks adequate understanding or layers to understand the complexity buried. Generally, it's far more fascinating to notice that AE and RBM are better and more famous for instruction and cyber threat identification by using unlabeled points and fine-tuning some label points. The results in Table 4 summarized the results of ID, MD with quantitative evaluation using various deep learning for analyzing the types of attacks, cyber-attacks and malware detection, correspondingly, discovering that the high-quality overall performance completed via assault detection techniques on KDDCup ninety-nine datasets by ACC values obtained via indexed techniques as the primary assessment index, significantly, 99.8%, performed with the aid. The samples of

**FIGURE 5.** System training and validation accuracy on 25 epochs.**FIGURE 6.** System training and validation accuracy on 25 epochs.

the NSLKDD database are more significant than others, and the accuracy (98.3%) performed with the aid demonstrates that the NSLKDD database is far more challenging than the KDDCup99 dataset due to the inclusion of uncertain times in the testing database. Another relevant element is that all CNN-primarily based techniques avoid using the KDD-Cup 89 and NSLKDD datasets because of their restricted sample size. I could not help demonstrating the noticeable strength of CNN for developing distinctive descriptors with lots of details. Therefore, several deep learning approaches, mainly unsupervised learning techniques, should expose the scarcity of sufficient schooling samples. We can see that the general performance of AE-primarily based strategies is unequal, with the most advanced AE-primarily based strategies being unquestionably superior to the traditional methods. The AE form may lose critical records during the compression process. However, with new designs, enhanced AE might better understand critical and informative components of the source file. Likewise, LSTM-primarily based and GRU-based strategies exceed RNN-primarily based techniques regarding gate efficiency and memory cell shape architecture. Such creative designs boost the capability to retain long-term period information, resulting in a more significant long-term connection, as shown in Figures 5 and 6.

Recently, researchers proposed various DBN and RNN-based methods for attacks and intrusion detection in image and text processing. To classify the DBN and RNN, traditional supervised and unsupervised methods are used, correspondingly compared, and elucidate the benefits and disadvantages of both groups. The RNN is an Essential and essence unit. It recalls information from the previous store moment, uses it in the current calculation as input, and keeps storing temporal information for more transparent and authentic classifications. Moreover, with enough instances, the RNN has an effective structure in the situation of old and new cyber-attacks; on the other hand, DBN is capable of automatically detecting features and patterns from the input.

**TABLE 6.** Hyperparameters.

Hyperparameters	Values
Epochs	25
Activation	Adam
Optimization	Softmax
Hidden units	600-800
Regularization (dropout values)	0.2
Batch Size	500

Lastly, the unsupervised DBN has a lower risk of overfitting.

$$ACC(Attack) = \frac{TP_{attack} + TN_{attack}}{TP_{attack} + FN_{attack} + TN_{attack} + FP_{attack}} \quad (4)$$

$$PR(Attack) = \frac{TP_{attack}}{TP_{attack} + FP_{attack}} \quad (5)$$

$$RE(Attack) = \frac{TP_{attack}}{TP_{attack} + FN_{attack}} \quad (6)$$

$$FNR(Attack) = \frac{FN_{attack}}{TP_{attack} + TN_{attack}} \quad (7)$$

$$FPR(Attack) = \frac{FP_{attack}}{FP_{attack} + TN_{attack}} \quad (8)$$

$$TNR(Attack) = \frac{TN_{attack}}{TN_{attack} + FP_{attack}} \quad (9)$$

$$FS(attack) = \frac{2 * PR(attack) * RE(attack)}{PR(attack) * RE(attack)} \quad (10)$$

This experiment is performed on Google colab with python 3 with GPU (Graphics processing unit) and TPU. (Tensor processing unit) with distinct settings. The system is tested on various hyper parameters such as regularization, activation (hard sigmoid, nadam, Adamax and Adam) and optimization (relu, sigmoid, softplus and softmax). The system's performance is greater than 95% in terms of accuracy with mentioned hyperparameters in Table 6.

## V. CONCLUSION AND FUTURE SCOPE

This paper discusses the involving challenges and limitations in previous studies, which have been investigating how to use deep learning in the early detection and eradication of cyber threats. These highlighted issues pose serious issues in today's world scenario. Many problems still exist that require investigation. And so, it is also quite challenging to amend DL methods for attack detection as a real classifier. As mentioned previously, the deep learning approaches reduce the features, pattern dimensions, and evaluation costs throughout the feature extraction. This study employs deep learning techniques for cyber-attack malware detection, such as identification and discriminative. However, the paper summarized the seven approaches, i.e., deep learning (RNN, CNN, and DNN) and generative models/methods (RBN, DBN, DBM., and DA). In addition, this research investigation focuses on accuracy and provided dictionaries in the research field. The experimentation of this study demonstrates IDS and Cybersecurity attacks, which are detected successfully using a collaborative technological environment. Also, we have investigated to find which DL techniques performed better among the others. According to this analysis, the use of deep learning methods increases the investigational rate of classification intrusion while providing a robust performance of state-of-the-art supervised systems. In this scenario, a part of future work, this study extended to include advanced deep learning methods and transfer learning approaches. Moreover, the robustness of the supervised system is validated using IDS training. Moreover, this proposed approach may not always be sufficient for all attacks. Therefore, this is a need to investigate other possible ways. Thus, when designing a newfangled Intrusion Detection System (IDS), the properties can be used in the real-time system to detect internal and external intruders and their malicious behaviors. This research will validate IDS and, in the future, identify the internal and external intruder's accurately in real-time and be used by several firms and MNCs to protect their value.

## REFERENCES

- [1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 2, pp. 84–90, Jun. 2017.
- [3] M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain, D. S. Duranta, and M. A. Rahman, "Melanoma skin lesions classification using deep convolutional neural network with transfer learning," in *Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA)*, Apr. 2021.
- [4] A. Ahmin, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," *Int. J. Commun. Syst.*, vol. 31, no. 9, p. e3547, Jun. 2018.
- [5] A. Ahmin, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 228–233.
- [6] Z. Dewa and L. A. Maglaras, "Data mining and intrusion detection systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 1–10, 2016.
- [7] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simoes, and H. Janicke, "A novel intrusion detection mechanism for SCADA systems which automatically adapts to network topology changes," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 4, no. 10, p. e4, 2017.
- [8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.
- [9] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115524.
- [10] A. A. Salih, S. Y. Ameen, S. R. Zeebaree, M. A. Sadeeq, S. F. Kak, N. Omar, I. M. Ibrahim, H. M. Yasin, Z. N. Rashid, and Z. S. Aeed, "Deep learning approaches for intrusion detection," *Asian J. Res. Comput. Sci.*, vol. 9, no. 4, pp. 50–64, 2021.
- [11] J. Azevedo and F. Portela, "Convolutional neural network—A practical case study," in *Proc. Int. Conf. Inf. Technol. Appl.* Singapore: Springer, 2022, pp. 307–318.
- [12] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.
- [13] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 27, 2014, pp. 1–9.
- [14] G. Awad, C. G. Snoek, A. F. Smeaton, and G. Quénot, "Trecvid semantic indexing of video: A 6-year retrospective," *ITE Trans. Media Technol. Appl.*, vol. 4, no. 3, pp. 187–208, 2016.
- [15] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 2818–2826.
- [16] M. Uddin, R. Alsaqour, and M. Abdelhaq, "Intrusion detection system to detect DDoS attack in Gnutella hybrid P2P network," *Indian J. Sci. Technol.*, vol. 6, no. 2, pp. 71–83, 2013.
- [17] R. L. Haupt and S. E. Haupt, *Practical Genetic Algorithms*. Wiley, 2004, doi: [10.1002/0471671746](https://doi.org/10.1002/0471671746).
- [18] D. Hossain, G. Capi, and J. M., "Optimizing deep learning parameters using genetic algorithm for object recognition and robot grasping," *J. Electron. Sci. Technol.*, vol. 16, no. 1, pp. 11–15, 2018.
- [19] O. E. David and I. Greental, "Genetic algorithms for evolving deep neural networks," in *Proc. Companion Publication Annu. Conf. Genetic Evol. Comput.*, Jul. 2014, pp. 1451–1452.
- [20] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with Naïve Bayes feature embedding," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102158.
- [21] E. Gyamfi and A. Jurcut, "Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, May 2022.
- [22] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, "A hybrid intrusion detection model using EGA-PSO and improved random forest method," *Sensors*, vol. 22, no. 16, p. 5986, Aug. 2022.
- [23] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I.-K. Wang, "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9310–9319, Jun. 2021.
- [24] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (AI)-empowered intrusion detection architecture for the Internet of Vehicles," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 144–149, Jun. 2021.
- [25] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.
- [26] A. S. Dina and D. Manivannan, "Intrusion detection based on machine learning techniques in computer networks," *Internet Things*, vol. 16, Dec. 2021, Art. no. 100462.
- [27] H. Zhang, J. L. Li, and X. M. Liu, C Dong, "Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection," *Future Gener. Comput. Syst.*, vol. 122, pp. 130–143, Sep. 2021.
- [28] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.
- [29] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, Jan. 2019.

- [30] J. Toldinas, A. Venčkauskas, R. Damaševičius, Š. Grigaliūnas, N. Morkevičius, and E. Baranauskas, "A novel approach for network intrusion detection using multistage deep learning image recognition," *Electronics*, vol. 10, no. 15, p. 1854, Aug. 2021.
- [31] G. Andresini, A. Appice, and D. Malerba, "Autoencoder-based deep metric learning for network intrusion detection," *Inf. Sci.*, vol. 569, pp. 706–727, Aug. 2021.
- [32] K. Gupta, D. K. Sharma, K. Datta Gupta, and A. Kumar, "A tree classifier based network intrusion detection model for Internet of Medical Things," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108158.
- [33] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2016, pp. 258–263.
- [34] F. Jiang, Y. Fu, B. B. Gupta, Y. Liang, S. Rho, F. Lou, F. Meng, and Z. Tian, "Deep learning based multi-channel intelligent attack detection for data security," *IEEE Trans. Sustain. Comput.*, vol. 5, no. 2, pp. 204–212, Apr. 2018.
- [35] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2019.
- [36] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Electr. Power Energy Syst.*, vol. 107, pp. 690–702, May 2019.
- [37] M. Uddin, A. A. Rahman, A. Alarifi, M. Talha, A. Shah, M. Iftikhar, and A. Zomaya, "Improving performance of mobile ad hoc networks using efficient tactical on demand distance vector (TAODV) routing algorithm," *Int. J. Innov. Comput., Inf. Control.*, vol. 8, no. 6, pp. 4375–4389, 2012.
- [38] A. A. Khan, A. A. Laghari, T. R. Gadekallu, Z. A. Shaikh, A. R. Javed, M. Rashid, V. V. Estrela, and A. Mikhaylov, "A drone-based data management and optimization using Metaheuristic algorithms and blockchain smart contracts in a secure fog environment," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108234.
- [39] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, "Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device," *Ad Hoc Netw.*, vol. 84, pp. 82–89, Mar. 2019.
- [40] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, "Hybrid intelligent intrusion detection scheme," in *Soft Computing in Industrial Applications*. Berlin, Germany: Springer, 2011, pp. 293–303.
- [41] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in *Proc. 2nd Int. Conf. Adv. Cloud Big Data*, Nov. 2014, pp. 247–252.
- [42] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *Proc. Nat. Aerosp. Electron. Conf. (NAECON)*, Jun. 2015, pp. 339–344.
- [43] A. Ayub Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," *IEEE Access*, vol. 10, pp. 78887–78898, 2022.
- [44] Z. A. Shaikh, A. A. Khan, L. Teng, A. A. Wagan, and A. A. Laghari, "BIoMT modular infrastructure: The recent challenges, issues, and limitations in blockchain hyperledger-enabled E-healthcare application," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–14, Sep. 2022.
- [45] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.
- [46] H. Zhang, X. Yu, P. Ren, C. Luo, and G. Min, "Deep adversarial learning in intrusion detection: A data augmentation enhanced framework," 2019, *arXiv:1901.07949*.
- [47] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, "Cyber-attack classification in smart grid via deep neural network," in *Proc. 2nd Int. Conf. Comput. Sci. Appl. Eng.*, Oct. 2018, pp. 1–5.
- [48] J. Kim, Y. Shin, and E. Choi, "An intrusion detection model based on a convolutional neural network," *J. Multimedia Inf. Syst.*, vol. 6, no. 4, pp. 165–172, Dec. 2019.
- [49] L. Zhang, L. Shi, N. Kaja, and M. D., "A two-stage deep learning approach for car intrusion detection," in *Proc. Ground Vehicle Syst. Eng. Technol. Symp. (GVSETS)*, Aug. 2018, pp. 1–11.
- [50] D. Li, R. Baral, T. Li, H. Wang, Q. Li, and S. Xu, "HashTran-DNN: A framework for enhancing robustness of deep neural networks against adversarial malware samples," 2018, *arXiv:1809.06498*.
- [51] Z. A. Shaikh, A. A. Khan, L. Baitenova, G. Zambinova, N. Yegin, N. Ivolgina, A. A. Laghari, and S. E. Barykin, "Blockchain hyperledger with non-linear machine learning: A novel and secure educational accreditation registration and distributed ledger preservation architecture," *Appl. Sci.*, vol. 12, no. 5, p. 2534, Feb. 2022.
- [52] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
- [53] H. Tian, S. Pouyanfar, J. Chen, S. C. Chen, and S. S. Iyengar, "Automatic convolutional neural network selection for image classification using genetic algorithms," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2018, pp. 444–451.
- [54] Y. Sun, B. Xue, M. Zhang, G. G. Yen, and J. Lv, "Automatically designing CNN architectures using the genetic algorithm for image classification," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3840–3854, Sep. 2020.
- [55] A. A. Khan, A. A. Laghari, M. Shafiq, O. Cheikhrouhou, W. Alhakami, H. Hamam, and Z. A. Shaikh, "Healthcare ledger management: A blockchain and machine learning-enabled novel and secure architecture for medical industry," *Hum.-Centric Comput. Inf. Sci.*, vol. 12, pp. 1–15, Nov. 2022.
- [56] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF)," *Neurosci. Informat.*, vol. 2, no. 1, Mar. 2022, Art. no. 100030.
- [57] A. F. M. Agarap, "A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data," in *Proc. 10th Int. Conf. Mach. Learn. Comput.*, Feb. 2018, pp. 26–30.
- [58] R. C. Aygun and A. G. Yavuz, "Network anomaly detection with stochastically improved autoencoder based models," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2017, pp. 193–198.
- [59] A. A. Khan, A. A. Laghari, M. Shafiq, S. A. Awan, and Z. Gu, "Vehicle to everything (V2X) and edge computing: A secure lifecycle for UAV-assisted vehicle network and offloading with blockchain," *Drones*, vol. 6, no. 12, p. 377, Nov. 2022.
- [60] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, May 2017, pp. 3854–3861.
- [61] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
- [62] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 22679–122695, 2022.
- [63] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019.
- [64] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS)*, 2016, pp. 21–26.
- [65] M. A. Umer, K. N. Junejo, M. T. Jilani, and A. P. Mathur, "Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations," *Int. J. Crit. Infrastructure Protection*, vol. 38, Sep. 2022, Art. no. 100516.
- [66] V. Ponnusamy, M. Humayun, N. Z. Jhanjhi, A. Yichiet, and M. F. Almufareh, "Intrusion detection systems in Internet of Things and mobile ad-hoc networks," *Comput. Syst. Eng.*, vol. 40, no. 3, pp. 1199–1215, 2022.
- [67] M. Sarhan, S. Layeghy, and M. Portmann, "Towards a standard feature set for network intrusion detection system datasets," *Mobile Netw. Appl.*, vol. 27, no. 1, pp. 357–370, Feb. 2022.
- [68] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, p. e4150, Jan. 2021.
- [69] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021.
- [70] M. H. Nasir, S. A. Khan, M. M. Khan, and M. Fatima, "Swarm intelligence inspired intrusion detection systems—A systematic literature review," *Comput. Netw.*, vol. 205, Mar. 2022, Art. no. 108708.

- [71] H. Alrubayyi, G. Goteng, M. Jaber, and J. Kelly, "Challenges of malware detection in the IoT and a review of artificial immune system approaches," *J. Sensor Actuator Netw.*, vol. 10, no. 4, p. 61, Oct. 2021.
- [72] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, "Enhancing IIoT networks protection: A robust security model for attack detection in internet industrial control systems," *Ad Hoc Netw.*, vol. 134, Sep. 2022, Art. no. 102930.
- [73] I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain, and H. Soliman, "Federated-SRUs: A federated simple recurrent units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems," *IEEE Internet Things J.*, early access, Aug. 19, 2022, doi: 10.1109/JIOT.2022.3200048.
- [74] I. A. Khan, N. Moustafa, D. Pi, K. M. Sallam, A. Y. Zomaya, and B. Li, "A new explainable deep learning framework for cyber threat discovery in industrial IoT networks," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11604–11613, Jul. 2021.



**IRFAN ALI KANDHRO** received the Master of Science degree in computer science from Mohammad Ali Jinnah University, Karachi, Pakistan, in 2019. He is currently pursuing the Ph.D. degree in computer science with Sindh Madressatul Islam University, Karachi. He has worked for more than seven years as a Lecturer and a Software Engineer. He has published multiple research papers in international and ISI indexed journals, conferences, and workshops. His research interests include programming languages machine learning, deep learning, computer vision, and natural language processing.



**SULTAN M. ALANAZI** received the master's degree in IT and the Ph.D. degree in computer science from The University of Nottingham, U.K. He worked as a Teaching Assistant at The University of Nottingham. He has more than ten years of experience in the IT field. He is currently an Assistant Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. He has published several research papers in reputed international journals and conferences. His research interests include cybersecurity, machine learning, NLP, social network analysis (mining), user-modeling, and recommender systems.



**FAYYAZ ALI** received the bachelor's degree in computer engineering from the Sir Syed University of Engineering and Technology, Karachi, and the Master of Science degree in software engineering from the University of Hertfordshire, U.K. He has worked for more than three years as a Lecturer and 11 years in industry on different positions in various companies. He has published multiple research papers in international and ISI-indexed journals, conferences, and workshops. His research interests include software methodologies, business processes, ERP systems, programming languages, machine learning, deep learning, computer vision, and natural language processing.



**ASADULLAH KEHAR** received the Ph.D. degree from Shah Abdul Latif University, Khairpur, Pakistan. He is currently working as an Assistant Professor at the Institute of Computer Science, SALU, Pakistan. His research interests include software engineering, digital image processing, and data sciences. He has supervised several post-graduate level students. He has published various research articles on state-of-the-art technologies.



**KANWAL FATIMA** is currently pursuing the bachelor's degree in computer science with Sindh Madressatul Islam University, Karachi, Pakistan. She has more than two years of experience creating blogs, articles, and other content for content writer in Pakistan. She has experience working on many websites as a Researcher and a Content Writer. Her research interests include programming languages, deep learning, computer vision, and natural language processing.



**MUEEN UDDIN** received the Ph.D. degree from Universiti Teknologi Malaysia (UTM), in 2013. He is currently working as an Associate Professor in data and cybersecurity at the University of Doha for Science and Technology, Qatar. He has published more than 130 international journals and conference papers in highly reputed journals with a cumulative impact factor of over 300. His research interests include blockchain, cybersecurity, the IoT security, and network and cloud security.



**SHANKAR KARUPPAYAH** (Member, IEEE) received the B.Sc. degree (Hons.) in computer science from Universiti Sains Malaysia, in 2009, the M.Sc. degree in software systems engineering from the King Mongkut's University of Technology North Bangkok (KMUTNB), in 2011, and the Ph.D. degree from TU Darmstadt with his dissertation titled Advanced Monitoring in P2P Botnets, in 2016. He has been a Senior Researcher/a Postdoctoral Researcher with the Telecooperation Group, TU Darmstadt, since July 2019. He has also been a Senior Lecturer at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, since 2016. He is currently working actively on several cybersecurity projects and working groups, e.g., the National Research Center for Applied Cybersecurity (ATHENE), formerly known as the Center for Research in Security and Privacy (CRISP).

• • •