Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-09 Issue-01 No. 01 : 2022

An Intelligent Network Intrusion Detection System using Deep Neural Network

Dr.S.Kalarani Professor, Department of Information Technology, St Joseph's Institute of Technology, OMR, Chennai, India : kala.rani1971@gmail.com

Abstract:
Machine learning techniques are extensively used to enhance intrusion detection (IDS) systems to detect and classify cyber-attacks on the network and host levels quickly and automatically. A comprehensive evaluation of DNN and other classic machine learning classifier experiments is presented in a variety of publicly available benchmark malicious datasets. The optimum DNN network parameters and network topology are determined using the KDDCup99 and NSDL-KDD Datasets by the following hyperparameter selection method. Network Intrusion Detection Systems (NIDS) support system administrators in their organizations in exploring network security breaches. All experiments in DNN run up to 1,000 epochs, where the learning rate varies in the range of 0.01-0.5]. Rigorous experimental testing confirms that DNNs perform well compared to traditional machine learning classifiers.

Keywords: cyberattacks, intrusion detection, malware, deep learning, deep neural networks, KDDCup99, NSL-KDD

1. *Introduction:*

The increase in connectivity is provided to all industries by the Industrial Internet of Things (IIoT), which creates information and intelligence for operations. Industrial Internet of Things is used in a variety of industries to connect information, services and people in various management areas such as smart energy, smart cities, medical care, automation, agriculture, logistics and transportation [1]. To maintain critical infrastructure, a larger network is required to connect to several sensors. IIoT aims to provide smart manufacturing products that create smart factories for effective communication between partners and customers [2]. Industry 4.0 focused on the problem of optimizing the industry for the consumption of data-driven service smart devices. This large-scale network implicates these smart devices to certain cyber attack threats. Industrial structures are closely integrated and scammers are more intelligent. Industrial Control Systems (ICS) consist of several classes of industrial process control systems and integrated components. ICS is facing more and more cyber attacks. Ineffective security measures negatively impact employees and organizations. Consequences include production delays, damage to buildings, medical and compensatory expenses, loss of property, business losses, legal fees, and damage to tools and equipment.

Intrusion detection systems identify weak points in network traffic in a network infrastructure. You can decide when the hacker starts scanning your device. This is the first step in building security in the Internet of Things [3]. In IDS systems, data security logs and system master data audit logs are collected and system key points are identified to determine if network security is at risk. An IDS solution for IoT must be adapted to the characteristics of the device. The Internet of Things uses deep learning methods to improve the efficiency of IoT applications. Balance the computational costs and efficiency of next generation IoT networks [4].

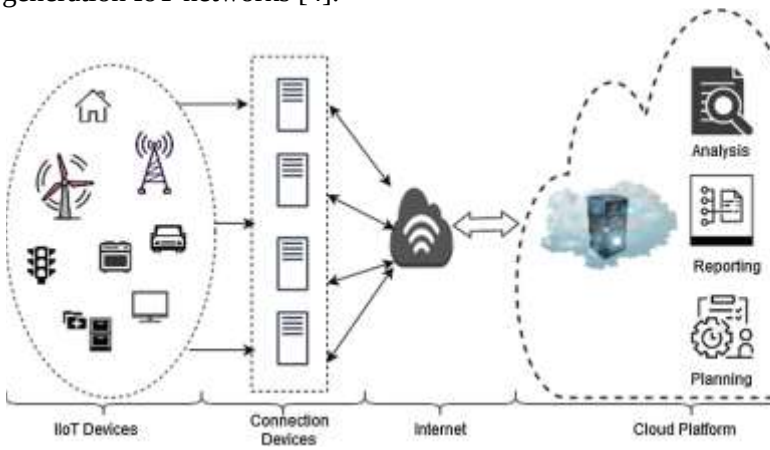

Fig. 1: IIoT Architecture

In several environments, IoT devices are deployed, including remote areas where maintenance work is not feasible, as shown in Figure 1. The logic of IoT device control cannot also be ascertained by the objective environment. IoT devices are susceptible to many attacks, including DDoS, DoS, identity robbery, privilege elevation and IoT networks [5].

A few studies have already shown different techniques of IDS. This article evaluates some many existing approach for detecting IoT intrusions. This chapter presents an analysis of key targets. This study describes first a systematic review of IoT and intrusion detection systems [6]. After that, we evaluate several emerging deep learning techniques with the benefits and drawbacks of IoT projects. The following focuses on several performance metrics and IDS-IIoT datasets. The limitations and challenges of current research integration methods are discussed [7]. Finally, solutions to these and future challenges are identified. The most important contributions are:

(a) Control IDS systems that rely on deep learning for numerous manufacturing IoT networks.
(b) Several IoT intrusion detection studies are under review. Research objective
Run algorithms to develop methods for identifying attacks
(C) A robust approach to anomaly detection using basic and deep CNN classification techniques

The rest of the work is organized as follows. Section 2 provides a brief review of the work in question. Chapter 3 describes the proposed model for identifying IoT attacks. Section 4 describes the analysis of the results and performance of the proposed model across different datasets. Conclusions and suggestions are presented in Section 5 for future work.

2. Background:

2.1 Intrusion Detection System:

IDS is used for tracking for malware activity on complex systems or nodes. It is an engage that can safeguard a node or a network against such an assailant [8]. Suspicious activity can be defined as a sensor node intrusion. Hardware or software tools can be IDS systems. IDS can identify known attacks and lead to malicious user actions of network behavior. It detects various hackers, analyzes network nodes and activity, and detects intrusions, then alerts users. In other words, they are called alarms or network monitors [9]. Minimize system damage by creating alerts before receiving malicious attacks. IDS systems are capable of detecting both internal (AI) and external (EA) attacks. AIs are generated by malicious nodes with interconnected networks. Expert Advisors are created by externally regulated third parties. IDS monitors and detects network packets as unauthorized or valid users. IDS has three stages: monitoring, searching and alerting. A monitor monitors network patterns, traffic and resources. Search is an important factor in determining intrusion by a particular algorithm. The alarm unit issued an alarm when the intrusion was confirmed [10].

*Requirement for IDS in Industrial IoT***:**
The Internet of Things is an innovative effort to build an intelligent ecosystem by leveraging the benefits of the Internet of Things to manage industrial operations. The IoT is rapidly expanding the following sectors and services: IoT devices are used in healthcare systems to monitor, detect and monitor machines, patients and medicines [11]. IoT devices are used in the agricultural sector to monitor farm safety, efficiently irrigate plants and store produce [12]. In the supply chain industry, transport and logistics play an important role [13]. IoT devices are being used in this field to retrieve the traceability vehicle. The delivery process for a commodity is also motivated. The energy sector evaluates IoT networks for supply, payment and loss. In the mining sector, IoT equipment is used to manage disaster alarms and signals, track the movements of underground mines and monitor shipments [14]. ICS is defined by the strengths of the automation industry, including network monitoring and data collection (SCADA) and programmable logic controllers (PLCs). Most cyber attacks are carried out against industrial automation systems, such as Stuxnet attacks, German oven attacks, Shamoon attacks on Mirai, etc.

Countless cyber attacks are primarily directed at manufacturing units globally. Many cyber-criminal security flaws in IoT devices for attempting to attack manufacturing process. Stable behaviour patterns create well-protected existing infrastructure [15]. Therefore, robust intrusion detection mechanisms are needed to protect against attacks, combat and industrial systems. This section describes the IIoT deep learning system, a traditional intrusion detection system.

2.2 Review on IDS IIoT:

The Internet of Things is increasing alarmingly in cyber attacks driven by the growing number of connected communication applications, devices and networks. When an IoT attack occurs, the system

available to end users degrades and the number, cost and revenue of impersonation and breaches increase. Several studies and studies on IoT IDS using deep learning have been published, but there are no studies on the IoT approach to IIoT. This section describes several IDS approaches for deep learning-based IoT and IoT applications [16]. Some of the deep learning methods described for IDS are:

The author offers some ICS machine learning identifiers. DNN was used by the researchers to design IDS for IBS by findings in many other fields of DNN. For example, vehicle information security IDS signifiers based on DNN are provided [17]. The process utilizes DNN to improve safety of the vehicle network. The DNN is designed to predict the network parameters from the possibility functional vectors of the smart transportation packages. The system defines each class's probability as normal or intrusive, depending on the flow of traffic that is causing damage to the vehicle. In the CAN bus system control area network [18] and also the IDS system there was even a high intrusion detection against phishing software on automated driving communications systems. VANET IDS systems were studied using ANN for DoS attacks in this study. The objectives of the current assessment are to detect attacks via network-generated data such as labeled dataset. As quantifiable tracking data, IDS uses the extracted properties.

The authors [19] used Omni SCADA intrusion detection with long-term memory (LSTM). It serves as a data acquisition or monitoring control and detects temporal and irrelevant attacks. Irrelevant F1 metrics were identified in the feed-forward network (FNN) 99.95 ± 0.045% of the time and 60 ± 3% for cross attacks. The combination of hybridization of FNN and LSTM improved IDS performance by 99.34 ± 0.05 percent in F1 measurements.

Two IDSs have been developed in 2018 using two types of deep learning models. The first model was Deep Belief Network (DBN). The design is here trained and tested with fairly small data sets. The second model trains the DBN using an unnamed dataset and observes changes in intrusive patterns of network traffic. Safe architecture was introduced in the same year. [20] Analyzes secure ICS and SCADA intrusion detection network traffic with IoT platforms. This architecture consists of IDS identifiers from the DBN and SVM assemblies.

In 2019, an IDS model was introduced that exploits a sparse method of deep learning, [21] which involved a deep and discontinuous automatic encoder of high-level network traffic. The monitor then uses a deep learning network to segment the network traffic. The proposed model evaluates the effectiveness of intrusion detection in IoT systems using datasets collected from remote pipeline systems.

In 2020, the author proposed IDS to protect and maintain IoT systems through the benefits of deep random neural networks [1]. Nevertheless, the system has been evaluated on the UNSW-NB15 dataset and the Internet of Things was proved as feasible and applicable. The identification efficiency of the model was 99.54% with a low false alarm rate. Similarly, fusion-based IDS is being implemented to protect the IoT in [22]. The system divides the function of the received network traffic into four parts based on the correlation between the functions.

The authors [23] sought to fill a huge gap in the literature limited to the lack of data sets available for IoT / IoT advocacy solutions. The study give a fair representation evaluation table of seven sensors and three layers of cloud, fog and edge to simulate IoT/IT systems and network traffic in the real world. A large sample was authored for research purposes as TON IoT and used simulated IoT/IIoT tests to differentiate among normal and disruptive network activity.

The different machine learning based IDS methods accuracy are surveyed and are tabulated in Table 1.

Table 1: The different Machine learning techniques in cybersecurity

Methods	Dataset	Ref No.	Domain	Accuracy (%)	Precall (%)
Naïve Bayes	DARPA	[24]	Misuse	99.90	99.04
	NSL-KDD	[25]	Misuse	81.66	
	KDD CUP99	[26]	Signature	99.72	
ANN	DARPA	[27]	Misuse	99.82	

	NSL-KDD	[28]	Anomaly	94.50	
	KDD CUP99	[29]	Anomaly	62.90	
SVM	DARPA	[30]	Anomaly	95.11	
	NSL-KDD	[31]	Anomaly	89.70	
	KDD CUP99	[32]	Misuse	96.08	
Decision Tree	KDD	[33]	Hybrid	99.96	
	NSL-KDD	[34]	Anomaly	93.40	
	KDD CUP99	[35]	Anomaly	92.87	99.90
RF	KDD	[36]	Anomaly	99.95	99.80
	NSL-KDD	[37]	Hybrid	96.30	81.40

2.3 Key Findings from Review:

The literature survey above shows that a large number of studies have been published on the application of deep learning methods to build efficient identifiers in IoT environments. Many cyber attacks have occurred in the industrial sector around the world and have suffered heavy losses, but relatively little research has been done to design ICS IDS for ICS. Compared to ICS and IoT environments, very few studies have been conducted in IoT environments. This clearly shows that IoT security is still in its infancy. Therefore, cybersecurity researchers recommend using deep learning methods to develop intrusion detection systems in IoT environments.

Problem Formulation:

Traffic network data is usually gathered and stored in a raw TCP dump format. This data can be pre-processed for sequential translation. An interaction is a series of TCP packets that also start and end during certain periods with a well-defined protocol. Each connection log contains 100 bytes of information and the type of attack is classified as a public or private attack.

All system events are collected per process, usually system calls. Each p process includes a number of system call $S = sp_1, sp_2, \dots sp_n \; where \; s_p \in S, s_p$ is the set of final system call and S is the set of host system call. To distinguish the behavior between common classes and attack classes, a variety of system call information is used. You can use sp on labels like a normal attack to learn normal and offensive behaviors.

3. Proposed Model:

System calls are essential to computer operating systems and are the large amount of unstructured hashed text that typical HIDS uses to detect intrusions and cyber attacks. This study explores text representations to characterize the behavior of tracer calling systems. Current machine learning methods include feature extraction, function engineering, and job representation.

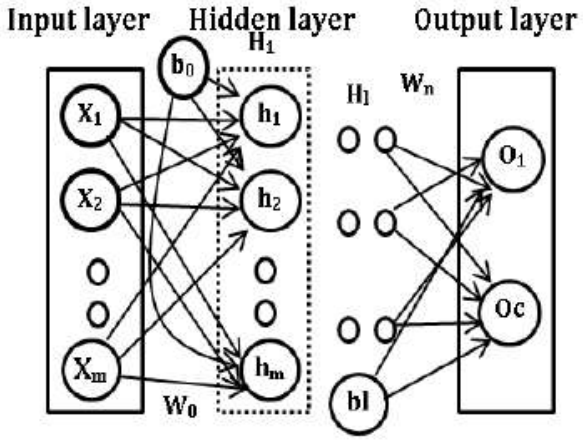

Fig. 2: Proposed DNN-ReLU IDS Prediction Model

Nevertheless, advanced built-in machine learning processes such as deep learning can totally prevent a need for design and resource extraction. To achieve contextual and consecutive relevant data from system calls, use sophisticated deep learning and text data visualization methods as shown in Figure 2.

3.1 Dataset:

For reasons of data protection and security, most of the datasets that currently represent attacks on

network traffic are private. Conversely, public datasets are subject to a number of anonymous risks. In particular, it is not possible to confirm that the dataset generally represents the current network traffic profile. KDDCup 99 is one of the most used public datasets. They report that many network properties, most notably remote client addresses, TTL options, TCP options, and TCP window size, are in fact wide range in real network traffic, even though the KDDCup 99 dataset appears to be small and of limited scope. Despite severe criticism, KDDCup 99 is the most widely used and reliable normative dataset for most studies on identity systems assessment and other security-related tasks [55]. To address some problems in KDDCup 99 [55], the more advanced version of NSL-KDD has been proposed. The paired correlation records were removed from the entire train and test data, and 136,489 and 136,497 invalid records were deleted from the test data. This protects the workbook from errors in the duplicate login history. NSL-KDD does not have a faithful representation of network traffic data.

The KDDCup 99 dataset was built on the 1998 DARPA dataset to challenge intrusion detection by processing the tcpdump data. We extracted the features from the raw tcpdump data using Automated Identity Model Mining (MADMAID) audit data. Detailed dataset statistics are shown in Table 1. At the MIT Lincon lab, the KDDCup1998 dataset was developed with thousands of UNIX and hundreds of users accessing it. The KDDCup99 dataset is available in two formats. They are entire datasets and 10% datasets. The dataset contains 41 characteristics and 5 classes ("Moderate", "DoS", "Probe", "R2L", "U2R").

NSL-KDD is a distilled version of intrusion data from KDDCup99. The filter is used for KDDCup 99 double-contact records deleted from test data, where it includes 136,489 and 136,497 contact records. NSL-KDD can inhibit machine learning algorithms from being skewed. This is helpful to monitor abuse of the KDDCup 99 dataset. Also there is a problem with the proof of identity of network traffic profile pages in real time. Table 2 provides detailed KDDCup99 and NSL-KDD dataset.

Table 2: Training and testing data from KDDCup 99 and NSL-KDD datasets

Type of Attack	Description	Data Set			
		KDDCup 99		NSL-KDD	
		Training	Testing	Training	Testing
Normal	Normal Connection Records	97,278	60,593	67,343	9710
DoS	Attacked in Network resource data	391458	229853	45,927	7458
Probe	Network Configuration Attack	4107	4166	11656	2422
R2L	Illegal Access	1126	16189	995	2887
U2R	Root computer attack	52	228	52	67
Total		494021	311029	125973	22544

4. Performance Measures:

Evaluations of various statistical measures should be based on truth values. The basic fact that consists of a series of related documents classified as normal or offensive is for binary classification. Allow L and A to be normal connection logs in the test dataset and attach the

connection logs. Each of these terms is used to define the quality of the evaluation model:
True Positive (TP) – The number of connection records properly classified into regular classes.
True Negative (TN) - The number of registers properly classified by category of attack.
Positive (FP): Number of global logs incorrectly classified as an attachment.
False Negative (FN) — The number of attachment logs wrongly classified as generic log records.

4.1 Experimental Design:

All experiments were performed using Ubuntu 14.0.4LTS with Python. All classical algorithms are implemented using Scikit-Learn3. A deep neural network (DNN) is implemented using TensorFlow4 on a back-end GPU which provides a high-level framework for Keras5. The GPU was an NVidiaGK110BGL Tesla K40 CPU configured with Gigabit Ethernet per second (32 GB RAM 2 TB fixed Intel® Xeon® CPU E3-1220 v3 at 3.10 GHz). Several test cases were considered to evaluate the performance of different DNNs and classifiers on different NIDS and HIDS datasets:
1) Classify network connection logs as benign or full capacity attacks.
2) Classify network connection logs as benign attacks, attacks, or classifications.
3) Classify network connection logs as benign or offensive and classify attacks with simple functions.

Since DNNs are parametric, it depends on their performance. The optimal parameters of the DNN network parameters and the DNN network topology were determined only on the KDDCup99 data set. Experiments were performed with the application of monitoring unit learning rates and activation functions using small and medium-sized constructs to determine optimal DNN parameters. The intermediate DNN has three levels. One is the input layer, the second is the cache, and the third is the output layer. Out of five neurons typically classify a connection register or attack the category attack.

The connections between modules from the input layer to the hidden layer and from the hidden layer to the output layer are fully connected. The first step was to normalize the train and test the datasets via L2 regularization. Two experiments with mean DNN were performed on hidden units 128,256,384,512,640,768,896 and 024. For each variable, experiments at 300 epochs were performed in the appropriate units. DNNs with a group of devices learned the normal 200-era communication pattern compared to those with attacks. It took 200 eras to acquire the critical ability to discriminate the connection logs of DNN attacks. For overfitting after 200 epochs, the normal connection log performance varies.
4.2 Results:
To identify the underlying methods, we evaluated traditional machine learning and DNN performance using the available NIDS and HIDS datasets. These datasets have been split and standardized with a second tier organization into a training dataset and a test dataset. The training datasets were used to train the machine learning models, as well as to evaluate the machine learning models for training using the test datasets. Multi-level training accuracy using KDDCup99 and NSL-KDD DNN. Most DNN topologies for the KDDCup 99 and NSLKDD datasets showed train accuracy between 98.5% and 98.6%.

Tables 3 and 4 show the detailed results of various classic machines and the binary and multiclass DNN classification. In the multiclass classification, the performance of NB is lower than that of KNN and RF, but exceeds the proposals LR, NB, KNN, RF SVM and DNN. This is because NB or SVM cannot be directly applied to multiclass classification problems. Multilayer strengthens the classifier when selecting individual attachments. In the KDDCup 99 and NSL-KDD tests, all classic TPRs were reduced as long as "R2L" and "U2R" were achieved compared to other categories such as "DoS" and "champion". The main reason for this is that the number of champions included in the training set is too small for each type of attack. In terms of accuracy, DNN's performance is far

superior to traditional machine learning classifications.

Table 3: Results of Multi-class classification KDDCup 99.

Method	Accuracy (%)				
	Normal	DoS	Probe	R2L	U2R
LR	81.2	83.2	98.7	98.7	97.4
NB	89.8	87.4	98.3	98.8	97.3
KNN	64.2	61.7	97.6	97.6	98.3
RF	64.6	64.3	97.5	96.4	97.1
SVM	62.4	69.2	97.7	98.6	97.5
Proposed DNN	93.8	96.3	99.4	99.5	98.5

Table 4: Results of Multi-class classification NSL-KDD

Method	Accuracy (%)				
	Normal	DoS	Probe	R2L	U2R
LR	68.2	77.2	89.9	91.7	87.9
NB	53.4	67.2	88.6	93.8	86.5
KNN	76.9	88.9	92.9	95.3	87.9
RF	76.8	91.5	97	96.9	88.2
SVM	71.2	90.7	94.2	95.7	90.6
Proposed DNN	89.5	94.6	96.3	98.6	96.4

Existing machine learning classifiers and DNNs have been successful in KDDCup99 compared to NSL-KDD. NSL-KDD is an enhanced KDDCup99 dataset version. The dataset consequently includes its own set of train registers and test links. NSL-KDD connection records are non-linear results in differences compared to KDDCup 99. In addition, traditional machine learning and DNN classifiers work far worse than KDDCup 99 and NSL-KDD.

The major finding of the proposed work is as follows.

The two IIoT standard data sets achieve a maximum accuracy of 99 percent. The Adam optimizer enhances the precision of ANN to offer the best overall efficiency. The accuracy of the proposed model for attack identification is evaluated by comparing to the last model in Tables 4 and 5. It is an intrusion detection method that incorporates various KDDCup99 and NSL-KDD datasets.

5. Conclusion:

In this paper, we propose a hybrid intrusion detection system and a highly scalable alarm system for analyzing network and host activity on consumer hardware servers. The DNN model was selected through a comprehensive evaluation of its performance against conventional machine classifications based on various IDS criteria. The proposed architectural design surpasses the traditional machine learning classifiers HIDS and NIDS. This is the only framework that uses DNNs to deploy, collect and detect network and host level attacks to the best of our knowledge. The results showed that the deep learning method has recovery rate, false alarm rate, accuracy, recall F score and other true negative acceptance rates, ROC curve, and

accuracy. The DNN-based IDS model also results in traffic-sensitive accuracy of 99.40% and 98.60% that outperforms the latest IDS methods tested in the KDDCup 99 dataset and NSL-KDD dataset.

References:

[1] Shahid Latif, Zeba Idrees, Zhuo Zou, and Jawad Ahmad. Drann: A deep random neural network model for intrusion detection in industrial IoT. In 2020 International Conference on UK-China Emerging Technologies (UCET), pages 1–4. IEEE, 2020.
[2] Abdullah Alsaedi, Nour Moustafa, Zahir Tari, Abdun Mahmood, and Adnan Anwar. Ton iot telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access, 8:165130–165150, 2020.
[3] Thavavel Vaiyapuri and Adel Binbusayyis. Application of deep autoencoder as an one-class classifier for unsupervised network intrusion detection: a comparative evaluation. PeerJ Computer Science, 6:e327,
2020.
[4] Adel Binbusayyis and Thavavel Vaiyapuri. Identifying and benchmarking key features for cyber intrusion detection: an ensemble approach. IEEE Access, 7:106495–106513, 2019.
[5] Adel Binbusayyis and Thavavel Vaiyapuri. Comprehensive analysis and recommendation of feature evaluation measures for intrusion detection. Heliyon, 6(7):e04262, 2020.
[6] Thavavel Vaiyapuri. Deep learning enabled autoencoder architecture for collaborative filtering recommendation in iot environment. CMCComputers, Materials & Continua, 68(2):487–503, 2021.
[7] Adel Binbusayyis and Thavavel Vaiyapuri. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class svm. Applied Intelligence, pages 1–15, 2021.
[8] Thavavel Vaiyapuri, Adel Binbusayyis, and Vijayakumar Varadarajan. Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. International Journal of Advanced Computer Science and Applications, 12(2):731–737, 2021.
[9] Peter Christiansen, Lars N Nielsen, Kim A Steen, Rasmus N Jørgensen, and Henrik Karstoft. Deepanomaly: Combining background subtraction and deep learning for detecting obstacles and anomalies in an agricultural field. Sensors, 16(11):1904, 2016.
[10] Min-Joo Kang and Je-Won Kang. Intrusion detection system using deep neural network for in-vehicle network security. PloS one, 11(6):e0155781, 2016.
[11] Samyak Jain and K Chandrasekaran. Industrial automation using internet of things. In Security and Privacy Issues in Sensor Networks and IoT, pages 28–64. IGI Global, 2020.
[12] Bambang Susilo and Riri Fitri Sari. Intrusion detection in iot networks using deep learning algorithm. Information, 11(5):279, 2020.
[13] Qasem Abu Al-Haija and Saleh Zein-Sabatto. An efficient deeplearning based detection and classification system for cyber-attacks in iot communication networks. Electronics, 9(12):2152, 2020.
[14] S Manimurugan, Saad Al-Mutairi, Majed Mohammed Aborokbah, Naveen Chilamkurti, Subramaniam Ganesan, and Rizwan Patan. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access, 8:77396–77404, 2020.
[15] Bandar Alotaibi and Munif Alotaibi. A stacked deep learning approach for iot cyberattack detection. Journal of Sensors, 2020, 2020.
[16] Wei Liang, Kuan-Ching Li, Jing Long, Xiaoyan Kui, and Albert Y Zomaya. An industrial network intrusion detection algorithm based on multifeature data clustering optimization model. IEEE Transactions on Industrial Informatics, 16(3):2063–2071, 2019.
[17] Chi-Ho Tsang and Sam Kwong. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In 2005 IEEE international conference on industrial technology, pages 51–56. IEEE, 2005.
[18] Chenglu Jin, Saeed Valizadeh, and Marten van Dijk. Snapshotter: Lightweight intrusion detection and prevention system for industrial control systems. In 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pages 824–829. IEEE, 2018.
[19] Ismail Butun, Magnus Almgren, Vincenzo Gulisano, and Marina Papatriantafilou. Intrusion detection in industrial networks via data streaming. In Industrial IoT, pages 213–238. Springer, 2020.
[20] Kai Yang, Qiang Li, Xiaodong Lin, Xin Chen, and Limin Sun. ifinger: Intrusion detection in industrial control systems via register-base

fingerprinting. IEEE Journal on Selected Areas in Communications, 38(5):955–967, 2020.
[21] Marjia Akter, Gowrab Das Dip, Moumita Sharmin Mira, Md Abdul Hamid, and MF Mridha. Construing attacks of internet of things (iot) and a prehensile intrusion detection system for anomaly detection using deep learning approach. In International Conference on Innovative Computing and Communications, pages 427–438. Springer, 2020.
[22] Mengmeng Ge, Naeem Firdous Syed, Xiping Fu, Zubair Baig, and Antonio Robles-Kelly. Toward a deep learning-driven intrusion detection approach for internet of things. Computer Networks, page 107784, 2021.
[23] Mahdis Saharkhizan, Amin Azmoodeh, Ali Dehghantanha, Kim- Kwang Raymond Choo, and Reza M Parizi. An ensemble of deep recurrent neural networks for detecting iot cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9):8852–8859, 2020.