ANNIDS: ARTIFICIAL NEURAL NETWORK BASED INTRUSION DETECTION SYSTEM FOR INTERNET OF THINGS

Mohini Prasad Mishra[1] Rupali Layak[2]
[1] *Computer Science & Engineering, Gandhi Engineering College(GEC, Bhubaneswar), India*
[2] *Electronics & Communication Engineering, Gandhi Engineering College(GEC, Bhubaneswar), India*

Abstract*: *Internet of Things (IoT) makes everything in the real world to get connected. The resource constrained characteristics and the different types of technology and protocols tend to the IoT be more vulnerable than the conventional networks. Intrusion Detection System (IDS) is a tool which monitors analyzes and detects the abnormalities in the network activities. Machine Learning techniques are implemented with the Intrusion detection systems to enhance the performance of IDS. Various studies on IoT reveals that Artificial Neural Network (ANN) provides better accuracy and detection rate than other approaches. In this paper, an Artificial Neural Network based IDS (ANNIDS) technique based on Multilayer Perceptron (MLP) is proposed to detect the attacks initiated by the Destination Oriented Direct Acyclic Graph Information Solicitation (DIS) attack and Version attack in IoT environment. Contiki O.S/Cooja Simulator 3.0 is used for the IoT simulation.

Keywords: Artificial Neural Network, IDS, IoT, Multilayer Perceptron

I. INTRODUCTION

The Internet of Things (IoT) paves way to connect large volume of real world objects to the global network. These objects communicate with other objects using their unique identifiers to perform certain tasks and for data transmission. The Low power and Lossy Networks (LLN) are deployed in large-scale to meet the high demand of this technology. Different technologies, protocols and standards used in IoT and the tremendous growth of IoT devices in the global network bring additional vulnerabilities to the IoT networks
[1]. On account of the resource constrained characteristics of the IoT nodes, the conventional authentication and cryptography security mechanisms are not desirable to the IoT networks. Hence, it is mandatory to provide additional security mechanism like IDS to protect the IoT network from security threats and vulnerabilities [2].

IDS can be software/hardware or the combination of both which is used to investigate the malicious traffic in the network or a particular node. If there is any attack, the IDS monitors, detects and alerts the administrator and logs the attacks for analysis [3]. Intrusion Detection System automates the process of monitoring and detecting and alerting the administrators to take necessary actions to prevent the destructive impacts of the attacks [4].

According to Jyothi et al., physical attacks are initiated on the hardware of the system, network attacks are performed on IoT network elements and Software attacks are performed by using software like malware, virus, spyware and worms [5]. Based on the security vulnerabilities targeting on network resources, network topology and network traffic Anthea et al., proposed the taxonomy of RPL attacks. Because of the fake control messages and building of loops in the Destination Oriented Direct Acyclic Graphs (DODAGs), the attacks reduce the lifetime of the RPL network [6].

DIS (DODAG Information Solicitation) attack and Version attacks are the two RPL attacks considered in this work. To get the topology related information, a new node sends DIS message to its neighbors before it becomes the member of the network. In DIS attack, the malicious node resets the DIO timer frequently and sends DIS messages to the nodes within one-hop distance. This reduces the throughput and leads the energy of the nodes also to be exhausted. The DIS attacker sends unicast, broadcast or multicast DIS messages to its neighbors. Thus, it increases the control overhead in the network traffic.

Each DODAG tree has its own version number. It will be reconstructed when a new version number greater than the current one is published. Version number attack will occur by reconstructing the DODAG tree frequently using higher version. The nodes start the process of constructing a new DODAG when they receive the higher version number which leads to inconsistency in the network topology [7]. The inconsistencies in the networks also upturn the possibilities of generating loops and rank inconsistencies in the network. When the attacker node communicating with other attackers, DIS attack and Version attack will lead RPL network to other types of attacks and which will collapse the entire network.

Machine Learning Algorithms are used to enhance the detection accuracy of the IDS. Artificial Neural Network (ANN) provides better detection accuracy rate in terms of true and false alarm rates [8]. In neural network, the weight, the associated bias and the number of epochs given for the training phase will determine the accuracy of the classification. Multilayer Perceptron (MLP) type of Neural Network is used for off-line analysis of data and also useful for intrusion detection [9].

In this paper, an Artificial Neural Network based IDS using MLP concept is suggested to detect the RPL attacks such as DIS attack and Version attack. The section 2 elucidates the basic concepts of Artificial Neural Networks and MLP. Section 3 explains
some related works in this research. Section 4 proposes the ANN based IDS for IoT.

Section 5 explains the results obtained by the proposed model. Finally, conclusion is given in the section 6 and this section also opens new perspectives related to this research.

II. ARTIFICIAL NEURAL NETWORKS

A set of processing units also called as neurons are interconnected according to the specified topology is termed as an Artificial Neural Network (ANN). It has the ability to learn by example and generalizes from limited, noisy and incomplete data. ANN has been successfully employed in a broad spectrum of data-intensive applications [10-11]. The neural network consists of an input layer, number of hidden layers and an output layer. Each layer has number of neurons. The information enters the neural network via the input layer, it is processed in the hidden layers and the result can be retrieved in the output layer. A typical neural network model with a hidden layer is shown in Fig.1.

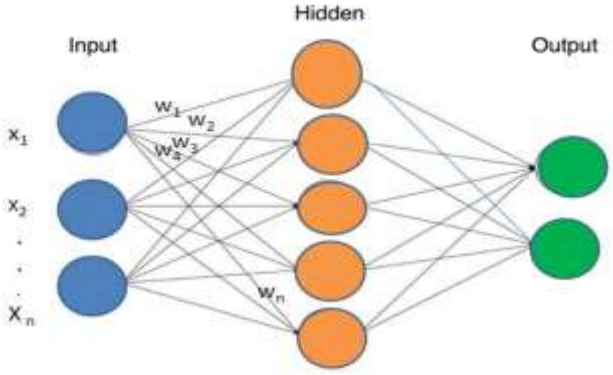

Fig.1. Neural Network Model

There are 'n' numbers of inputs available for a single neuron in this network and each input is associated with a weight on it. 'x_0' is the bias value which is added to the input of the activation function. Let x_1, x_2, x_3, ……..x_n are the inputs to a neuron and let w_1, w_2, w_3, …….w_n are weights, let 'b' is the bias and then 'a' is the out of the neuron which is calculated using the equation (1).

$$a = f(\sum_{i=0}^{n} \text{wixi} + \text{b}) \qquad (1)$$

where, f is the activation function which is used to get the output of that layer and feed it as an input to the next layer [12]. Artificial Neural Network is made up of nodes and corresponding weights which typically require learning based on the given patterns. Some examples of learning patterns include supervised learning and unsupervised learning. In supervised learning, the output has been labelled and so the network has a known expected answer. The Back-propagation algorithm and Multilayer Perceptron (MLP) belong to this category [13]. In unsupervised learning, the neural network analyses the input patterns and extract the features based on the characteristics of the given input. The Self-Organizing Map is an example of this unsupervised learning [14].

Multilayer Perceptron

Multilayer Perceptron is the widely used neural network model. It is based on supervised learning technique which uses the historical data as input to generate a labeled output. In Multilayer Perceptron, a set of input and its corresponding output are trained to learn the relationship between those input and the output. In the training phase, the parameters like weights and biases are adjusted, so that the error is minimized. This trained MLP model is used in the testing phase to classify the test dataset.

MLP is a feed forward neural network which involves forward and backward pass. The signal flow moves through the hidden layer from the input layer to the output layer. The result of the output layer is measured against the labels and the error is calculated. In order to minimize the error, the weights and bias are adjusted in the backward pass. The error is minimized in all iteration and finally it will be closer to the approximate output. Determining the optimal number of hidden layers and the hidden units in each layer is also challenging issue. It is difficult to determine the optimal hidden units than the hidden layer. Based on empirical method, the optimum number of hidden units suitable for the MLP can be assigned [15].

III. RELATED WORKS

Petteri et al. [16] performed a study on the requirement analysis of a benchmark dataset for Network and Host Intrusions Detection System (NHIDS). The requirements were finalized based on the dataset features, overall composition, and systems used to produce the datasets. Nine datasets starting from the traditional KDD CUP'99 dataset to UNSW-NB15 were reviewed.

The coexistence of both Host-based and Network-based entities was rare in a single dataset. According to this study, the real-world network environment is difficult to replicate using the test-bed datasets.

Kelton et al. [17] reviewed various machine learning techniques suitable for intrusion detection in IoT environment. The recent research works related to IoT security were analysed with a special concern on the Intrusion Detection Systems using machine learning approaches. In this review the protocols, intelligent techniques like machine learning techniques and precision obtained in the recent works were highlighted. Finally, the research challenges and future directions for IoT security were also emphasised.

Ganesh et al. [18] proposed an approach for ANN based Intrusion Detection System with less number of features. Important features from KDD Cup'99 dataset were selected by using Mutual Information based feature selection method. The performance of Mutual Information with ANN was compared with Support Vector with ANN and Mutation Information approach outperformed without any false positive and less negative rates. Though there are many advantages in this method, it requires more computation in terms of number epochs to obtain the accuracy.

Mohammad et al. [19] assessed the challenges of IoT security by considering various machine learning techniques in smart cities. Taxonomy of machine learning algorithms and the issues and challenges
regarding the data analytics of machine learning algorithms were also discussed. They suggested
some machine learning algorithms like ANN that are useful for the IoT security and fraud detection.

Alex et al. [20] suggested that the IDS to analyze the data packets and to detect malicious shell code. In their work, integer values were obtained by converting the byte level data retrieved from the data transmission of the nodes and fed into the ANN. Their best classifier identified 100% of malicious file contents in the test set. This ANN model is useful for detecting the script attack and SQL injection.

IV. PROPOSED ANNIDS MODEL FOR IOT

Multilayer Perceptron (MLP) is applied in the research work for detecting the attacks in IoT environment. The DIS attack and Version attack are simulated and the raw datasets are pre-processed to make them ready for detection process. The proposed ANN based IDS model for IoT environment is depicted in Fig.2. It has three phases such as simulation phase, pre-processing phase and ANNIDS model phase.

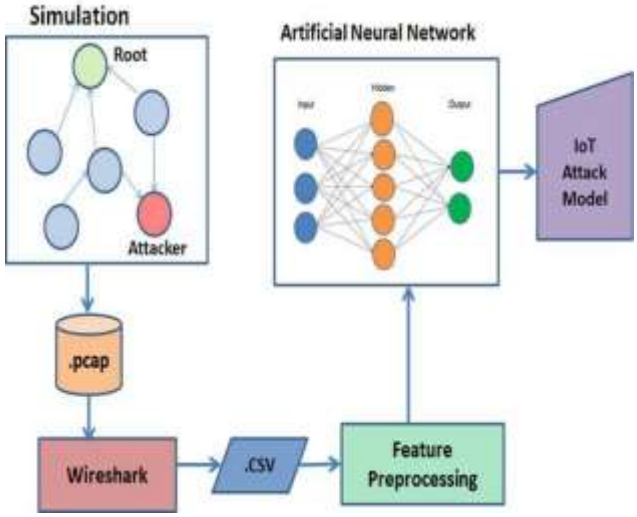

Fig.2. ANNIDS Methodology Diagram

1) **Simulation Phase:** In the simulation phase, the open source Contiki/Cooja simulator is used to generate the data packet details equivalent to the real-time data packets. At first, the packet capture file (.pcap) generated by the Cooja simulator is transformed into the CSV file format for further processing.
2) **Pre-processing Phase:** In this phase, the CSV files will undergo the pre-processing stages like feature extraction and normalization. After this step, the dataset will be ready for the ANNIDS phase.
3) **ANNIDS Phase:** In this phase, the pre-processed datasets are produced which consists of a mixture of normal packets and attack data packets. Then the dataset are fed into Artificial Neural Network system. The input,
weight and bias values are adjusted and the IoT Attack Detection Model based on MLP is created.

The flowchart in Fig.3 explains the overall functionality of the proposed technique.

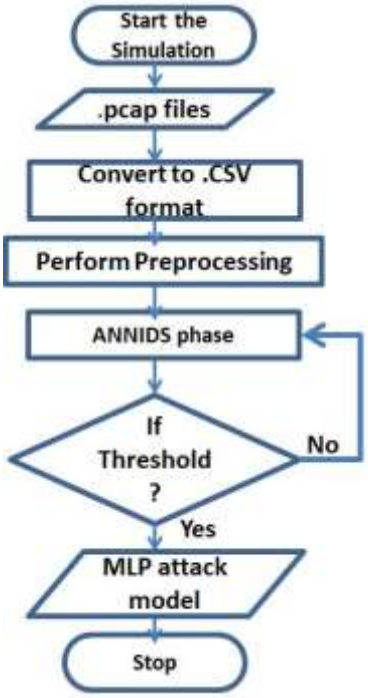

Fig.3. Flowchart for ANNIDS

IoT devices are resource constrained, so that in the proposed work minimum burden is given to the IoT network. The packet traces are only taken from IoT simulated environment. The proposed pseudo code for the ANNIDS technique is given as follows:

Procedure ANNIDS

Input: IoT Simulation Dataset
Output: MLP Model for detecting Attacks

Step 1: Start
Step 2: Perform Simulation with server node, normal nodes and attacker nodes
Step 3: Capture the .pcap file of the simulation using 6LoWPAN packet analyzer
Step 4: Open the .pcap files in Wireshark
Step 5: Import the .pcap file into .csv
Step 6: Perform pre-processing
Step 7: Use Resampling technique to get training and test set
Step 8: Use ANN to classify the attacks and benign packets
Step 9: Generate MLP model for IoT attack
Step 10: Stop

This ANNIDS pseudo code is implemented to produce a MLP model for detecting the attacks in IoT environment.

V. RESULT AND DISCUSSION

This section shows the outcomes obtained from the ANNIDS model that is used for intrusion detection. The proposed model was implemented in Contiki O.S. Cooja Simulator 3.0. The Simulation parameters used in this research is given in the Table 1. According to the given

parameters the simulation is performed.

Table- I: The Simulation Parameters

Simulation	Cooja Simulator 3.0
Mote Type	Sky mote
Root node (node no 1)	1
Child node (node no 2-13)	12
Malicious Node (node no 14,15)	2
Radio Medium	UDGM: Distance Loss
Transmission Range	50 m
Interface Range	100 m
Mote start delay	1000 ns
Random Seed	123,456
Positioning	Random Positioning

At the beginning of the simulation, the Destination Oriented Direct Acyclic Graph (DODAG) generated by the Cooja simulator is shown in Fig.4.

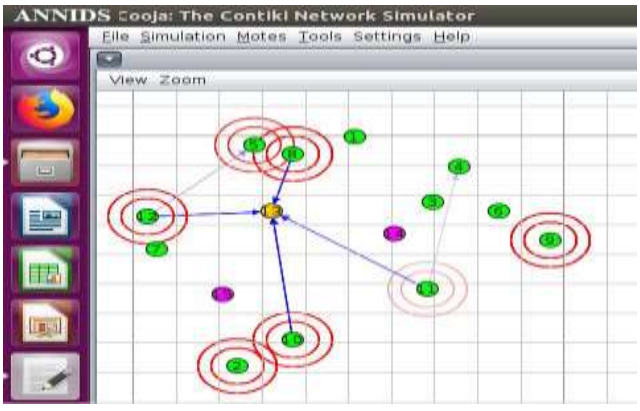

Fig.4. DODAG generated in Contiki O.S. Cooja Simulator

As it is given in the Table 1, there are 12 child nodes, one root node and two attackers used in this simulation. The mote output generated by the ANNIDS simulation environment is shown in Fig.5.

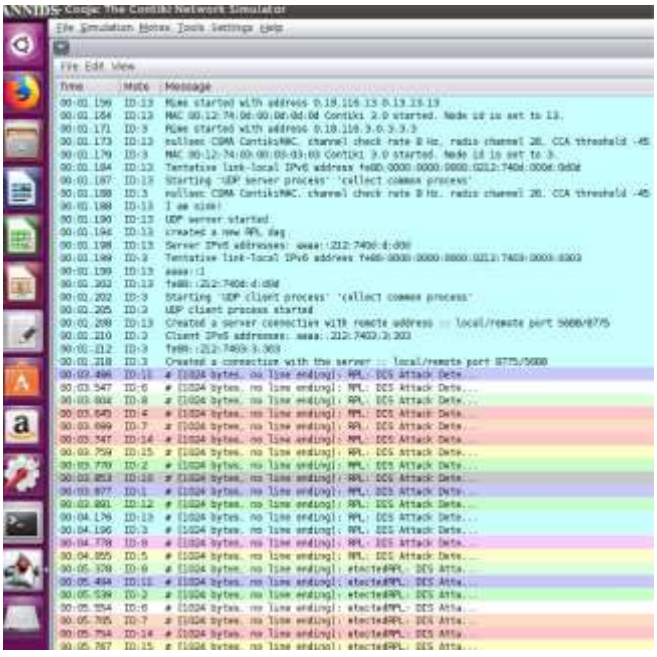

Fig.5. Mote output having attacks

In the second phase of the proposed system, the data packets generated by the Cooja simulator are captured using Wireshark tool as a .pcap file. Fig.6 shows the .pcap file captured by the simulator and also the I/O graph of this .pcap file. It contains the details of Packet_No, Time, Source_IP, destination_IP, Protocol, Length and other details about the simulated packets.

Fig.6. pcap file and I/O graph

The radio message generated by the two attacker nodes 14 and 15 are shown in the Fig.7. Next, the .pcap files are converted into .csv file for analyzing the data. Then the .csv file is fed into the Artificial Neural Network to generate the IoT Attack model.

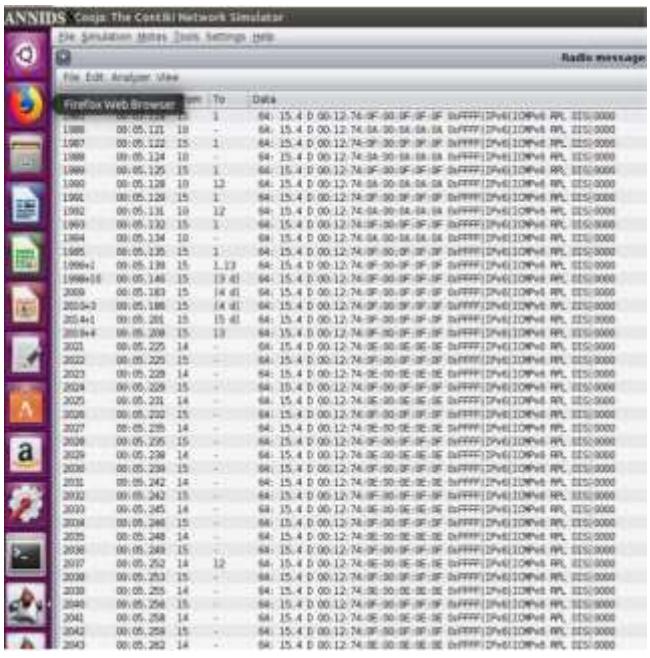

Fig.7. Radio messages Generated by the attacker nodes

Totally 73,880 data packets were captured in the IoT simulation experiment and among them attacker node 14 generated 325 malicious data packets whereas node 15 generated 982 malicious data packets.

Since MLP is a supervised Learning technique, it has training as well as testing phases. From the total dataset, 80% of data packets (59,104) are used to train the data model and 20% data packets (14,776) are used in the testing phase. The MLP model classified the data packets like attacks and normal packets according to the IPV6 source of the corresponding packets. Among the 14,776 data packets of the testing dataset, there are 260 attack packets and 14516 normal packets. The confusion matrix and other measures obtained during the testing phase are shown in the Fig.10.

VI. CONCLUSION

In this paper, an ANN based IDS is proposed to detect two RPL attacks such as DIS attack and Version attack. The simulated data is captured as a .pcap file and it is sent to the feature pre-processing phase and finally it is fed into the Multilayer Perceptron (MLP) to generate an IoT attack model. The proposed ANNIDS technique can be implemented with the Intrusion Detection System to enhance its performance. In future, instead of the simulated dataset, the real-time sensor data from smart city application can be captured and perform neural network based data analytics to detect the security attacks of the Internet of Things.

REFERENCES

[1] Bruno Bogaz Zarpaelo, Rodrigo Sanches Miani, Claudio Toshio Kawakani and Sean Carlisto de Alverenga (2017) A Survey of Intrusion Detection in Internet of Things. International Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2017. 02. 009.
[2] RaviTeja Gaddam and Nandhini (2018) An Analystical Approach to
[3] enhance the Intrusion Detection in Internet of Things Network. International Journal of Latest Trends in Engineering and Technology,
[4] Volume 9, Issue 3, pp.258-267, e-ISSN: 2278-621X, DOI:
[5] http://dx.doi.org/10.21172/1.93.43.
[6] Tariqahmad Sherasiya and Hardik (2016) Intrusion Detection for Internet of Things. International Journal of Advance Research and Innovative Ideas in Education, Volume 2, Issue 3, ISSN: 2395-4396
A. Arul Anitha (2011) Network Security using Linux Intrusion Detection System. International Journal of Research in Computer Science, 2 (1): pp. 33-38, doi:10.7815/ijorcs.21.2011.012.
[7] Jyoti Deogirikar and Amarsinh Vidhate (2017) Security Attacks in IoT: A Survey. International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC. Anthea Mayzaud, Remi Badonnel and Isabelle Chrisment (2016) A Taxonomy of Attacks in RPL-based Internet of Things. International Journal of Network Security, Volume 18, Issue 3, pp. 459-473.
[8] Divya Sharma, Ishani Mishra and Dr. Sanjay Jain (2017) A Detailed Classification of Routing Attacks against RPL in Internet of Things. International Journal of Advanced Research, Ideas and Innovations in Technology, Volume 3, Issue 1, ISSN: 2454-132X.
[9] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson (2016) Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System. International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6.
[10] Teik-Toe Teoh, Yok-Yen Nguwi, Yuval Elovici, Wai-Loong Ng and Soon-Yao Thiang (2018) Analyst Intuition Inspired Neural Network Based Cyber Security Anomaly Detection. International Journal of Innovative Computing, Information and Control, Volume 14, Issue 1, pp. 379–386.
[11] Omar Y. Al-Jarrah , Yousof Al-Hammdi, Paul D. Yoo , Sami Muhaidat and Mahmoud Al-Qutayri (2018) Semi-supervised Multi-layered Clustering Model for Intrusion Detection. Journal of Digital Communications and Networks, Volume 4, pp.277-286, DoI: https://doi.org/10.1016/j.dcan.2017.09.009.
[12] Seungwon Lee, Changbae Mun and Ook Lee (2018) A Study of Neural Network Based IoT Device Information Security System. Journal of Theoretical and applied Information Technology, Volume 96, Issue 22, ISSN: 1992-8645, E-ISSN: 1817-3195.
[13] Yuntian Chen, Haibin Chang, Jin Meng and Dongxiao Zhang (2019) Ensemble Neural Networks (ENN): A gradient-free stochastic method. Neural Network Journal, Volume 110, pp. 170-185.
[14] Dongwoo Lee , Sybil Derrible and Francisco Camara Pereira (2018) Comparison of Four Types of Artificial Neural Network and a Multinomial Logit Model for Travel Mode Choice Modeling. Journal of the Transportation Research Board, Volume 2672, Issue 49, pp. 101-112, DOI:10.1177/ 0361198118796971.
[15] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac and Parvez Faruki (2018) Network Intrusion Detection for IoT Security based on Learning Techniques. IEEE Communications Surveys and Tutorials, Volume. 00, Issue 0, DOI: 10.1109/COMST.2019.2896380.
[16] McCarthy, R. V., McCarthy, M. M., Ceccucci, W., and Halawi, L. (2019) Predictive Models Using Neural Networks. Applying Predictive Analytics,
[17] 145–173, Springer Nature Switzerland AG 2019, doi:10.1007/978-3-030-14038-0_6
[18] Petteri Nevavuori and Tero Kokkonen (2019) Requirements for Training and Evaluation Dataset of Network and Host Intrusion Detection System. Springer Nature Switzerland AG, WorldCIST'19, AISC 931, pp. 534–546, https://doi.org/10.1007/978-3-030-16184-2_51.
[19] Kelton A.P. da Costa, Joao P. Papa, Celso O. Lisboa, Roberto Munoz and
[20] Victor Hugo C. de Albuquerque (2019) Internet of Things: A Survey on Machine Learning-based Intrusion Detection Approaches. Computer
[21] Networks, PII: S1389-1286(18)30873-9, DOI:
[22] https://doi.org/,10.1016/j.comnet.2019.01.023.
[23] P. Ganesh Kumar and D. Devaraj (2010) Intrusion Detection using Artificial Neural Network with Reduced Input Features. ICTACT Journal on Soft Computing, Volume 1, Issue 1, ISSN 2229-6956(Online), DOI: 10.21917/ijsc.2010.0005.

[24] Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi and Amit P. Sheth (2018) Machine Learning for Internet of Things Data Analysis: A Survey. Journal of Digital Communication and Networks, Volume 4,
[25] pp.161-175, DOI:10.1109/COMST.2019. 2896380, IEEE: https://doi.org/10.1016 /j.dcan. 2017.10.002.
[26] Alex Shenfield, David Day and Aladdin Ayesh (2018) Intelligent Intrusion Detection Systems using Artificial Neural Networks. ICT Express, Volume 4, pp.95-99, DOI: https://doi.org/10.1016/ j.icte.2018.04.003.