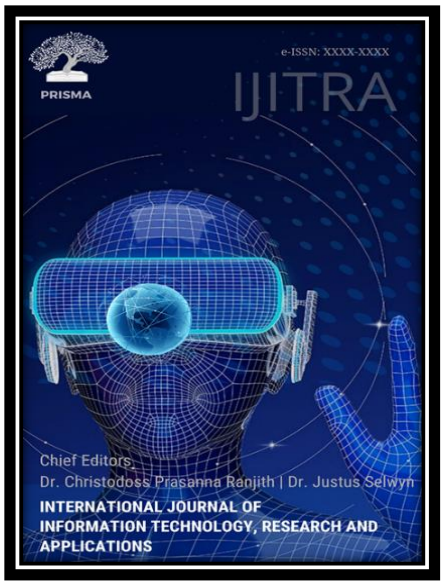

International Journal of Information Technology, Research and Applications (IJITRA)

Ammar Khamis Al-Muzaini, Maha Abdullah Al-Dhuhli, Miysaa Salim Al-Braiki and Rajesh Natarajan (2023). Intrusion Detection System to Advance IoT Security Environment, 2(2), 10-17.

ISSN: 2583 5343

DOI: 10.59461/ijitra.v2i2.48

The online version of this article can be found at:
https://www.ijitra.com/index.php/ijitra/issue/archive

Published by:
PRISMA Publications

International Journal of Information Technology, Research and Applications (IJITRA) is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.

PRISMA
PUBLICATIONS

https://www.prismapublications.com/

Intrusion Detection System to Advance IoT Security Environment

[1]Ammar Khamis Al-Muzaini, [2]Maha Abdullah Al-Dhuhli, [3]Miysaa Salim Al-Braiki, [4]Rajesh Natarajan

[1] Bachelor – Network Computing Specialization
Information Technology Department
Shinas College of Technology
[1] 66J17334@shct.edu.om, [2]66S1863@shct.edu.om, [3]66J18118@shct.edu.om
[4]rajesh.natarajan@shct.edu.om

Article Info

Article history:

Received: Dec 21, 2022
Accepted: Feb 07, 2023
Published: June 22, 2023

Keywords:

Attack Detection
Security
Threats Reporting
Signature Matching
Protection System

ABSTRACT

Nowadays, with the technological improvement, communications with the things become easier. It helps people to live an easier life, live and work smarter as well as take back control of their lives completely. this smart communication is done in an environment that called Internet of Things (IoT) environment. The Internet of Thing is multiple physical objects that communicate using the internet, allowing sending, and receiving of data. Since it's a data so it's prone to attack in a goal of steal it, change it and so many reasons. In addition, nowadays hackers are everywhere with so many types. So, it needs to protect those data and the devices, if Internet of Things devices doesn't have enough security to protect the system from being compromised, then many threats and attacks will occur. If the administrator does not apply strong security and develop a plan for system and device prevention, the Internet of Things environment will be weak, which will make the system and devices prone to attack. Unauthorized access will be prevented if the login system includes a signature matching system. This research aims to analyze the traffic security and analyze threats and risks using IoT devices from intruders by applying an IDS to the IoT environment. when the attacker will try to enter to the traffic or send any packets to any IoT devices, the intrusion detection system will send an alert to the administrator that there's something wrong need to check, the IDS will detect the attacker's name, type and from which device he tries to enter to the system, it will analyze the traffic system, as well as will prevent the devices and data from threats.

Corresponding Author:

Rajesh Natarajan
Information Technology Department
Shinas College of Technology
rajesh.natarajan@shct.edu.om

1. Introduction

We did not realize as human beings that the devices around us can communicate with us and communicate with them this is called the Internet of Things (IoT). The Internet of Thing is multiple physical objects that communicate using the internet, allowing sending, and receiving of data. Nowadays, with the technology improvement, hacking become very easy for those people who have a good knowledge about hacking and who are interested on it, so that they can even enter to any device without the owner can know. But for sure, there are advance security software's, hardware's, and ways to get rid of those hackers and prevent the device from any internal or external threat and unauthorized external intrusions likely to happen. As any devices in this world, Internet of Things devices is also expected to prone to attack while any actions possible to be happen, such as varies types of hackers, attackers can infiltrate data to the cloud and threaten to keep, erase it, modify, or make the data public in purpose of have fun, personal gain like steal bank information or transfer a fund to their bank account, or in aim of revenge when have a personal grudge against someone in the organization .The Internet of Things has been deployed in intelligent environments such

as smart cities and smart homes. The goal of developing such environments is to make human life more productive and comfortable by solving challenges related to living environment, energy consumption and industrial needs. Scientists, manufacturers, transport owners and security officers in organizations are the most people who are interested in this. This objective is reflected in a significant growth in services and applications related to the Internet of Things. Most of the developed countries, especially European countries, use Internet of Things in their daily life and this makes their life easier. Most countries know about this Internet of Things and how much security it needs, but they have not been able to solve it 100 percent till now. On the other hand, some countries still don't know that securing these Internet of Things devices requires much effort, so they just do a little bit of stuff to secure the Internet of Things devices. Smart environments are made up of sensors that work together to perform operations. Wireless sensors and wireless technologies contribute to the expansion of intelligent environments. These environments range from smart cities and smart homes to smart healthcare and smart services. It makes the integration of Internet of Things systems more efficient. However, Internet of Things systems are vulnerable to various security attacks. With the large number of Internet users, numerous attempts to penetrate, and unauthorized persons entering some networks and Internet of Things devices, the hacker must find a loophole to enter the network. In current studies, the security is not securing 100 percent; there are a few things that have not been completed yet, such as a strong algorithm, or they just apply the normal security plan. Internet of Things developers are trying to update these devices constantly to avoid such hacks. What is new in this research is that we will make an IDS system to combat attacks and avoid unauthorized access to it, and we will work to reduce security holes to make the Internet of Things more secure. The security vulnerabilities in IoT-based systems create security threats that affect smart environment applications. Thus, there is a crucial need for intrusion detection systems (IDSs) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities [1].

2. Literature Review

Literature review helps to facilitate the process of searching of our topic and to facilitate find methods, algorithms and techniques that can be used on it, and to understand the basic information. Also, to gain more information that help to write the research.

The CNN, LSTM and combined CNN-LSTM algorithms [2] is used but although it achieves a good controlling of the traffic, but it still has some limitations like not able to detect all the types of the attacks. Temporal Convolution Neural Network and Efficient Feature Engineering methods [3] are used, it depended on built layers, but she faced some limitations in storage and applying a good performance efficiency. Reptile Search Algorithm [4] is used, it works well, and it achieves the second rank, but it has a limit in being time-consuming resulting from learning the model. Convolutional Neural Networks decision regression for an intrusion detection method as a special framework [5] is used, it detects only Man in the Middle Attack and DoS attack but no other threats. Network flow generator technique and deep packet inspection method [6] is used, both are related only to the IP address and MAC address if someone tries to break or block but it will not send an alert to the administration. trust integrated RPL protocol (TRPL) technique in IDS [7] is used, it successes in detecting black whole attack from the network in the IoT but it went with limitation in storage and computing capabilities. state-of-the-art algorithm [8] is used, it is related only to the hardware, but it has limitations like if the hardware fails down the administrator will not know. 5G Network Using Deep Learning is used [9], it achieves a good result in distinguishing between outside and inside attacks, but it limits and rely on the speed of the interne, if its slow, then no such efficiency in the performance. Autoencoder deep learning is used by [10], it detects anomaly attacks, but it has a limitation in the efficacy and low performance. AIS (Artificial Immune System) method is used [11], it detects the new signature, it has a limitation in using powerful hardware. machine learning methods, and pattern recognition algorithms is used [12], it helps to preprocessing and detect malware attacks, its limitation in resources and performance efficiency. Attack detection methods with deep learning [13], which could automatically detect unauthorized, but it has a limitation in model complexity. ML-based IDS [14], Distinguishes between malicious and normal network traffic, distinguishes behaviors, and audits host logs, but has limitation in cannot detect the attack at the first time. Machine learning (ML) used [15], incoming traffic flow is captured, but has limitation in not able to identify new attacks in multiple attack scenarios. Machine learning algorithms used [16], used to find anomalies in systems running on IoT networks, but it has some limitations like limited resources and limitation in energy and processing capacity. multi-layered security method [17], helps to monitor the IoT network to recognize the activities done by normal or malware user, it has limitation in processing power and only used for small size of data. A stacked sparse autoencoder network model [18] is presented for detecting purposes, but it has a limit constraint on the middle layer's sparsity. A hybrid placement method to intrusion detection [19] that makes use of a multi-agent platform, blockchain, using deep learning methods, it has a

limitation in the design complexity. A hybrid convolutional neural network model used by Smys [20], it can identify several types of attacks, but has some limitation only allowing visibility for one host. unsupervised techniques [21], handles the network data and does out anomaly detection using an ensemble of autoencoders, but it is not deal with all types of the attacks.

3. Research Methods

3.1 Research Objectives

This research aims to analyze the traffic security and analyze threats and risks using IoT devices from intruders.

3.2 Research Method

The research was depending on mixed approach. The quantitative side is for the calculation of the data stream and data flow measurements. Qualitative approaches are for descriptive purpose, evaluating and understanding of different aspects of the problem. We used secondary data to gather data that is related to IoT security in IoT environment. The data information is related to the dataset named BoTNeTIoT-L01 [26], Research results is an experimental research data results of the proposed system to developed IoT security environment using intrusion detection systems. The developed IoT security approach is evaluated, and the evaluation process is evaluated, using a variety of evaluation metrics, including security, data accuracy, correct percentages, good performance.

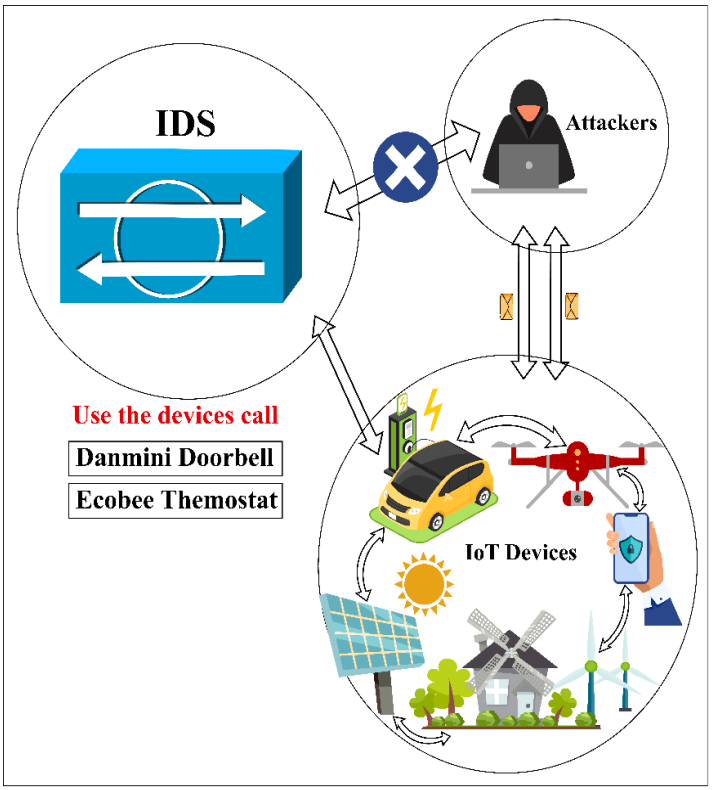

Figure 3.1 - IDS working for IoT environment

Attackers are trying to access the data in IoT devices for several reasons, including changing them or trying to steal them, but IDS senses that there is a threat or attack in it, so it will hunt it down using devices called the Danmini doorbell and the Ecobee thermostat and an intrusion detections system work in the following way: IDS have sensors to detect signature and some advance Intrusion detection systems have behavioral activity detections to determine malicious activity in the network. Even if the signature doesn't match this activity, IDS still can alert the administrator about the possible attack. If the signature matches, then it moves to the next step or the connections are cut down from that IP source, the packet is dropped, and the alarm notifies the admin. Once the signature is matched, then sensor pass on anomaly detection, whether

the received packet or request matches or not. If the packet passes the anomaly stage, then state full protocol analysis is done. After that the packets are passed through switch to the network. If anything mismatches again, the connection is cut down from that IP source, the packet is dropped, and the alarm notifies the admin.

3.3 Research Instrument

We gathered the data information from articles and related dataset. **The dataset name is** BoTNeTIoT-L01 [27], it is a data set embedded in all IoT device data files. It covers new version that reduced the redundancy of the original data set in just by selecting features from a time window of 10 seconds. In the name of the label class, 0 stands for attack and 1 for normal tests-user. It has the most recent data information, traffic from nine IoT devices being tracked by Wireshark on a local network via a central switch. There are two Botnet attack in it called (Mirai and Gafgyt) by two devices called Danmini Doorbell and Ecobee Thermostat. The data set contains 23 statistically designed features extracted from the p-cap files. Sex statistical measures (weight, mean, variance, standard, COV, magnitude) were calculated during the 10-second time window with a decay factor of 0.1 with the additional three categories called (device name, attack type, attack subtype). There's a possibility to get a good data accuracy and correct percentages in a table and graph. We choose this method because it is the most appropriate and best way to gain the data information needed that we could find accurately and be correct will be through the experiments results. The results of the experiment were accurate with correct percentage, it shows that there's increases in detecting the precision, there's an improvement of recall and improve F-Score correlation among data values.

3.4 Sampling Design

The sampling technique that used is probability statically sample approach. Its classification method to identify if there's an attack or not, based on independent variable which is call label, 0 stands for attack and one is stands for normal user. For testing the problem it's considers as a random testing. The system which chooses from collecting data about 1000, the sample data is 30% of the actual data that will uses to predict if there's an attacker or not by two devices that is called Danmini Doorbell and Ecobee Thermostat and which type of the attack and its sub-type.

3.5 Data Analysis Plan

Planning to do data accuracy, correct percentages, good performance and analyze the traffic security about the data quantitate and qualitative which is in the experimental results and analyze it to achieve the research objective and prove the hypotheses.

4. Result and Analysis

No	name of the dataset	duration (hrs)	packets	flows	Pcap Size	Name	mean
1	CTU-IoT-Malware-Capture	23	233,000	23,146	121 MB	Mirai	85389.66667
2	CTU-IoT-Malware-Capture	1	82,000,000	67,321,810	6 GB	Mirai	49773937
3	CTU-IoT-Malware-Capture	2	1,309,000	238	1.7 GB	Mirai	436413.3333
4	CTU-IoT-Malware-Capture	8	18,000,000	5,410,562	1.3 GB	Mirai	7803523.333
5	CTU-IoT-Malware-Capture	24	64,000,000	19,781,379	4.6 GB	Mirai	27927134.33
6	CTU-IoT-Malware-Capture	24	50,000	3,210	3.9 MB	torii	17744.66667
7	CTU-IoT-Malware-Capture	24	50,000	3,287	3.9 MB	torii	17770.33333
8	CTU-IoT-Malware-Capture	8	24,000	4,427	2.8 MB	trajon	9478.333333
9	CTU-IoT-Malware-Capture	24	271,000,000	3,851,029	21 GB	Gagfyt	91617017.67
10	CTU-IoT-Malware-Capture	24	109,000,000	54,659,864	7.8 GB	kenjiro	54553296
11	CTU-IoT-Malware-Capture	24	13,000,000	13,654,107	992 MB	okiru	8884710.333
12	CTU-IoT-Malware-Capture	24	54,000,000	54,454,592	3.9 GM	kenjiro	36151538.67
13	CTU-IoT-Malware-Capture	24	23,000	10,404	2.1 MB	hakai	11142.66667
14	CTU-IoT-Malware-Capture	24	46,000,000	10,447,697	3.6 G	Mirai	18815907
15	CTU-IoT-Malware-Capture	24	13,000,000	3,394,347	1.2 GB	Mirai	5464790.333
16	CTU-IoT-Malware-Capture	7	73,000,000	73,568,982	5.3 GB	IRCBot	48856329.67
17	CTU-IoT-Malware-Capture	24	11,000,000	11,454,723	897 MB	linux,Mirai	7484915.667
18	CTU-IoT-Malware-Capture	24	6,437,000	6,378,294	472 MB	linux.hajme	4271772.667
19	CTU-IoT-Malware-Capture	36	497,000	156,104	56 MB	Muhstic	217713.3333
20	CTU-IoT-Malware-Capture	112	1,686,000	1,008,749	140 MB	Hide and Seek	898287

Table 4.1: [28] Data Collected.

packets	
40138052.63	Mean
14977493.23	Standard Error
13000000	Median
50000	Mode
65285379.4	Standard Deviation
4.26218E+15	Sample Variance
8.768080559	Kurtosis
2.722346394	Skewness
270977000	Range
23000	Minimum
271000000	Maximum
762623000	Sum
19	Count

Table 4.2: Features of data collected Depends on Packets.

protocol	Parquet's	size	percentages (%)
1. ICMPv6	40 500 000	76	40.5
2. 6LoWPAN	25 000 000	79	25
3. CoAP	6 900 000	29	6.9
4. UDP	4 900 000	8	4.9
5. IEEE 802.15.4	2 000 000	100	2
6. IPv6	20 700 000	40	20.7

Table 4.3: [29] Protocol Distributions.

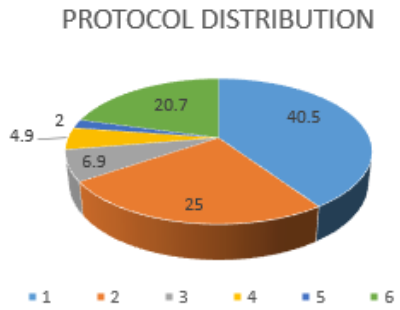

Figure 4.1: Protocol Distributions.

Frequency	*packets*
5	23000
1	24000
0	50000
0	50000
1	233000
0	497000
1	1309000
0	1686000
4	6437000
1	11000000
1	13000000
0	13000000
1	18000000
1	46000000
0	54000000
2	64000000
1	73000000
1	82000000
0	109000000
0	271000000
0	More

Table 4.4: frequency of Packets.

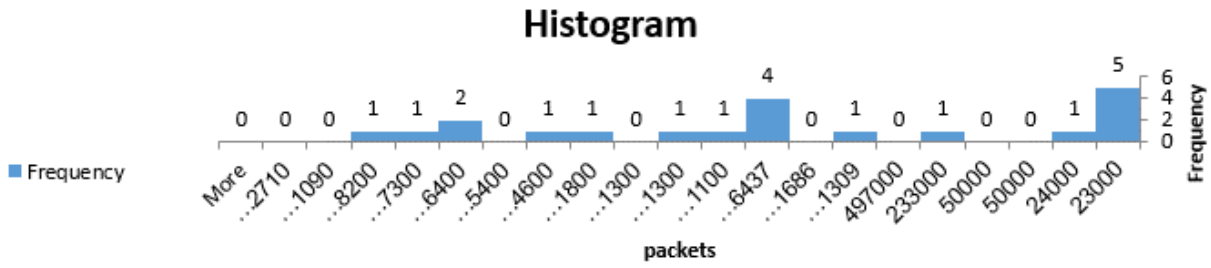

Figure 4.3: frequency of Packets.

The data clearly shows a summary of twenty malicious data in table 4.1. The first column shows the scenario number ID, dataset name, duration in hours, number of packets, the number of Zeek IDs flows in the log file (obtained by running Zeek network analysis framework on the original PCAP file), PCAP is packet captured file contains a network's packet data and are used to examine the network's properties, the size of the original PCAP file and the a potential name for the malware sample that was utilized to attack the system. Malware captures run continuously for a long time. So it rotated the PCAPs files every 24 hours due to the quantity of the traffic each infection generates. But occasionally, the PCAP file was expanding too quickly, so it chose to halt the capture before the twenty-four hours had passed. Because of this, the number of hours in certain grabs varies. The various nodes of the network communicate with one another using wireless communication protocols such IPV6, ICMPV6, 6LoWPAN, IEEE 802.15.4, CoAP, and UDP. The distributions of different protocols in display in table 4.3. The (6LoWPAN, IPv6) protocols is for network, transport (UDP), and application (CoAP).

5. Summary, Conclusion and Recommendation

The IoT environment is always vulnerable to attackers because it contains the important data, and with the technological development it has become easy for any attacker or any person to enter the data and change it, steal it, or fix things in it. The results showed that many attacks occurred over the days, they were trying to attack the IoT environment and steal data, some of them succeeded in logging in and spent hours and days in the system, but some of them failed because of their tools. It was a little bad in terms of getting into the system. The IoT environment should be high security and a strong firewall to secure data, the data must be protected and should not be as data leakage. In addition, there's so many ways to protect the data as well as the IoT environment itself, one of these ways is intrusion detection system that can protect from any internal or external attackers, capable with many technologies as features. The results and analyzes showed, icmpv6 is the most protocol captured the data by 40.5%, shows that the most duplicated attacker name is Mirai, while less attackers name presented is trajon, Gagfyt, okiru, hakai, IRCBot, Muhstic and Hide and Seek. It seems that the Mirai attacker is less security for the IoT environment and others is less presented attacker is more secured for IoT environment. Hide and Seek attacker toke the longest duration inside IoT system that is 112 hours. IoT networks are at great risk, and attackers can enter and take some data or modify it for easy access. There are many hackers who try to breach people's privacy and sell it later or blackmail the person. All of these factors can have an impact on the data from the IoT device system. This problem has been going on for a long time and is getting worse day by day, and security threats and problems are increasing due to the development of technology. In addition, there's a data leakage (information leakage) that shows a data or information that is transferred without authorization from within a company to a location outside its guarded network. Our recommendation to solve this problem is that intrusion detection systems that meet the security requirements of smart environments based on the Internet of Things can be used to enhance the security of the Internet of Things to protect and secure devices from hacking without negatively affecting their safety and confidentiality, and modern technologies such as deep learning, 5G, and many others can be used. Other techniques for monitoring security risks before or as they occur.

References:

[1]. Elrawy, M., Awad, A., & Hamed, H. (2020). Intrusion detection systems for IoT-based smart environments: a survey. *Journal Of Cloud Computing*, *7*(1). https://doi.org/10.1186/s13677-018-0123-6

[2]. Alkahtani, H., & Aldhyani, T. H. (2021). Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. *Complexity*, *2021*, 1–18. https://doi.org/10.1155/2021/5579851

[3]. Derhab, A., Aldweesh, A., Emam, A. Z., & Khan, F. A. (2020). Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. Wireless Communications and Mobile Computing, 2020, 1–16. https://doi.org/10.1155/2020/6689134

[4]. Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-qaness, M. A., & Forestiero, A. (2022). Intrusion detection system for IOT based on Deep Learning and modified reptile search algorithm. *Computational Intelligence and Neuroscience*, *2022*, 1–15. https://doi.org/10.1155/2022/6473507

[5]. Akhtar, M. S., & Feng, T. (2021). Deep learning-based framework for the detection of cyberattack using feature engineering. Security and Communication Networks, 2021, 1–12. https://doi.org/10.1155/2021/6129210

[6]. Dat-Thinh, N., Xuan-Ninh, H., & Kim-Hung, L. (2022). MidSiot: A multistage intrusion detection system for internet of things. *Wireless Communications and Mobile Computing*, *2022*, 1–15. https://doi.org/10.1155/2022/9173291

[7]. Patel, A., & Jinwala, D. (2021). A trust-integrated RPL protocol to detect Blackhole Attack in internet of things. International Journal of Information Security and Privacy, 15(4), 1–17. https://doi.org/10.4018/ijisp.2021100101

[8]. Arshad, J., Azad, M. A., Amad, R., Salah, K., Alazab, M., & Iqbal, R. (2020). A review of performance, energy and privacy of intrusion detection systems for IOT. *Electronics*, *9*(4), 629. https://doi.org/10.3390/electronics9040629

[9]. Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion Detection System on IoT with 5G Network Using Deep Learning. *Wireless Communications And Mobile Computing*, *2022*, 1-13. https://doi.org/10.1155/2022/9304689

[10]. Ugendhar, A., Illuri, B., Vulapula, S., Radha, M., K, S., & Alenezi, F. et al. (2022). A Novel Intelligent- Based Intrusion Detection System Approach Using Deep Multilayer Classification. *Mathematical Problems In Engineering*, *2022*, 1-10. https://doi.org/10.1155/2022/8030510

[11]. Khan, A., Kashif, M., Jhaveri, R., Raut, R., Saba, T., & Bahaj, S. (2022). Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions. *Security And Communication Networks*, *2022*, 1-13. https://doi.org/10.1155/2022/4016073

[12]. Esmaeili, M., Goki, S., Masjidi, B., Sameh, M., Gharagozlou, H., & Mohammed, A. (2022). ML-DDoSnet: IoT Intrusion Detection Based on Denial-of-Service Attacks Using Machine Learning Methods and NSL-KDD. *Wireless Communications And Mobile Computing*, *2022*, 1-16. https://doi.org/10.1155/2022/8481452

[13]. Wu, Y., Wei, D., & Feng, J. (2020). Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey. *Security And Communication Networks*, *2020*, 1-17. https://doi.org/10.1155/2020/8872923

[14]. Yang, X., Peng, G., Zhang, D., & Lv, Y. (2022). An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph. *Security And Communication Networks*, *2022*, 1-21. https://doi.org/10.1155/2022/4748528

[15]. Diwan, T., Choubey, S., Hota, H., Goyal, S., Jamal, S., Shukla, P., & Tiwari, B. (2021). Feature Entropy Estimation (FEE) for Malicious IoT Traffic and Detection Using Machine Learning. *Mobile Information Systems*, *2021*, 1-13. https://doi.org/10.1155/2021/8091363

[16]. Saba, T., Khan, A. R., Sadad, T., & Hong, S.-phil. (2022). Securing the IOT system of smart city against cyber threats using Deep Learning. *Discrete Dynamics in Nature and Society*, *2022*, 1–9. https://doi.org/10.1155/2022/1241122

[17]. Sangeetha, S. K. B., Mani, P., Maheshwari, V., Jayagopal, P., Sandeep Kumar, M., & Allayear, S. M. (2022, September 20). *Design and analysis of multilayered neural network-based intrusion detection system in the internet of things network*. Computational Intelligence and Neuroscience. Retrieved October 20, 2022, from https://doi.org/10.1155/2022/9423395

[18]. Zhang, W., & Zhang, Y. (2022). Intrusion detection model for industrial internet of things based on improved autoencoder. *Computational Intelligence and Neuroscience*, *2022*, 1–8. https://doi.org/10.1155/2022/1406214

[19]. Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S., & Idris, N. B. (2020). Intrusion detection system for the internet of things based on blockchain and multi-agent systems. *Electronics*, *9*(7), 1120. https://doi.org/10.3390/electronics9071120

[20]. Dr. S. Smys, Dr. Abul Basar, & Dr. Haoxiang Wang. (2020). Hybrid intrusion detection system for internet of things (IOT). *December 2020*, *2*(4), 190–199. https://doi.org/10.36548/jismac.2020.4.002

[21]. Wang, Y., Sun, G., Cao, X., & Yang, J. (2022). An intrusion detection system for the internet of things based on the ensemble of unsupervised techniques. *Wireless Communications and Mobile Computing*, *2022*, 1–11. https://doi.org/10.1155/2022/8614903