Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Intrusion Detection in IOT Networks using Machine Learning Techniques

Ahmed Adnan Hadi[1*], Khalid Murad Abdullah[2]

[1,2]Open Educational College, Al-Qadisiyah Center, Iraq.*

Email: [2]Khalid.mu.abdullah@gmail.com
Corresponding Email: [1]ah2036@gmail.com*

Received: 28 September 2023 **Accepted:** 17 December 2023 **Published:** 01 February 2024

Abstract: ***Artificial intelligence (AI) and machine learning (ML) are essential for processing vast datasets and forecasting unknown events, offering innovative solutions to IoT security challenges. Recurrent neural networks (RNNs) have extended the predictive capacity of traditional neural networks, particularly in forecasting sequential events. With the increasing frequency of system attacks, the integration of machine learning into intrusion detection systems (IDS) is vital to identify and report potential threats, thereby safeguarding IoT infrastructure against destructive attacks***

Keywords: ***Internet of Things (IoT), Intrusion Detection System (IDS), Distributed Denial of Service (DDoS), Artificial Intelligence (AI), and Long Short Term Memory (LSTM).***

1. INTRODUCTION

The term" IoT" denotes a growing web of sensors linked to the Internet, these sensors assigned an IP address akin to conventional devices. This network relies on sensors for environmental data collection, yielding inputs for decision-making by controllers and subsequent activation of actuators. AI, a cornerstone of computer science, facilitates machine learning and decision- making, particularly evident in IoT through AI models constructed using extensive training data to guide system operation.
IoT security confronts challenges such as DoS/DDoS attacks, intrusion detection. Traditional solutions are limited by their incapacity to process large datasets and attain real-time efficiency, necessitating the integration of machine learning to extract insights from IoT big data, thereby offering innovative security solutions.

Neural networks, powerful in pattern recognition, lack the capacity for event storage and linking. The advent of RNNs has broadened the realm of ML, particularly in predicting sequential events.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Amidst escalating system attacks, notably the dangerous nature of denial-of-service (DOS) attacks, the imperative for robust technological security is evident. Augmenting traditional IDS with ML techniques is essential to detect and report attacks promptly, mitigating potential human errors and reducing recovery costs, thus safeguarding IoT infrastructure against potential devastation.

Purpose of the Research

The research aims to keep the IOT system safe by building an IDS system using ML techniques to detect DOS attacks on data. The IDS system design requires a database of normal and abnormal data (attack data), so we will capture the data during the normal flow and once during an attack carried out using a hostile system. We will use a RNN with LSTM to detect a DOS/DDOS attack on either a web server or a raspberry pi for a water tank monitoring system, where the sensor (distance sensor) reads the tank's water level and sends this data to the raspberry controller. pi 3 B+, and then the controller sends the result to an Internet site.

2. RELATED WORK

In this study[1], some future ideas for applying AI with IOT were discussed, and among these ideas is making tools equipped with sensors transmit information to each other, and the second idea is data mining, and the research presented a definition of the IOT and AI and its areas of use, then addressed the integration AI with IOT. He mentioned the challenges facing AI with IOT. A blueprint for a smart-industrial was presented using a fake neural system and AI security. It uses phone cells as smart objects and uses back engendering for training. This proposed model will be applicable in the future with IPV4 and the industrial revolution.

The research [2] presented a theoretical study on the Internet of Things (IOT) and the concept of artificial intelligence (AI), and presented an architecture for IOT with AI, which includes building a set of models using machine learning algorithms with a set of training data. The second stage is to use the best model to create an inference between the input and output data of the system. The research then touched on the challenges of AI with IOT, and among these challenges is security to ensure that important data sent from the sensor remains safe. Finally, the research dealt with some applications of AI with IOT, and among these applications are Home automation, oil field production, and smart hotels. We note that the research was limited to studying theory. It did not mention any practical application.

In this study[3], the concept of the IoT was presented with an explanation of the three-layer architectural structure, then the reasons for the security threats to which the IoT was exposed were presented, including the lack of human supervision and resource-constrained devices that limit the application of strict security procedures, the openness of the Internet of Things, and the lack of independence of the Internet of Things layers. In the event of an error occurring, the research then addressed the security threats to which the perception layer is exposed, which are physical attack, exposure to data sent from the IOT nodes, and bypassing identification and authentication to carry out intrusion. Then the research presented the

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

security threats to which the network transport layer is exposed, which suffers from DOS and DDOS attacks that affect the entire system. Security problems were presented at the application layer, which includes system and data security. Some of the necessary requirements for implementing security were presented, including monitoring normal and abnormal work patterns in real time and early warning in the event of anomalies. In case of unpredictability due to the diversity of the attack, which leads to more effective security requirements that are able to control data effectively, and design secure IOT systems that learn and upgrade the security scheme in a timely manner.

Then the research focused on the new capabilities that artificial intelligence provides for Internet of Things security, including machine learning ML. The algorithms are divided into transaction Algorithms and decision algorithms, and the pros and cons of the strategies of each section for achieving security in IOT are presented.

The research also highlighted AI solutions using machine learning for four security threats in IoT, which include DOS/DDOS attack, intrusion detection, and the research showed the flow of solutions in the basic process.

The research [4] highlighted the characteristics of the IoT system (sensing, deterministic automation of work and communication, limited network resources, and homogeneity), then shed light on some attacks on the Internet of Things system, such as the DDOS attack. Then, it talked about the role of ML techniques for both host-based and network-based security, focusing on the limitations associated with each technology, computing limitations, and energy consumption to arrive at the pros and cons of each technology.

Finally, the research discussed some of the challenges that machine learning techniques must face to build a more secure and effective IoT system.
IDS in [5] was invented based on the structure of RNN with LSTM .The proposed model resulted in high detection rate, accuracy, and low false alarm rate. Hence, the (NSL-KDD) dataset was used for training and testing.

IOT
IoT is a vast interconnected ecosystem consisting of numerous physical objects that are seamlessly connected to the internet. These objects, which can range from everyday devices to sensors and machines, are assigned IP addresses, enabling them to communicate with each other and exchange data. Through the utilization of sensors embedded within these objects, the IoT facilitates the collection of real-time information about the surrounding environment. This data is then processed and utilized by various controllers and actuators to make informed decisions and initiate automated actions. The integration of AI and ML further enhances the fields of IoT systems by acquiring knowledge from collected data and adjust to dynamic circumstances., and deliver intelligent insights and solutions. The IoT has brought about a significant transformation in multiple sectors, offering substantial opportunities to enhance operational efficiency, boost productivity, and drive overall improvement..[6][7]

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

IOT Components
It comprises of as in the figure (1):

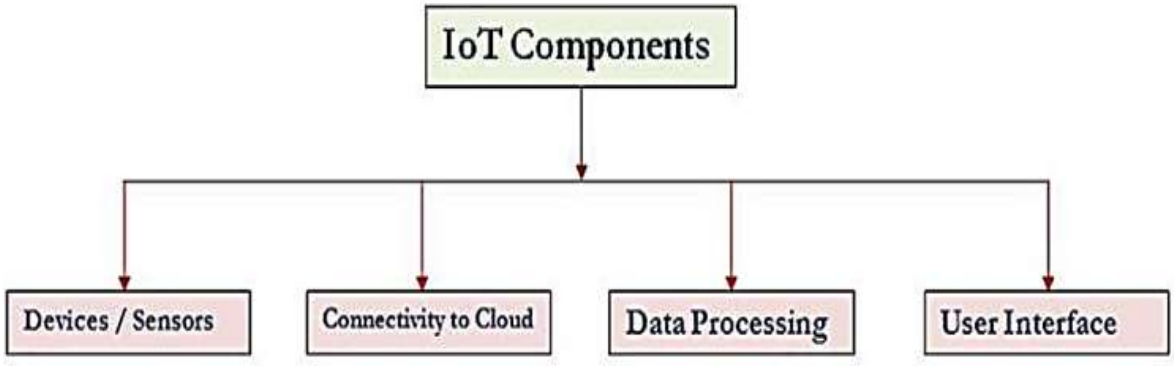


Figure. 1 IoT Components [8]

Sensors: They are responsible for collecting data from the environment, then data is transferred to the next layer in the IoT system for processing, analysis, and further actions [8].

Connectivity to Cloud: most modern smart devices and sensors can be connected to low-power wireless networks such as Wi-Fi, ZigBee, Z-wave, etc. which have advantages and disadvantages in terms of power consumption, data transmission rate, and overall efficiency. [8]

Data Processing: IOT systems generate a substantial amount of data, and this data must be managed efficiently to achieve valuable results. Using cloud enables efficient data management, effective utilization of the gathered data ...[8]

User Interface: it has role in bridging the gap between users and the complex technologies of IoT, as the processed data is transferred to the user interfaces.[8]

Three Layer Architectures for IOT
Different researchers have been proposed different architectures, Three Layer structure consists of three layers as in figure (2):

Perception Layer: this layer contains sensors that senses some physical parameters, and then data is transferred to the next layer.

Network Layer: handles communication between different smart objects, network devices, and servers. Here sensor data are transmitted and processed. **Application Layer**: is accountable for delivering specialized functions to the user. It recognizes the various applications that can be implemented within the Internet of Things.[9]

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

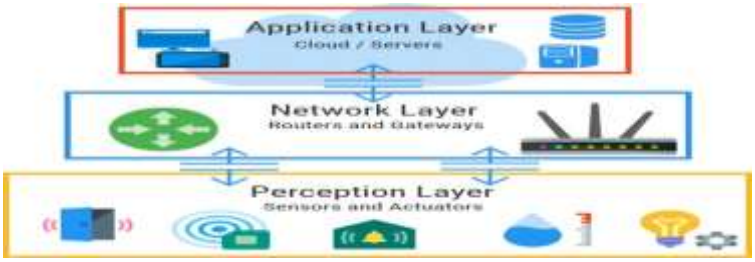


Figure. 2 Three Layer Architectures for IOT

ML: ML is an AI technique that enables systems to learn and improve from data without explicit programming. In the realm of IoT security, there are pressing issues such as DDoS attacks. Conventional approaches suffer from inefficiency and poor real-time performance. However, ML with different types as in figure (3) can leverage the vast amounts of IoT data to detect abnormal behavior and classify normal patterns and attacks. This makes ML a powerful tool to tackle IoT security challenges.

Supervised Learning: it is based on the presence of data and its correct evidence at the time of learning so that this data constitutes real examples from which the model can learn. Among the most famous algorithms that are used to detect a DDOS attack are the DNN, KNN, SVM, and Naïve Bayes.[10]

Unsupervised Learning: It is learning that results from the presence of data without its correct evidence. One of the most famous types of unsupervised learning is cluster analysis, and one of the most famous techniques used to detect a DDOS attack is the K-Means algorithm.[10]

Deep Learning: is a subfield of AI that focuses on developing algorithms work as human brain. It involves the use of artificial neural networks, allowing the system to learn and extract complex patterns and representations from large sets of data. Deep learning enables machines to automatically learn and improve performance through experience, without requiring explicit programming. [10]

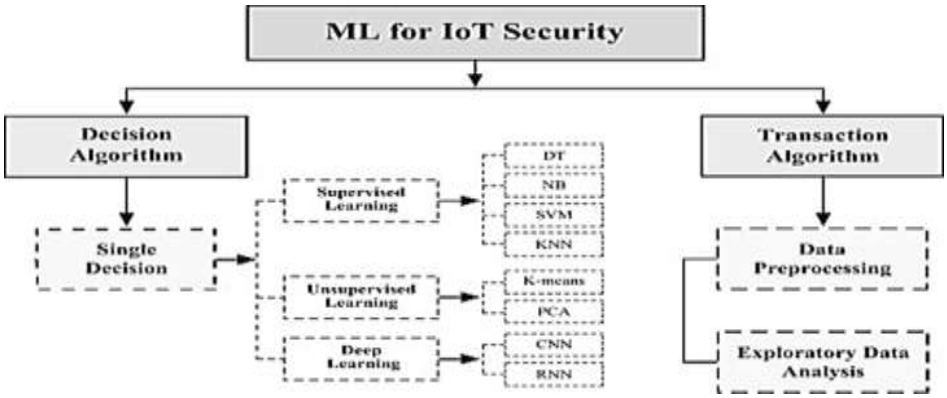


Figure. 3 Ml for IOT security

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

RNNs

Standard neural networks lack the ability to store and link events together. For example, it is easy for a neural network to distinguish between two different types of fruits, but it is difficult for it to predict stock prices or complete texts automatically. Here lies the importance of RNNs as they contain memory.

Very similar to traditional neural networks, they are successive copies of the same network, each of which passes the message to the next ring, as Figure (4) shows.

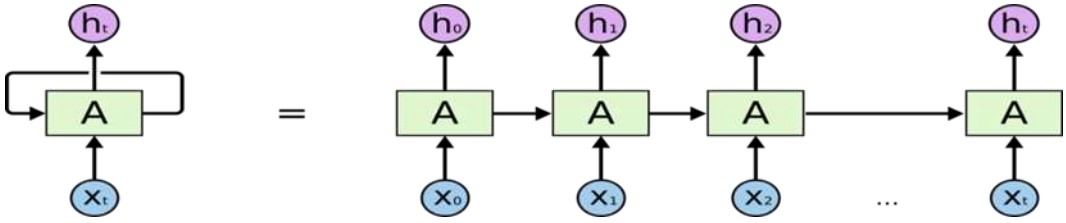


Figure. 4 RNNs

RNNs (Recurrent Neural Networks) are specialized for handling sequential data and perform the same operation on each element of a sequence, with the output influenced by previous computations. RNNs employ bidirectional information flow, reusing input from the previous time step in the current one. In contrast, feed-forward neural networks consist of input, hidden, and output layers, with the output of each node determined by weight matrices and an activation function. Backpropagation adjusts the network's weights to achieve the desired output.

RNNs are distinguished by their backward connections, allowing outputs from one layer to feed back into the same layer or a previous one, enabling them to maintain a state utilizing previous time step values as short-term memory. Commonly used for analyzing time series or sequential data, RNNs have broad applications due to their ability to handle sequential information effectively.

$$h_t = \sigma(Wx_t + Uh_{t-1} + b_h), \text{ for } t = T, \ldots, 1 \qquad (1)$$

RNNs utilize a nonlinearity function (σ) to process input vectors (x_t) at each time step and maintain a current state vector (h_t). The network incorporates weight matrices (W, U) and a bias term (b_h) to influence the transformation of inputs.

Unfolding an RNN transforms it into a standard neural network, with each node representing a layer. This unfolded network is then trained using backpropagation through time. However, capturing long-term dependencies has proven challenging for RNNs due to the "vanishing gradient" problem. To address this, specialized RNN architectures like LSTM have been developed. These architectures effectively tackle the issue of capturing long-term dependencies.

In an LSTM network, an LSTM cell is responsible for storing the network's state over time. This is achieved through the use of (input ,output , forget) gates that control access to the cell which allow the cell to hold data for varying durations and discard it when no longer necessary.[5]

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

$$a_t^j = o_t^j \tanh(c_t^j) \quad (2)$$

$$o_t^j = \sigma(W_o x_t + U_o a_{t-1} + V_o c_t)^j \quad (3)$$

$$c_t^j = f_t^j c_{t-1}^j + i_t^j \widetilde{c}_t^j \quad (4)$$

$$\widetilde{c_t^j} = \tanh(W_c x_t + U_c a_{t-1})^j \quad (5)$$

Where c^j_t is j-th LSTM memory at time t

a^j_t is the output or the activation,

o^j_t output gate that modulates the amount of memory content exposure

σ is a logistic sigmoid function,

V_o is a diagonal matrix, and f^j_t is the forget gate

DDOS Attack

DDoS is a cyber-attack that floods a targeted network, system, or website with a huge volume of traffic, using compromised computers or devices. Its purpose is to disrupt normal functioning by overwhelming the target's resources, leading to denial of service for legitimate users. The attackers often exploit botnets, which are networks of infected devices under their control. Such malicious actions can have severe consequences for businesses, organizations, and individuals, causing downtime, financial losses, and reputation damage.

DDOS Attack Types

HTTP GET: Attacks involve coordinating multiple computers or devices to inundate a target server with a deluge of requests, such as images or files. This flood of incoming requests and responses overwhelms the server, resulting in a denial of service for legitimate users. An example of this attack is when an Apache server bombards a page or website, pushing the server to its limits and rendering it unavailable.

UDP Flood: Attacks exploit a transport layer protocol (TCP/IP) that does not require establishing a reliable communication channel. In this attack, multiple unauthorized connections are established between the attacker and the server, using random ports. The server responds to each connection with ICMP packets, considering them as legitimate requests. These ICMP packets are sent in large volumes, overwhelming the server and causing it to become congested and unresponsive. This attack effectively floods the server, leading to its incapacitation.

TCP Flood: attacks exploit the characteristic of the TCP protocol that establishes a connection for every packet, ensuring that the packets arrive at the server in the correct order. In this type of attack, the attacker establishes numerous connections to the targeted server or device, overwhelming it with an excessive number of communication channels. Consequently, the server becomes flooded with an overwhelming amount of data traffic, causing it to become unresponsive and effectively blocked from providing its service.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

ICMP (Ping) Flood Attack: ICMP, short for Internet Control Message Protocol, is a communication protocol used for sending control or error messages within the TCP/IP protocol suite. One of its commonly used functionalities is the Ping command, which verifies if a target device is connected or not. Most devices respond to ICMP packets by sending back similar packets. Exploiting this behavior, attackers can effortlessly incapacitate a targeted device by inundating it with an overwhelming volume of ICMP packets.

The working principle of this attack closely resembles that of the flood attack discussed earlier, where the objective is to overwhelm the target with an excessive barrage of requests. However, in the case of an ICMP flood attack, the attacker specifically utilizes ICMP packets to keep the target device occupied with constant responses. This results in the target device consuming substantial resources, crippling its ability to effectively handle incoming and outgoing data. Due to its wide availability and simplicity, the use of ICMP packets in this attack has become widely prevalent.

The ICMP flood attack can be divided into two main steps:

- The attacker employs multiple devices, often forming a botnet, to send a large influx of ICMP echo request packets to the target server.
- The destination server, upon receiving each request, issues an ICMP echo reply packet back to the originating device, unknowingly adding to the overall congestion.[11]

IDS:
The concept of intrusion detection is defined by the RFC2828 standard as a security service that monitors and analyzes system events to detect unauthorized access attempts. It issues alerts in real or near-real time when such attempts are detected.
The intrusion detection system operates with three main components:

Sensors: These collect data from various sources.

Analyzers: These determine if a breach has occurred by analyzing the collected data.

User interface: This allows users to view the system's output or control its functionality.

Classification of IDS:
IDS can be classified into three categories:

Host-based IDS (HIDS): It monitors the activity of a specific computer to detect any suspicious behavior while it is running.

Network-based IDS (NIDS): It examines data passing through a network, analyzing the content of packets at different layers (network, transport, and application) to detect suspicious activity.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Distributed or hybrid IDS: This system collects information from a group of sensors and channels it to a central analyzer. The sensors can be host-based or network-based, enhancing the effectiveness of identifying and responding to hacking activities.[12]

3. METHODOLOGY

The system consists of three main components:

IOT system: We will build an IOT system based on monitoring a water tank, where the sensor (distance sensor) reads the tank's water level and sends this data to the raspberry pi 3 B+ controller as in figure (5)(6), and then the controller sends the result to a website where we will use the Ubuntu server, and on it The web server was used as Apache, HTML and CSS were used as front-end, and PHP was used as back-end.

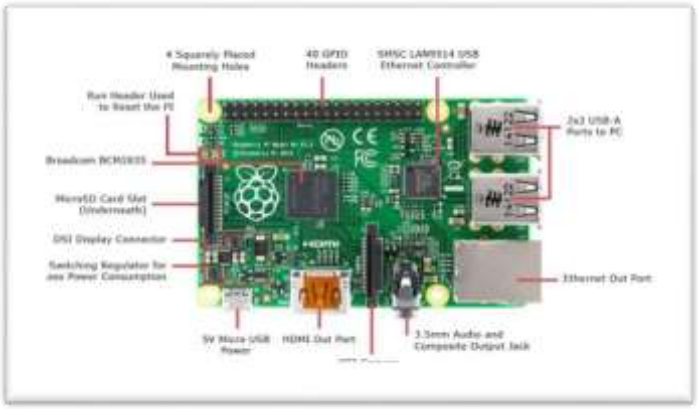


Figure. 5 raspberry pi



Figure. 6 distance sensor

Generating a DOS/DDOS attack on either a web server or raspberry pi where either a UDP Flood or HTTP GET attack can be applied using the tool LOIC (Low Orbit Ion Cannon) that can be used for testing load in networks and generating DDOS attack, depicted in figure (7).

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

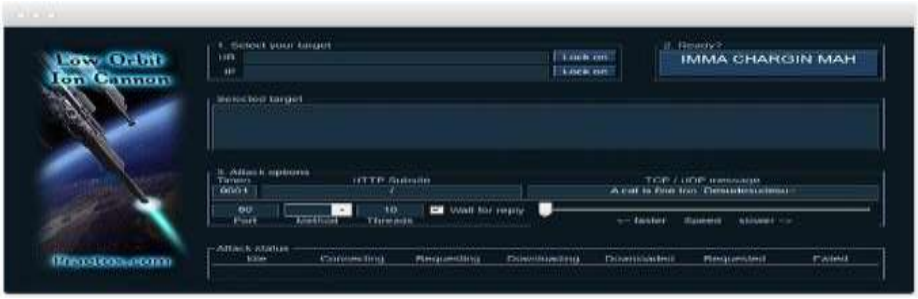


Figure. 7 LOIC tool

Building an IDS System: After applying the attack, we will build an intrusion detection system by monitoring the network and taking samples (dataset), then training it using artificial intelligence techniques (ML) and using the model trained in the IOT system to detect attacks on it. And report it.
The IDs system we developed is based on machine learning, its main purpose is to detect that the network has been attacked by DDoS.
The system uses Wireshark (in the CLI) to capture all traffic that occurs on the network.
Once the traffic is captured, we pass it through artificial intelligence that has been trained to detect suspicious packets and prevent them from harming the network. This system used the Tensor Flow AI package to create neural networks, which in our case consisted of two LSTM layers and two layers of connected neurons.

He has several commands:
Start: Makes the system scan the network and record all malicious traffic.
Stop: Stops the system from scanning the network.
DDOS: Tests for DDOS attacks.
MITM: Tests for man-in-the-middle attacks.
DDOS & MITM: Tests for both attacks.

It has a graphical interface as in figure (8) that can be accessed through the browser through the following address: http://localhost:5000

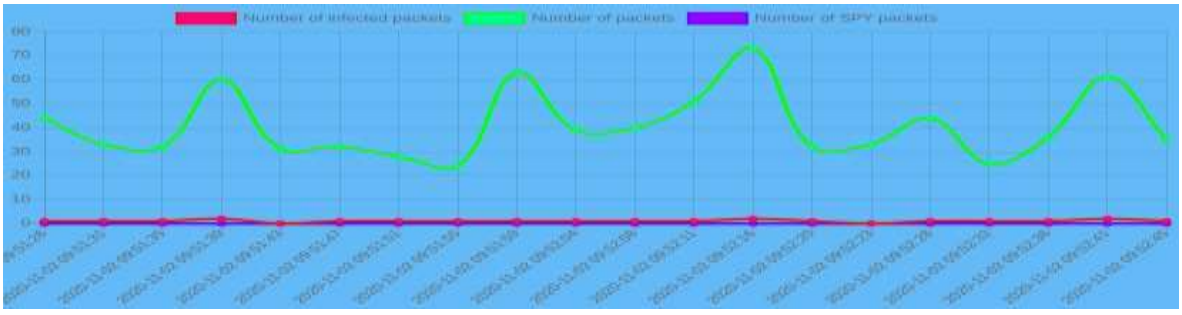


Figure. 8 graphical interface for IDS

First, we have to run the sensor code through the Raspberry Pi controller, which is the sersor.py file, which contains the most important functions.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Get distance (): It is the function that calculates the water level in the tank using the pulse received from the sensor signal.

Send Data _to_remoteServer (dist): It is the function that sends the value that expresses the water level in the tank to the web server.
Then the website files are run, which receives the data sent from the sensor and processes these values by placing them on the graphical interface.
The site consists of files for the graphical interface (front-end) and files for the programming interface (back-end) ,depicted in figure (9).

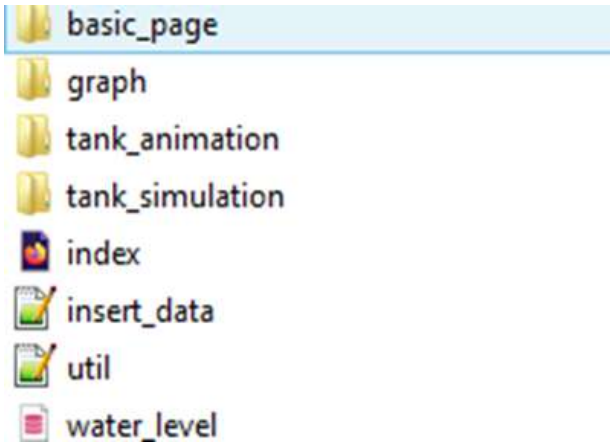


Figure. 9 website files

The most important of these files is the util.php file, which establishes communication with the database and uses the insert data file, which inserts the values received from the sensor into the data base, depicted in figure (10).


Figure. 10 util.php file

When the site is turned on, it appears to us in Figure (11), which expresses the tank level and whether the value sent by the sensor has been received.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18



Figure. 11 front-end for website



When requesting the database through the website phpMyAdmin, we find all the sensor values stored within the database, as shown in Figure (12).

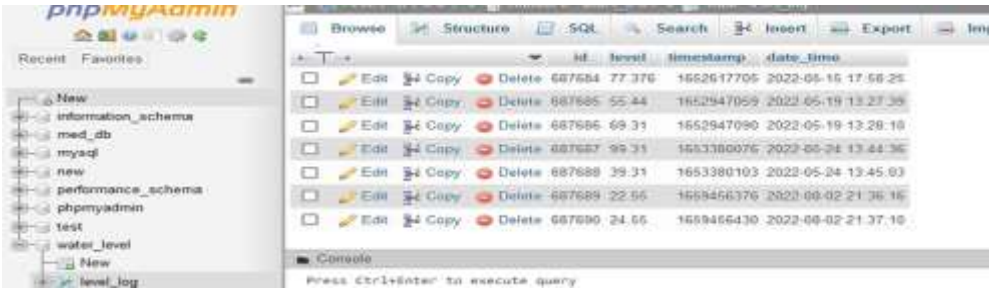


Figure. 12 database

Now from the second stage of the project, which is to implement a DDOS attack on the server or on the controller, we use LOIC by setting the IP address of any device and then choosing the number of botnets to be placed in the attack and the method to attack, where the UDP method is chosen as shown in the figure (13).



Figure. 13 Setting up a DDOS attack

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

When our IDS system is running, the system shows the attack detection, depicted in figure (14).

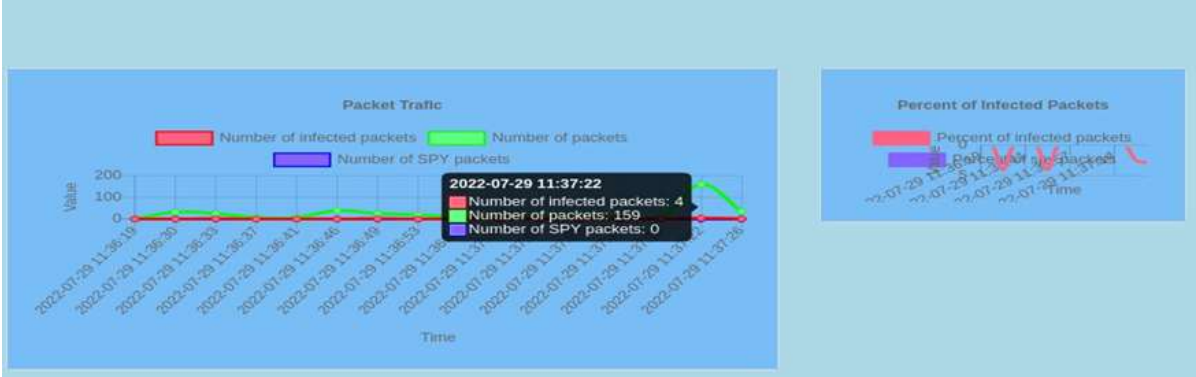


Figure. 14 DDOS detection

We used dataset, namely CICDDoS2019 that encompasses both benign traffic and the latest prevalent DDoS attacks, closely mirroring real-world PCAP (Packet Capture) data. This dataset not only provides insights into common DDoS attack patterns but also includes the outcomes of network traffic analysis utilizing CICFlowMeter-V3. The labeled flows within the CSV files offer a comprehensive view of network activity, incorporating details such as timestamps, source and destination IPs, ports, protocols, and specific attack classifications. This level of detail is critical for understanding and effectively mitigating DDoS threats, making the CICDDoS2019 dataset an invaluable resource for cybersecurity professionals seeking to bolster their defense strategies against these disruptive and evolving attack vectors.

Evaluation

To obtain model's performance, we used accuracy, recall, precision and F as shown in table (1) And Response time was calculated for both the TCP Syn Flood and UDP Flood attacks, in addition to the HTTP Get attack in two scenario.

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

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{Recall}=\frac{TP}{TP+FN}$$

$$\text{F}=2\frac{Precision*recall}{precision+recall}$$

where TP is true positive, TN is true negative, FP is false positive, and FN is false negative.

We compared our results with results in paper [13].

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Table. 1 performance metric for CICDDoS2019

Algorithm	ACCURACY	Precision	Recall	F
RNNs(LSTM)	0.96	0.96	0.95	0.96
Na¨ıve Bayes	0.45	0.41	0.11	0.05
Logistic regression	0.35	0.25	0.02	0.04

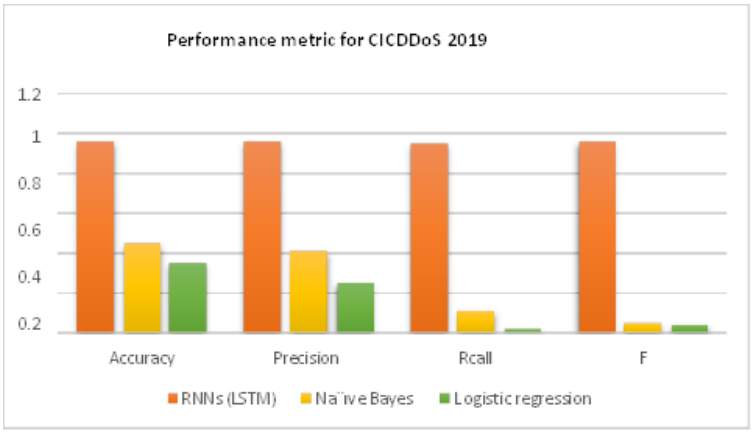


Figure. 15 performance metric for CICDDoS2019

It is worth noting that a DDOS attack makes the website or web server's response slow, so we studied the effect of the attack on the website's response time, as these values were calculated by ping through the RTT (Round Time Trip) time [13].

First Scenario: Response time was calculated for both the TCP Syn Flood and UDP Flood attacks, in addition to the HTTP Get attack, where an attack time of 100 seconds was chosen and the number of botnet (threads) was 1000 threads.
We found the following results:

TCP Syn Flood

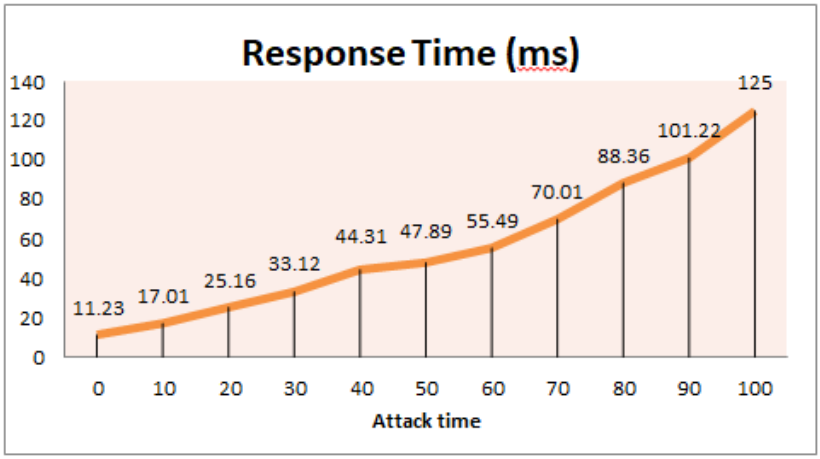


Figure. 16 response time TCP Syn Flood in 1st scenario

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

It is clear from the figure (16) that as the attack time increases, the packets sent by the botnet to our server increase, and therefore the server is like any computer that has resources (processor, RAM), which makes its response time to other clients short and sometimes goes out of service, and thus the concept of the attack has been achieved.

HTTP Get:

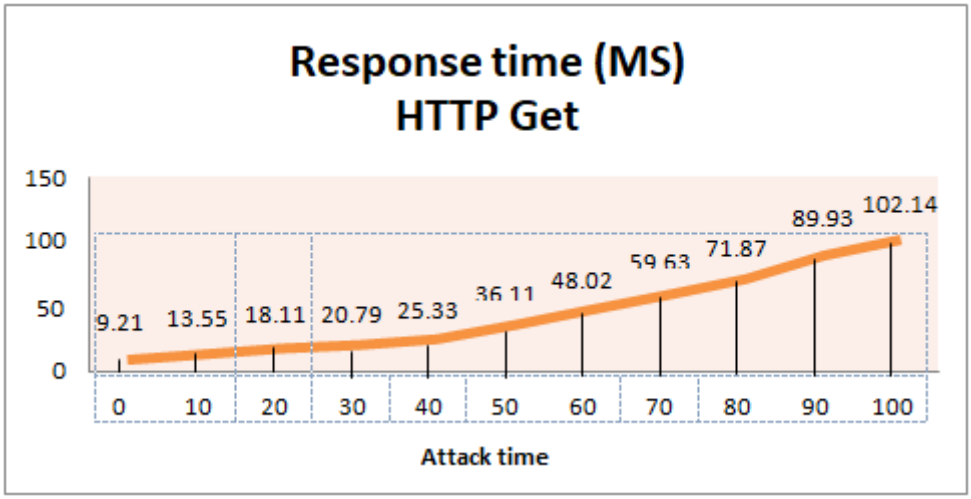


Figure. 17 response time for http get in 1st scenario

UDP Flood:

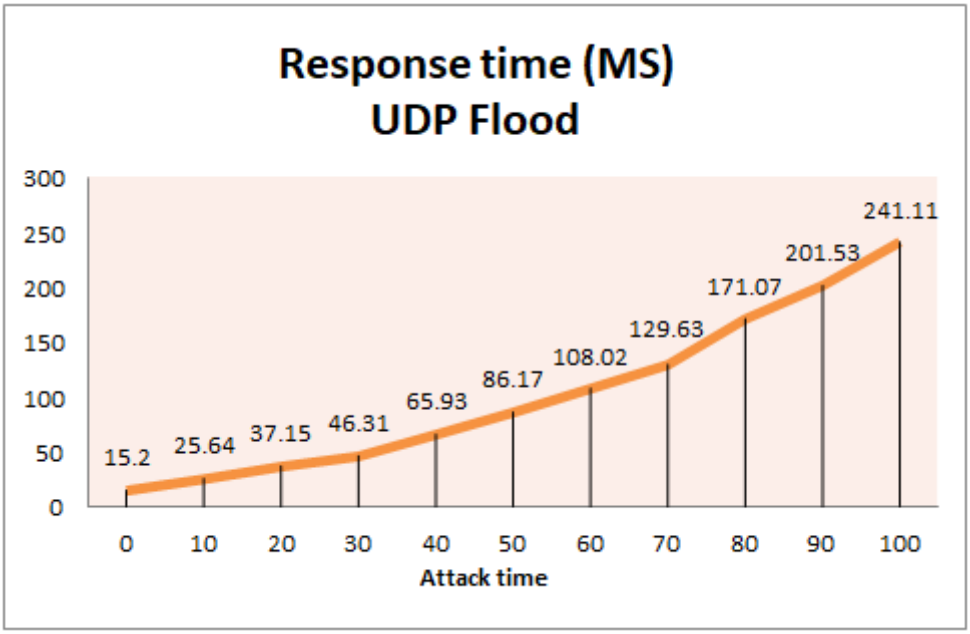


Figure. 18 response time for UDP Flood in 1st scenario

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

Second scenario: the botnet was increased to 1200, 1400, 1800, and 2000 threads, and the response time was calculated during a specific moment of the attack time, which is t=50 sec.

TCP Syn Flood:

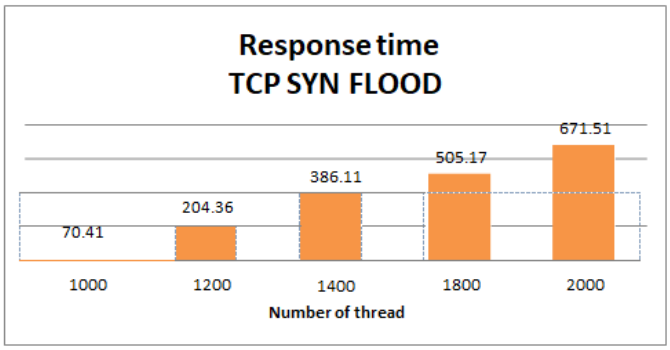


Figure. 19 response time TCP Syn Flood in 2st scenario

HTTP GET:

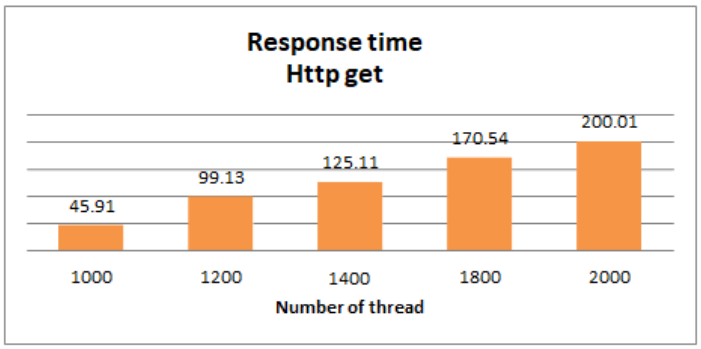


Figure. 20 response time for Http get in 2st scenario

UDP Flood

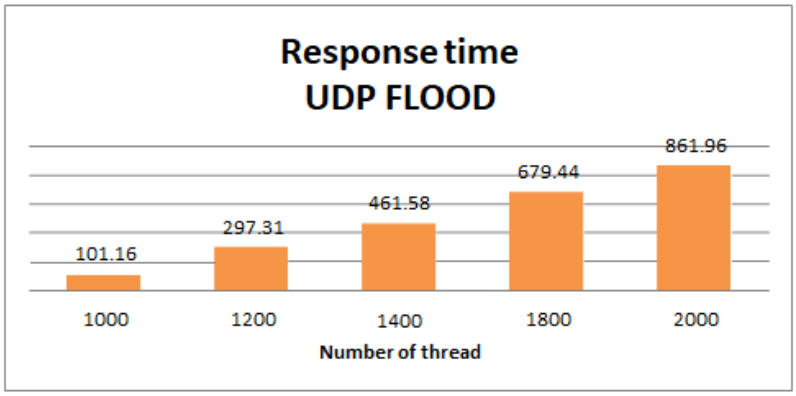


Figure. 21 response time for UDP Flood in 2st scenario

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

4. RESULTS

The LSTM algorithm outperformed the NAIVE BYES algorithm and the Logistic regression algorithm because RNNs have some properties that make them well suited for DDoS detection tasks:

- Ability to learn patterns in sequence/time-series data: Network traffic data used for DDoS detection often has a temporal sequence/order to it. RNNs are designed to capture patterns in sequential data via their recurrent connections between nodes. This helps them learn normal vs anomalous traffic patterns.
- Handle variable length input: DDoS attacks can occur over varying durations. RNNs do not require fixed length input sequences, so they can process traffic data of different lengths.
- Contextual information: The recurrent connections allow RNNs to maintain contextual information about past inputs/states, which helps in analyzing the flow/context of network traffic over time.
- Naive Bayes may work better for detecting certain flooding attacks where features are more independent. While Logistic regression would perform better for attacks with complex inter- feature relationships as it can model those linear interactions

5. CONCLUSION

The research presented within this document aimed to address the escalating security threats within IoT networks, focusing on the detection of DoS/DDoS attacks using machine learning techniques. The integration of Recurrent Neural Networks (RNNs) with Long Short Term Memory (LSTM) units has shown promise in enhancing the capabilities of traditional intrusion detection systems. By leveraging a dataset composed of both normal and abnormal traffic, including that from a simulated attack, the proposed IDS was able to learn and distinguish between legitimate and malicious data patterns.
Throughout the study, the importance of IoT security was emphasized, highlighting the vulnerability of IoT infrastructures to various forms of cyberattacks. The employment of AI and ML has been critical in developing a system that can not only detect known attack vectors but also adapt to new and evolving threats. This adaptability is crucial given the dynamic nature of IoT environments and the sophistication of modern cyberattacks.

The results of the research indicate that the use of an RNN with LSTM can effectively identify potential threats, thereby significantly reducing the likelihood of successful DoS/DDoS attacks on IoT systems. The proposed model demonstrated high detection rates and accuracy while maintaining a low rate of false positives, as evidenced by the performance metrics obtained during the evaluation phase using the (NSL-KDD) dataset.

This conclusion serves as a testament to the potential of machine learning techniques in fortifying IoT networks against cyber threats. By continuing to refine these techniques and integrate them into IoT security strategies, it is possible to create more resilient and intelligent systems capable of withstanding the ever-growing challenges of cybersecurity.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.42.1.18

6. REFERENCES

1. Arun Kuma, Sachin Dhawan, Ram Krishna, Sharad Sharma. “Review on Artificial Intelligence with Internet of Things - Problems, Challenges and Opportunities" Operational Research in the Digital Era–ICT Challenges. Springer, Cham, 2019. 11-22.
2. E. Mohamed, " The Relation of Artificial Intelligence with Internet of Things: A survey," in JCIM, Vol. 1, No.1, PP.30-34, 2020.
3. K. G. Srinivasa, S. Srinidhi, K. S. Kumar, V. Shenvi, U. S. Kaushik and K. Mishra, "Game theoretic resource allocation in cloud computing," The Fifth International Conference on the Applications of Digital Information and Web Technologies doi:10.1109/ICADIWT.2014.6814667
4. Zafari, Faheem & K. Leung, Kin & Towsley, Don & Basu, Prithwish & Swami, Ananthram. (2019). “A Game-Theoretic Framework for Resource Sharing in Clouds”.
5. M. Ibrahim, R. Elhaf," Modeling an intrusion detection using recurrent neural networks”. Journal of Engineering Research in Vol. 11, Iss. 1, March (2023).
6. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.
7. https://www.leverege.com/iot-ebook/how-iot-systems-work
8. https://www.ibm.com/topics/infrastructure
9. https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/
10. Sh.Zeadally, Michail .Tsikerdekis,” Securing Internet of Things (IoT) with machine learning “Wiley, 2020.
11. M.Reazul, S.ChinTan, C.Kwang, , B.Chowdhry, R.Buyya, Automated Controller Placement for Software-Defined Networks to Resist DDoS Attacks
12. J. Sicato, S. Singh, Sh. Rathore, J.Park,”A Comprehensive Analyses of Intrusion Detection System for IoT Environment” Journal of Information Processing Systems, September 2020.
13. I. Sharafaldin, A.Lashkari, S. Hakak, Ali. Ghorbani.”Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy “IEEE, 2019.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)