International journal of engineering science and management (IJESM).
ISSN: XXXX-XXXX.
https://doi.org/XX.XXXXX/XXXXXXXXX/IJESM-XXXXXXXXXX

Volume: 24, Issue 1, 13-24, April 2024.

ENHANCING DATA SECURITY USING INTRUSION DETECTION TECHNIQUE

Dr. K. SURESH BABU[1], MADASU ASHWAN KUMAR[2]
[1]Professor, Department of CSE, JNTUH, Email Id: Kare_suresh@yahoo.co.in
[2]MTECH, COMPUTER NETWORKS AND INFORMATION SECURITY (21031D6404), JNTUH, Email Id: ashwanmadas21@gmail.com

Received: 2 March 2024 Revised: 24 March 2024 Accepted: 03 April 2024 Published: 16 April 2024

ABSTRACT:
The Internet of Things (IoT) is a rapidly evolving concept with the potential to revolutionize interactions between individuals and organizations in the physical world. IoT connectivity aims to enable seamless and secure communication among various "things" by leveraging IT infrastructure. This technology has found applications in diverse domains, including healthcare, education, resource management, and data processing. However, the integration of IoT technology raises significant safety and privacy concerns that require addressing before widespread adoption. One critical aspect of improving the cybersecurity of IoT devices and networks involves mitigating Distributed Denial of Service (DDoS) attacks, which can exploit the bandwidth of IoT devices. IoT networks, characterized by their wireless nature, self-configurability, independence from existing infrastructures, and numerous nodes with unpredictable mobility patterns, require robust security measures. To enhance the cybersecurity of IoT devices and networks, we propose a method designed to counteract DDoS attacks, which represent a challenging and hard-to-detect threat that can severely degrade network performance. DDoS attacks involve a coordinated effort by malicious nodes to target a victim, effectively denying legitimate users access to network services and resources. Intrusion Prevention Systems (IPS) within IoT devices complement Intrusion Detection Systems (IDS) by actively combating and thwarting identified attacks. Our proposed approach focuses on analyzing bandwidth-based attacks, particularly DDoS attacks, which are highly disruptive and can significantly impair network functionality. The suggested methodology relies on insights derived from IDS reports, generated after thorough data analysis during forensic examinations. By leveraging the information from these reports, we can proactively enhance the security of IoT devices and networks, bolstering their resilience against DDoS attacks and other malicious activities.

INDEX TERM'S – Intrusion Detection, Internet of things, DDoS attacks.

1. INTRODUCTION:

An Intrusion Detection System (IDS) is a remote set of resources or computing resources that monitors a network or infrastructure for signs of improper functioning or method breaches. Typically, a Security Information and Event Management (SIEM) platform is employed to report any incidents or security breaches to a central authority or supervisor [1].

A SIEM platform collects data from a wide range of sources and employs algorithms to distinguish between potentially malicious activity and false alarms. While IDS systems are designed to monitor networks for potentially harmful events, they may also generate false alerts [2].
Therefore, when implementing IDS systems within an organization, they require initial configuration. This entails tuning the intrusion detection systems so that they can differentiate between routine operational activities and behavior indicative of attempted malicious actions.

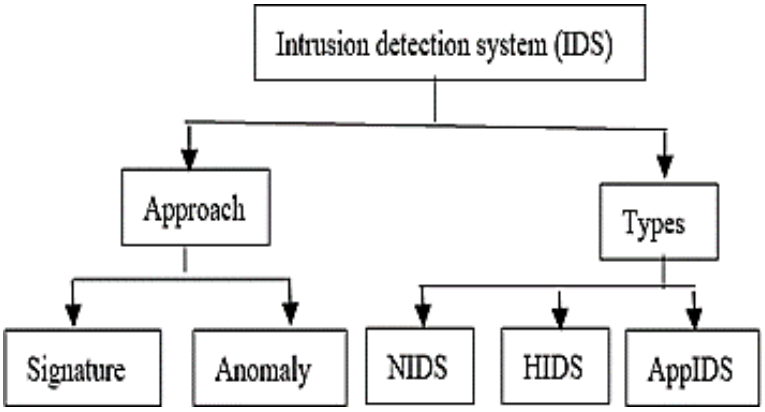

Figure 1 Classification of IDS

The Internet of Things (IoT) is a developing worldwide pattern in the plan of information that is based on the web. It makes it simpler for labor and products to be exchanged the worldwide production network organization [3].

IoT is a sort of program that unites various types of innovations and social spaces. It has said that IoT is "an organization of things, every one of which has remote sensors worked in and is associated with the web [4].

"The principal objective is to ensure that a wide assortment of things can be connected and controlled so they can converse with one another and clients [5].

A functioning IT framework can set up open correspondence conventions among genuine and virtual characters of things through astute associations. IoT permits two-way, steady sharing of information and data about the climate that is seen and quickly makes strides in view of what is happening in reality. The security of the IoT is quite possibly of its most serious issue, not its development. We as a whole realize that standard wired networks are more protected than IoT networks that don't utilize wires. Traditional framework networks let information travel through various course gadgets like switches, doors, and so forth, which are frequently safeguarded with exceptionally set firewalls and numerous other security the executives' procedures. In this way, these organizations are prepared for any sort of hacking or Denial of Service (DOS) strikes [6].

Then again, IoTs, which are additionally called shared networks, are compact and can be gone after in a wide range of ways. Conventional methods for established networks forbiddance function

happily in unrehearsed arrangings, place the design of capital of massachusetts changes repeatedly, contact between network centers is approved by chance, and skilled is no main issue of control [7].

Along these lines, each point that conveys needs to have some sort of safety framework worked in to stop any sort of assault.

2. LITERATURE REVIEW:

Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms

The Internet of Things (IoT) is an evolving general pattern in electronic data plan that create it more natural for things to exchange administrations and belongings over an institution outside talking in a group or to a PC. It can change how individuals and associations associate in reality. IoT can be utilized in numerous significant ways, like in medical services, overseeing assets, getting the hang of, handling data, and numerous different spots. IoT faces a ton of safety and security issues with regards to being utilized in reality. These issues should be settled for IoT to be utilized on a major scale that is financially conceivable. This paper takes a gander at the security issues of IoT networks by breaking down the genuine review that has previously been finished. The objective is to find out about the security needs of IoT organizations. The review's outcomes showed that security chances are one of the greatest and most developing issues for IoT, and that they should be managed amazingly for this stage to find actual success.

Defense Scheme to Protect IoT from Cyber Attacks using AI Principles:

Despite the fact that it is up until now new, the Internet of Things (IoT) has proactively caught analysis of most contemporary trades, like outstanding towns, boats, and dispassionate novelty. Since IoT joins everything, it very well may be gone after in numerous ways that can cause a great deal of harm. Having various devices associated with the web makes it simple for lawbreakers to begin their strikes. This study tells the best way to shut down these assaults by utilizing the essential thoughts behind Artificial Neural Networks to do an assault investigation. The directed ANN (Multilevel Perceptron) is prepared with Web information follows and afterward tried subsequent to preparing to stop DDoS assaults. This study piece is generally about putting traffic patterns in an IoT network into two gatherings: lawful traffic and assault traffic. A virtual IoT network is utilized to test and evaluate the ANN techniques. The aftereffects of the tests show that DDoS assaults can be found all the more precisely.

An IoT-Aware Architecture for Smart Healthcare Systems:

Over ultimate current couple of age, Internet of Things (IoT)- authorized plans have advanced considerably, that has incited the progress of new and spellbinding purposes. This pattern is being compelled by advances like radio frequency identification (RFID), wireless sensor networks (WSN), and intelligent container phones. In light of this pattern, this paper intends a new, IoT-aware, intelligent anticipate register observant and following of sufferers, stick, and natural novelty in hospitals and nursing schools. In accordance with the IoT concept, we suggest a smart hospital system (SHS) that resorts to various still exchanged advances, like RFID, WSN, and savvy adjustable. These changes talk in a group through a Constrained Application Protocol (CoAP)/IPv6 over low-power wireless personal area network (6LoWPAN)/representational state transfer (REST) network bedrock. Through an excellent depressed-capacity composite grasping network (HSN)

encompassed of 6LoWPAN centers accompanying UHF RFID value, the SHS can take dossier about the environmental factors and the substance of inmates following. Detecting facts are consigned off a control society, place an extreme level monitoring request (MA) create it natural for both surroundings and distant customers to visualize the facts through a REST netting presidency. The fundamental proof of plan used to assert the urged SHS has proved that it has differing key capabilities and new details that are a main acquire from the rank of the craftsmanship.

Responsibility and non-repudiation in resource-constrained Internet of Things scenarios:
Brilliant programmed frameworks are turning out to be increasingly normal, so it means quite a bit to think of ways of ensuring their proprietors and individuals in control can be found. The objective concerning this paper search out examine the responsibility of Things and what they mean for the existences of things in a weighty style. These origins accompanying a counted flash at IoT characters like freedom, approachability, and inescapability. We express that Things that are forced by a chief should have a certain friendship between two together, what confirmation and non-retraction are meaningful pieces of all IoT circumstances that demand reliable cooperations. However, property maybe an issue. For instance, abundant Things are created to attempt supplies accompanying depressed capacity. Thus, we likewise recommend a method to demonstrate the way that we can ensure that elaborate Things are truly in a setting where there are no associations and scarcely any assets.

Integration of Agent-based and Cloud Computing for the Smart Objects-oriented IoT:
Later on Internet of Things (IoT), savvy things will be the essential makeup blocks for making mathematical real shining endless foundations in an thorough assortment of exercise domains, from first-contact medical care to conveyance, tasks to clever networks and city societies. Executing an IoT namely concentrated about famous belongings is a bothersome endeavor taking everything in mind the evidence that IoT parts accompanying miscellaneous standards of criticism and complication need to receive by agreeing each one, accompanying established arranged IT foundations, and accompanying human customers. In this paper, we recommend assembling Specialists and Cloud, which are two famous approaches to doing huge scope disseminated figuring that function admirably together. As far as multi-specialist frameworks, specialist-based registering can assist with making IoT frameworks that are decentralized, dynamic, open, and work together. Distributed computing can improve IoT things by giving them elite execution processing and a great deal of putting away space. Specifically, we present a cloud-helped and professional located IoT plan fated in near future created real by ACOSO, a doctor organized compute for clever parts that aid, and Body Cloud, a sensor-cloud foundation for gigantic opportunity sensor-located foundations.

3. METHODOLOGY:

However, trying this innovation raises a great deal of safety and protection worries that should be tended to before IoT innovation can be utilized on a major scale [8]. A method for halting DDoS assaults, which go through the transmission capacity of current Internet of Things (IoT) gadgets, is proposed to work on the digital protection of IoT gadgets and organizations [9]. Since these organizations are remote, self-designing, needn't bother with a previous framework, and have a ton of hubs that move around in capricious ways, security is one of the main things to ponder.

Disadvantages:

The security of the IoT is quite possibly of its most concerning issue, not its development.

The proposed strategy depends on the review and examination of transfer speed assaults, which generally center around DDoS, which is an extreme issue that is difficult to recognize and dials back the organization [10].

DDoS utilizes a gathering of guilty party hubs to focus on the person in question and prevent lawful clients from utilizing network administrations and assets [11].

Interruption anticipation frameworks in IoT gadgets are like "additional items" to the interruption discovery framework. They effectively battle against and stop goes after that are found by the IDS's observing cycles [12].

Advantages:

The projected era depends on the report that is to say created apiece IDS after it has examined the report from the determinable test.

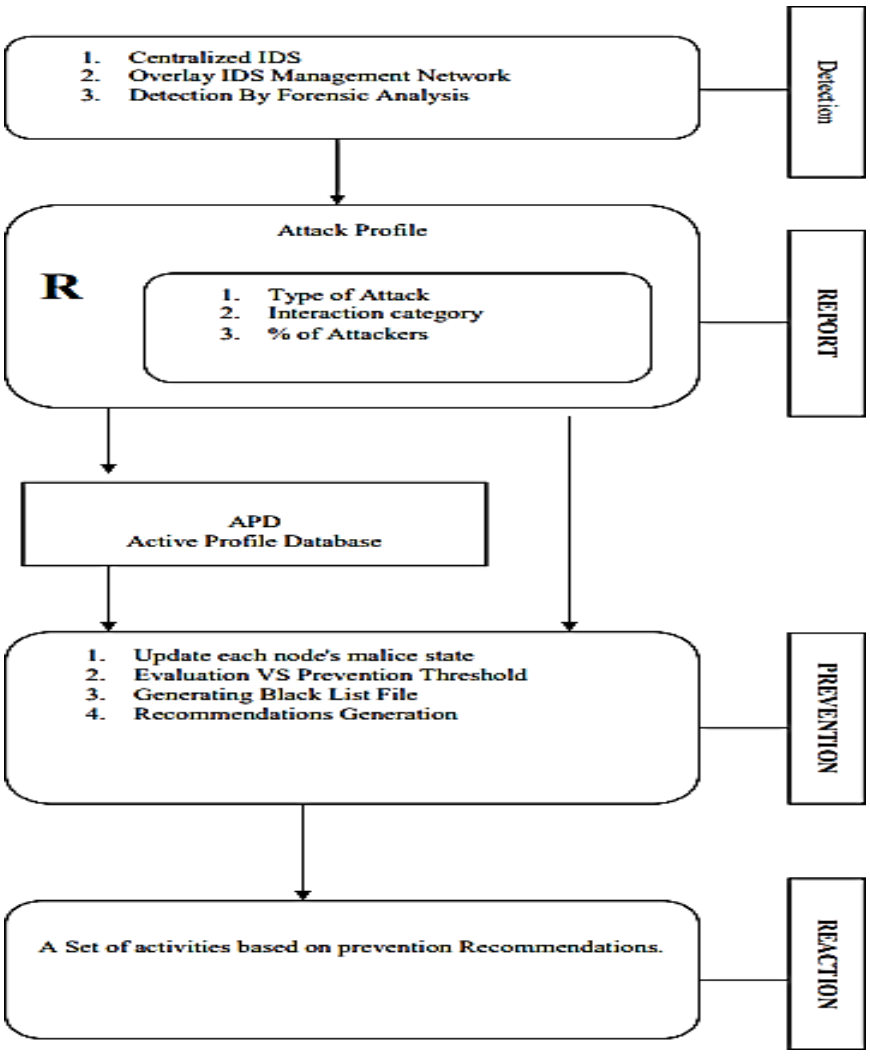

Figure 2 System Architecture

Algorithm:

Data Collection: Gather a dataset of network traffic data, where each data point represents a network event or communication session. Include relevant features such as source IP, destination IP, port numbers, packet counts, and timestamps.

Data Preprocessing: Prepare the dataset by cleaning and formatting the data. This may involve handling missing values, normalizing numerical features, and encoding categorical variables.

Feature Selection: Choose a subset of relevant features that are effective for distinguishing between normal network behavior and potential intrusions. This step helps reduce the dimensionality of the data and improve the efficiency of the SVM.

Labeling: Annotate each data point as either "normal" or "intrusion" based on historical data or domain knowledge. This step is essential for supervised learning with SVM.

Training Phase:

a. Split the labeled dataset into training and testing sets for model evaluation.
b. Apply the SVM algorithm to the training data, aiming to find a hyperplane that best separates the "normal" and "intrusion" data points while maximizing the margin between them.

Model Tuning: Adjust SVM hyperparameters (e.g., kernel type, regularization parameter) through cross-validation or grid search to optimize the model's performance.

Testing and Evaluation:

a. Use the trained SVM model to predict intrusion events on the testing dataset.
b. Evaluate the model's performance using metrics such as accuracy, precision, recall, and F1-score.
c. Fine-tune the model further if necessary.

Real-Time Intrusion Detection:

a. Deploy the trained SVM model in a real-time intrusion detection system.
b. Continuously monitor incoming network traffic and classify events as "normal" or "intrusion" using the SVM model.
c. Raise alerts or take appropriate action when an intrusion is detected.

Periodic Model Updates: Regularly retrain the SVM model with new data to adapt to evolving network threats and changes in network behavior.

Alert Handling: Develop a mechanism for handling and responding to alerts generated by the intrusion detection system, which may include logging, blocking, or notifying security personnel.

By applying the Support Vector Machine (SVM) algorithm in this manner, organizations can enhance data security by effectively identifying and responding to network intrusions. SVMs are known for their ability to handle high-dimensional data and find complex decision boundaries, making them a valuable tool in the field of intrusion detection.

4. EXPERIMENTAL RESULTS:

"IoT," an abbreviation for "Internet of Things," refers to small devices capable of transmitting or receiving data over the internet. These devices find applications across various fields such as healthcare (where doctors may implant IoT devices in patients' bodies or use them as wearable monitors to track vital signs and relay that information to a hospital server), agriculture, the military, and more. Powered by batteries, these compact devices require minimal infrastructure and can autonomously establish connections with neighboring devices for data exchange.

However, the inherent lack of a robust infrastructure (and the corresponding absence of human control) poses security risks for these small devices. Complex security measures are impractical due to their limited battery capacity. As a consequence, any attacker can potentially infiltrate these devices and access their data. Subsequently, malicious actions can be taken, such as masquerading as a legitimate device, intercepting data packets, dropping them, or flooding the network with fake packets to disrupt operations.

Two primary categories of attacks are insider attacks, where the attacker leverages information from a genuine node for nefarious purposes, and outsider attacks, where the attacker physically approaches a genuine node to engage in malicious activities. Given the impracticality of deploying intrusion detection systems (IDS) on these small devices, this paper introduces a straightforward concept called "LOG monitoring" to safeguard IoT devices. In this proposed method, two distinct types of nodes, namely Ordinary Hubs and IDS Hubs, collaborate.

Ordinary Hubs handle packet transmission and reception, while IDS Hubs monitor all network activities and generate reports.

These reports include the Hub ID, event type (indicating whether the nodes successfully transmit or drop packets, discernible by receiving acknowledgments from the nodes), and timestamp. The generated log reports are sent to a central STATION, which analyzes them to identify well-behaving and malicious nodes. Based on this information, the STATION isolates IoT nodes engaging in malicious activities from the network.

If an attacker node drops or interferes with a higher number of packets than a specified threshold, it is classified as a malicious actor and dealt with accordingly."

To set this undertaking in motion, I created a model and a generator that can make both norm and IDS hubs.

To begin this undertaking, double tap the 'run.bat' document to get to the underneath screen.

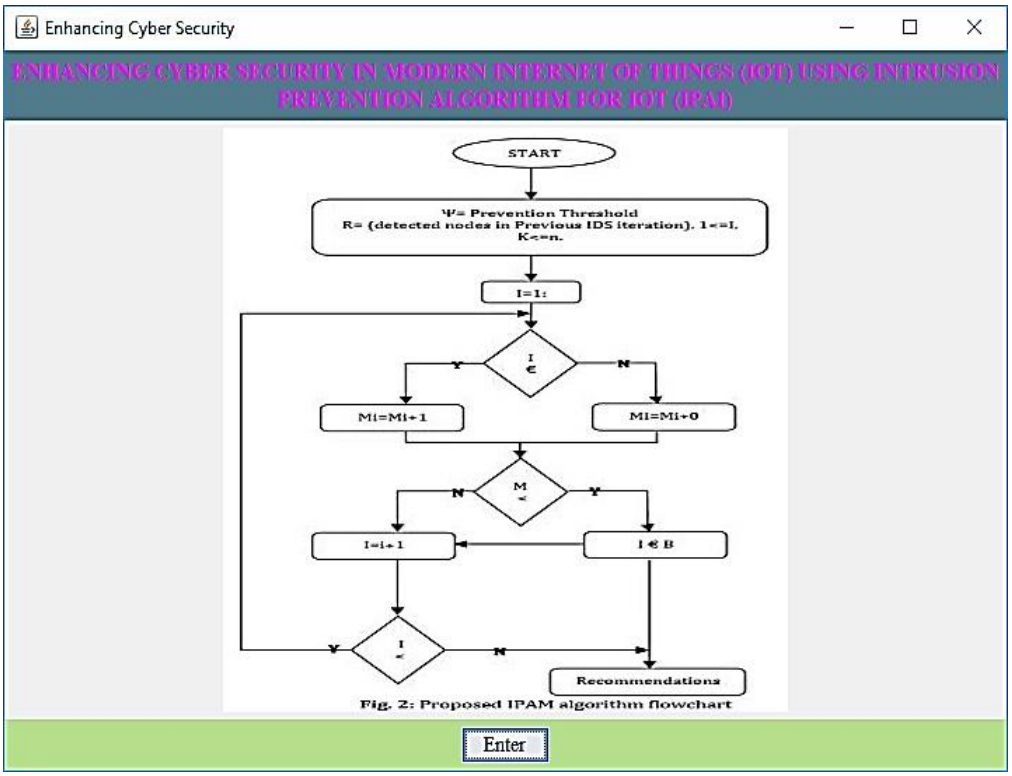

Figure 3: Click on enter button.

Click the "Enter" button on the screen above Fig 3 to get to the screen beneath.

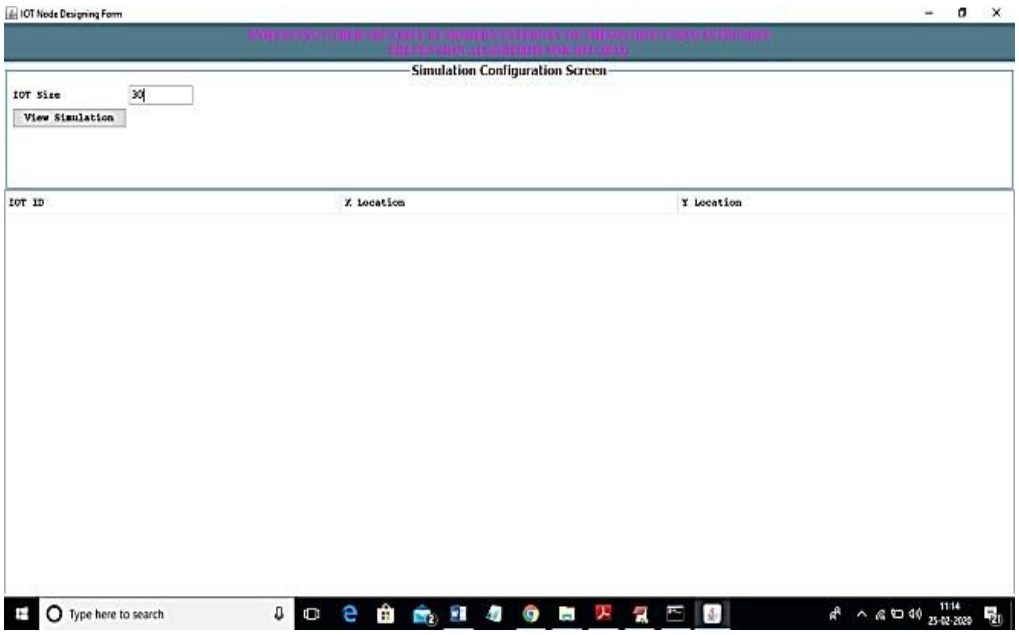

Figure 4: The screen depicts to enter the IOT size for recreation.

On the screen above Fig 4, enter the IOT size for recreation. On the screen above, I entered 30 for the IOT size. Presently, click on the "View Reenactment" button to see the screen underneath.

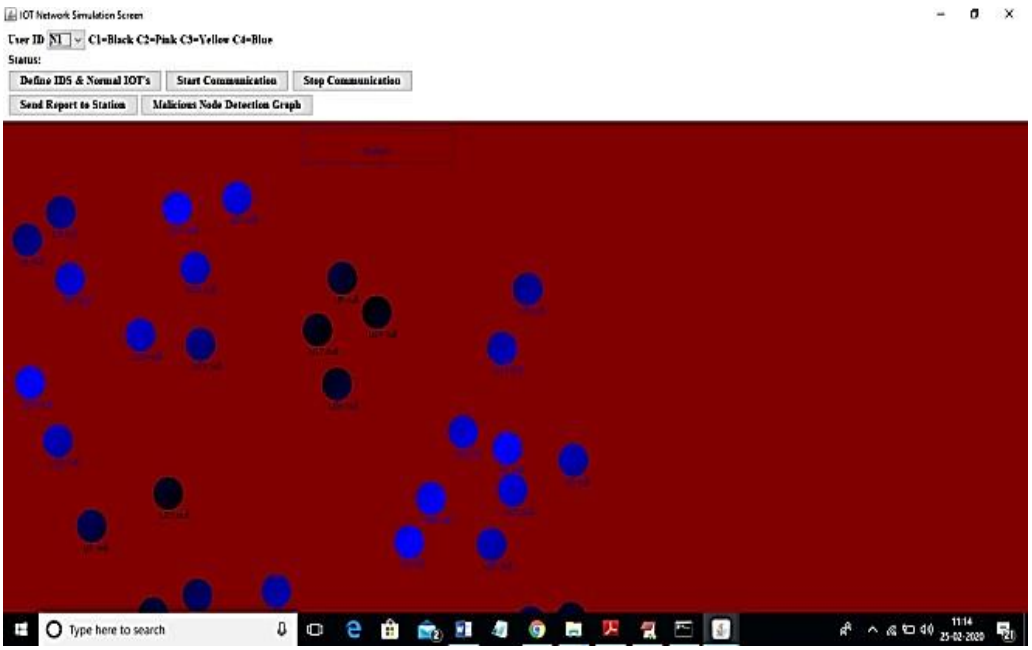

Figure 5: Displaying IOT gadgets.

On the screen above Fig 5, we can see that each of the 30 IOT gadgets are in better places. Consider each circle one IOT contraption. Presently, click the "Characterize IDS and Typical Iot's" button to make a few hubs IDS and different hubs ordinary. I'm making IDS hubs out of the multitude of hubs that are nearer to STATION so they can send LOG Reports to STATION.

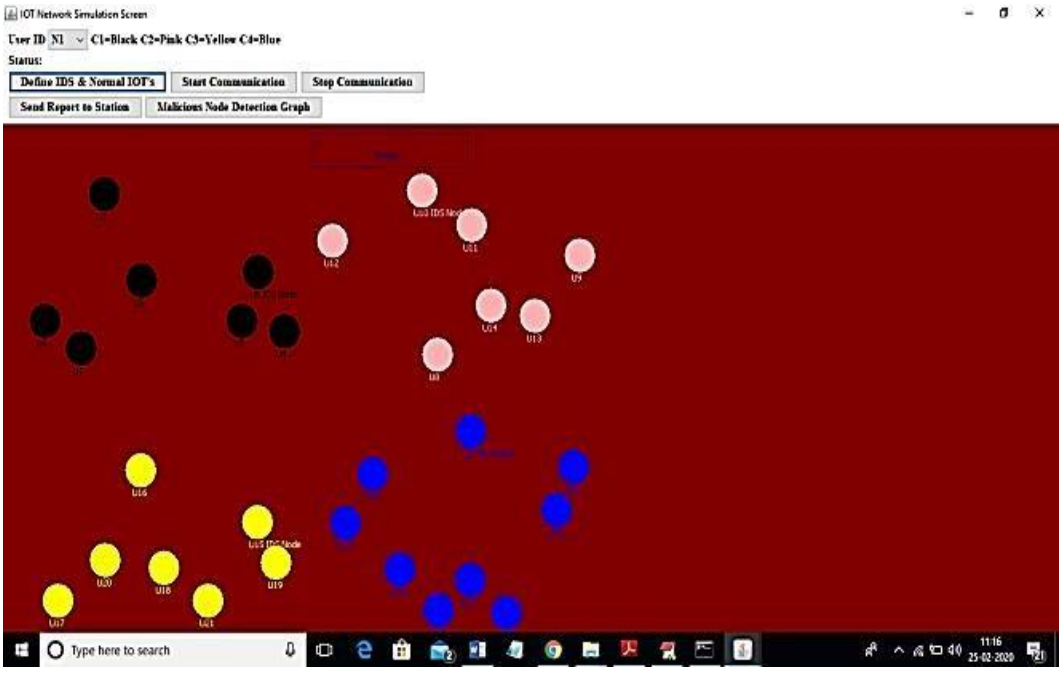

Figure 6: displaying various kinds of IOT.

On the screen above Fig 6, hubs with IDS will have an IDS mark, while hubs without IDS will just have a name. See the last screen to find out where everything is in X and Y. See the screen beneath.

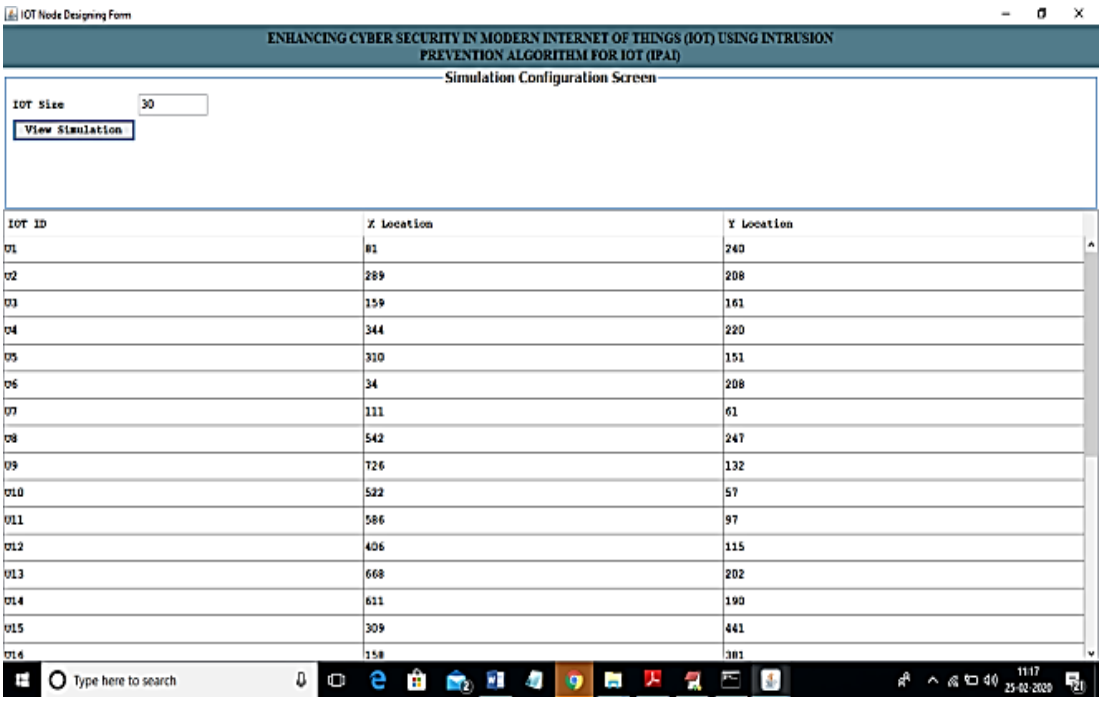

Figure 7: Tabulated data information.

The above screen fig 7 displays the Presently, return to the past screen and snap on the "Start Communication" button to send and get information between the arbitrarily picked source and target.

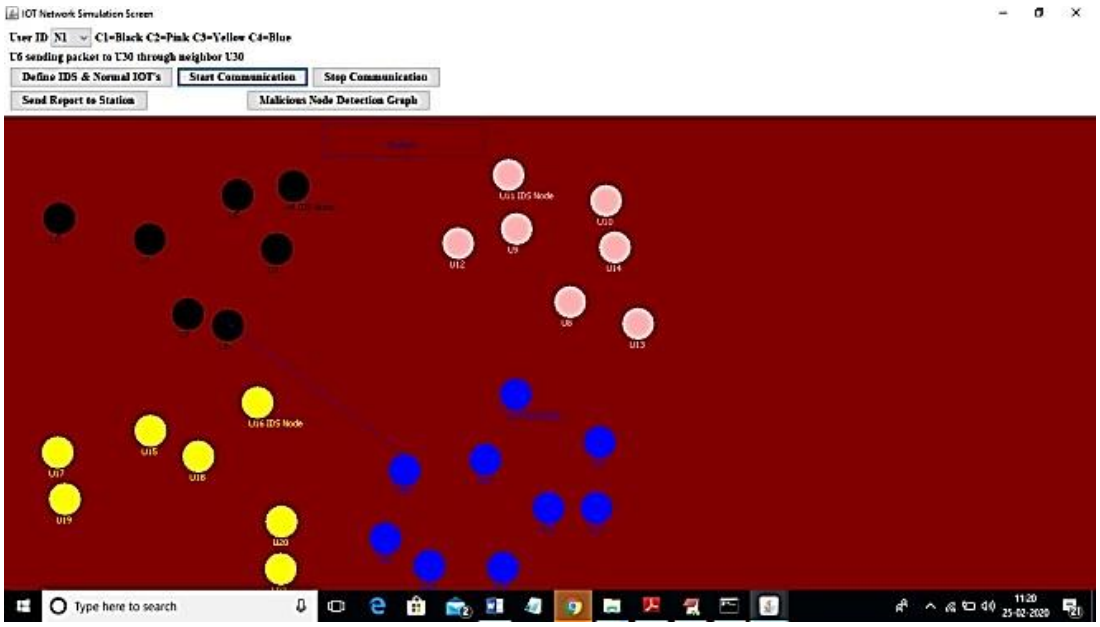

Figure 8: Displaying IoT.

On the screen over Fig 8, the blue line between two hubs shows that information is being sent between them. Assuming the line goes down, it implies that the hub close to it is dropping bundles. Here, I'm letting some know hubs to drop a few parcels to carry on like foe hubs, and STATION will actually want to track down them by checking the report out. You can stop gearbox by tapping on the "Stop Recreation" button. Presently, click the "Send Report to Station" button on every IDS hub to send the report to the base station.

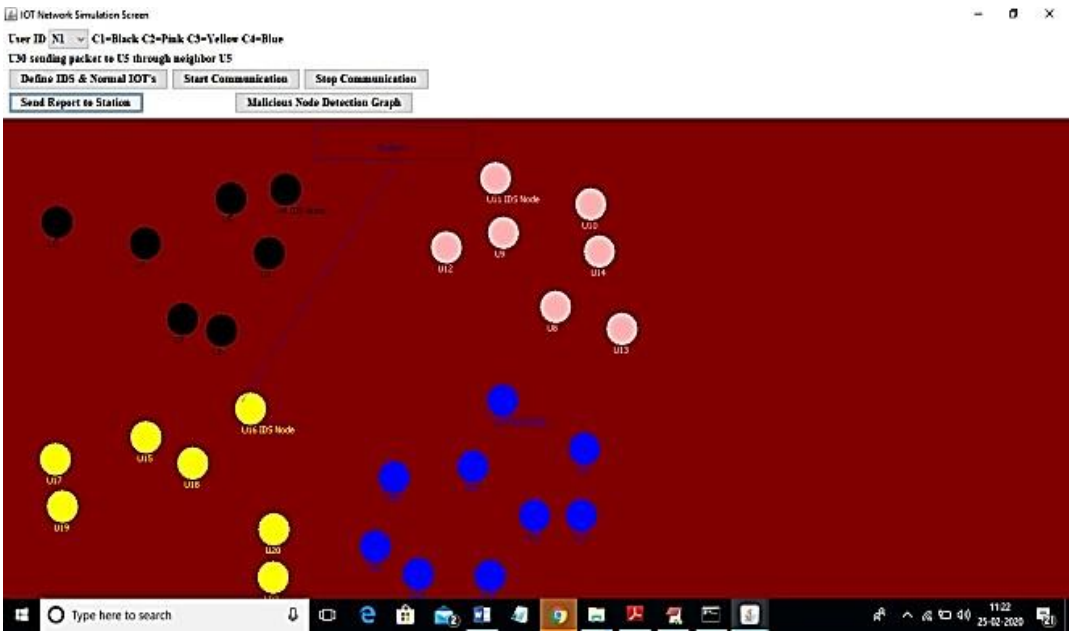

Figure 9: The IDS sending report to primary station.

On the screen over Fig 9, every IDS will send a report to the primary station, and we can see the lines of contact between them. Presently, click the "Malicious Node Detection Graph" button to see which hubs are ordinary and which are aggressors.

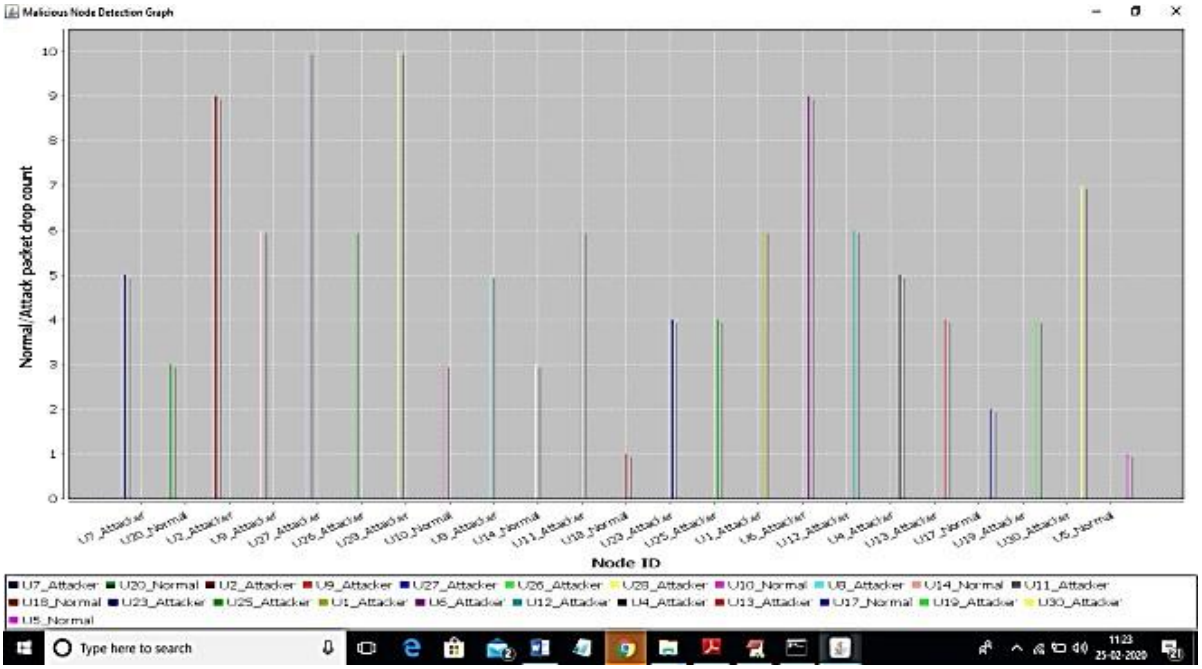

Figure 10: graphical representation of x-pivot & y-hub graph.

In the above picture Fig 10, the x-pivot shows the hub ID and the y-hub shows hub movement, for example, the quantity of parcel drops or sticks. I kept hindrance at 3 here. On the off chance that a hub gets rowdy by dropping or sticking multiple times, it will be viewed as an assailant.

5. CONCLUSION:

The size of Distributed Denial of Service (DDoS) attacks and the resultant damage they inflict have increased as the number of attack sources has grown. This development has simplified the ability for malicious actors to compromise the security and performance of IoT technology. The impact of such an attack and its frequency can disrupt network operations, rendering it impossible for legitimate users to access network services. In this piece, we delve into potential security strategies and propose an effective approach to thwarting DDoS attacks in IoT networks that are susceptible to them. Leveraging the foundational structure and responsibilities of contemporary Intrusion Detection Systems (IDS), we have devised the recommended algorithm to yield results that correlate with time. The proposed evasion algorithm entails a blacklist table that can be concurrently updated and modified based on the currently available information. Implementing this approach can lead to the generation of recommendations for the response module, thus enhancing network security, ensuring its resilience against attacks, and preserving its operational integrity.

6. REFERENCES:

[1] T. A. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," in IEEE Access. doi: 10.1109/ACCESS.2018.2876939 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8519613&isnumber=6514899

[2] Ahamad Ahanger, Tariq. (2018). Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. International Journal of Computers Communications & Control. 13. 915-926. 10.15837/ijccc.2018.6.3356.

[3] K. Rose, S. Eldridge, and L. Chapin, “THE INTERNET OF THINGS: AN OVERVIEW, Understanding the Issues and Challenges of a More Connected World,” 2015.

[4] R. H. Weber, “Internet of Things – New security and privacy challenges,” Comput. law Secur. Rev., vol. 26, pp. 23–30, 2010.

[5] IEEE, “Towards a definition of the Internet of Things (IoT),” 2015.

[6] L. Catarinucci et al., “An IoT-Aware Architecture for Smart Healthcare Systems,” IEEE, 2015.

[7] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.

[8] E. Oriwoh, H. M. al-Khateeb, and M. Conrad, “Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios,” in Conference: Conference: International Conference on Computing and Technology Innovation, 2015.

[9] G. Fortino, A. Guerrieri, C. Savaglio, and W. Russo, “Integration of Agent-based and Cloud Computing for the Smart Objects-oriented IoT,” researchgate, 2014.

[10] V. Dastjerdi and R. Buyya, “Fog Computing: Helping the Internet of Things Realize Its Potential,” IEEE, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[11] H. Lin and N. W. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” MDPI, 2016.

[12] R. Petrolo, V. Loscri, and N. Mitton, “Towards a Smart City based on Cloud of Things,” Int. ACM MobiHoc Work. Wirel. Mob. Technol. Smart Cities, 2014.