RESEARCH ARTICLE OPEN ACCESS

A Performance Comparison on DoS and DDoS attacks in Internet of Things

S.chithra [1], Dr.R.Kalaiarasi[2]

[1], [2] School of computer science,TNOU,Chennai – India

ABSTRACT

Distributed Denial-of-Service attacks are the terrorization audition on the internet that diminishes the network bandwidth. Internet-of-Things (IoT) is an pioneering technology that is used to connect plenty of tiny electronic devices and gadgets with the internet in a cost-effective way. IoT engages a hefty number of interconnected devices, together with household appliances, public facilities, wearable equipment, medical equipment, unmanned aerial vehicles, and interconnected vehicles as well as other applications that necessitate networking. Topical DDoS attacks have naked that ambiguities are omnipresent in IoT, which is still in the initial stage. Without security defense, the enormous majority of IoT devices may inadvertently become accessory to DDoS attacks. This paper investigates about Distributed Denial of Service attack, and various methodologies for preventing IoT devices from DoS attacks and algorithm for preventing the devices from the attacks.

I. INTRODUCTION

Internet of Things exploited for manufacturing or small industry is considered as Industrial Internet of Things [1]. The continuous improvement of Internet of Things and raising applications in various fields, the nature or approach of attacks DDoS and DoS attacks are sprouting and necessitate for enhanced approach to their detection and alleviation. DDoS attack impact the accessibility of data at end users as attackers can be hidden by making detection of DDoS very difficult [2].To accomplish the triumph of Internet of Things; it is indispensable to widen advanced mechanisms capable to ensure suitable security levels to perceive cyber-attacks and alleviate cyber-threats on every occasion occur in the cope IoT network. This pretenses a great confront as IoT devices may knob perceptive information and many viable IoT low-end devices do not habitually sustain strapping security mechanism , building them uncomplicated intention to kowtow the malicious network of devices for diverse attacks such as DoS and DDoS (Distributed Denial of Service) [3] [4]. The cross-layer heterogeneous IoT devices communication with issue of numerous attacks analyzed [5][[6][7]. Even though these challenges occur in other environments, their brunt can be more detrimental in the IoT environment, which is troublesome as it facilitates intruders to infiltrate the environment.

These attacks may lead to financial loss in IoT used organization. Furthermore, existing literature source have not focused on data exhilarations caused by Distributed DoS and DoS attacks.

For this reason, LEACH is designed to overcome the issues of the various attacks and for designing the IoT environment with more security. Due to DDoS and DoS, Data exfiltration raised in the IoT environment without the owner's consent has happened [8][9][10][11]. The following diagram

(Fig:1) represents the DDoS Attacks in Internet of Things. The table 1.1 shows the various attacks in Wireless Sensor Network and Internet of Things.

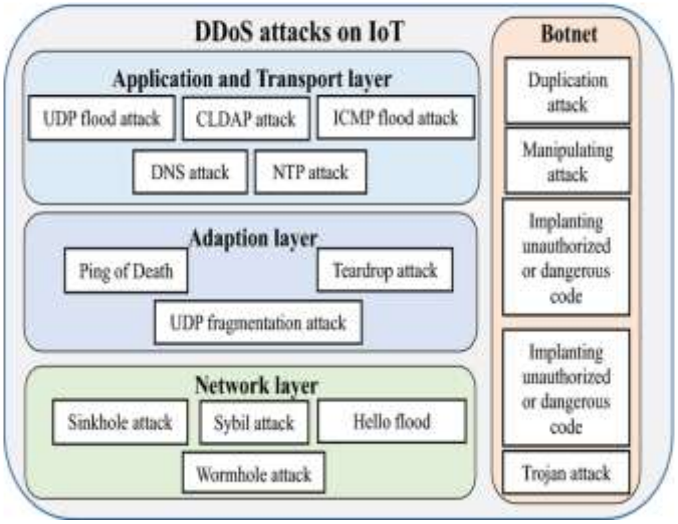


Figure: 1 DDoS Attack in Internet of Things

Table 1.1 DOS ATTACKS based on LAYERS
Attack and Activity of the attack at Physical and Datalink Layer

Sr.No	Name of the Attack	Activity
1	Congestion	Prevention of reading RFID tag
2	Immobilize	Disconnection of data raised by tags disability
3	Wide-band Denial & Pulse Denial	obstruct the entire Radio Frequency spectrum causing by DoS
4	De-Synchronizing	Permanent disabling of RFID tags
5	Node-Specific and message specific Denial	Hijacking of legitimate launching information for specific attacks

Table 1.2 Attack and Activity of the attack at Network Layer

Sr. No	Name of the Attack	Activity
1	Flooding Attack	Authentication of user's resources disrupted by the attacker
2	Reflection - based flooding Attacks	Attacker propel malevolent request by employing Botnets, thereby fatiguing victim's resource and making it Intricate to block the attacker.
3	Amplificatio nAttacks	Incoming traffic raised by the Attacker genuine application.

Table 1.3 Attack and Activity of the attack at Application Layer

Sr. No	Name of the Attack	Activity
1	Re-programming Attack	Infinite loop making raised by the Attacker
2	Pathbased DoS	Attacker barrage the devices with counterfeit packets on Communication paths

II. EXISTING METHODS

Existing methods explain various methods and algorithms for tracing and mitigating the attacks against Denial of Service. There are eight different categories of methodologies are available as now. Some of the prominent exiting methodologies are Detection and Mitigation of DoS and DDoS Attacks in IoT-based Stateful SDN : An Experimental Approach [12][13][14]. A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach[14], Towards Detection of DDoS Attacks for Next –Gen Industrial Internet of Things[15], DDoS Attack in IoT: Vulnerabilities and Mitigation Techniques[16] , Performance Analysis of Denial of Service and Distributed DoS attack of Application and Network layer of IoT[17][19], Detection and Prevention Algorithm of DDoS Attack over the IOT Networks[18] A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing[20], SDN Based DDoS Mitigating Approach Using Traffic Entropy for IoT Network[21]. Since the research topic of Protection Mechanism for IoT-private cloud against DoS and DDoS attacks is relatively new, there are limited numbers of articles found through the sources and they are mentioned above.

2.1 Detection and Mitigation of DoS and DDoS Attacks in IoT-based Stateful SDN: An Experimental Approach (DMSDN-IoT)

In this paper, Stateful SDN security resolution for real IoT traffic that can perceive and mitigate DoS and DDoS attacks pedestal on the perception of entropy as the detection method. Entropy based protection of network against DoS attack has three stages which are Traffic/Flow monitoring, Anomaly Detection and Mitigation. The switch monitors the flows but the detection of the malicious flows done by the controller. First stage of the entropy is monitoring the network to obtain the information about the network, implementing the detection algorithm based on the entropy calculation algorithm. The switch maintains the flow and state tables. This approach allows obtaining the required information to detect a DDoS attack because the switch can count the exact number of events for a traffic distinguishing monitored, increasing the precision of the algorithm. Second stage is detection algorithm which is based on the equation

$$H(X) = -\sum_{i=1}^{n} p(x_i) \frac{\log_2 p(x_i)}{\log_2 n}$$

Where p(x_i) connotes the possibility of the event xi, and n represents the number of events. To analyze the traffic, an initial learning segment isrequired to feed the algorithm, scheming the entropy and the limits of the distribution, defined by the equation 1.

Limits are calculated as:

$$\text{limits} = \mu \pm \theta\sigma$$

Third stage is Mitigation; the mitigation mechanism preserves end-users when a malicious attack is detected. The meticulousness of the mitigation convention depends on the quantity of information of the attack can be attained. The controller configures the rules in the switches using OpenFlow ordinary messages, sending messages FlowMod. Intrusion Detection System and Advanced procedures and methodologies are used to mitigate the attacks. The following diagram represents the flowchart of the Algorithm.

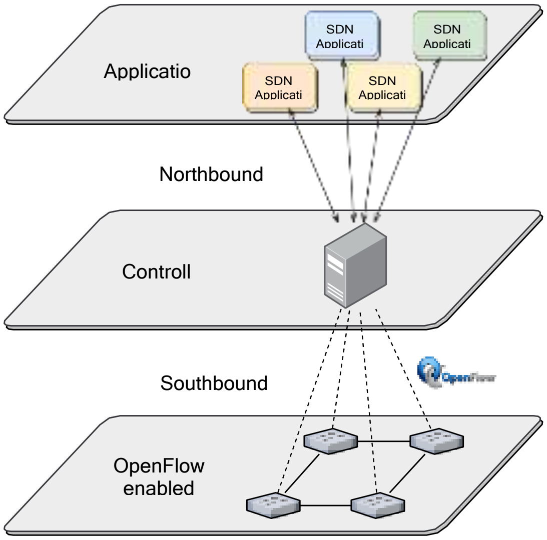
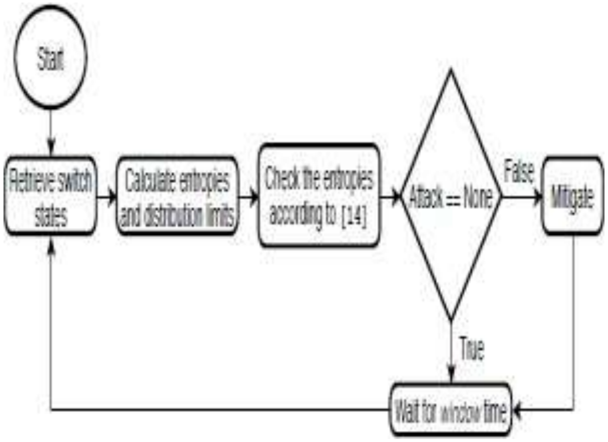


Figure: 2.1 Software Defined Network Architecture

Figure: 2.2 Algorithm Flowchart


Start
Retrieve switch states
Calculate entropies and distribution limits
Check the entropies according to [14]
Attack == None
False
Mitigate
True
Wait for window time

2.2 A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach [FMDEHA]

This work introduced enhanced Low-Energy Adaptive Clustering Hierarchy (LEACH) and which is used to provide the security and improve the IoT network lifetime, energy consumption, and throughput in order to mitigate DDoS and DoS attacks in the IoT setting. The proposed approach was divided into three steps. First stage is preprocessing phase. In this stage, random key is used to diminish attacks by intruders, particularly DDoS and DoS attacks. The cluster head also elected by the similar random keys. The elections of the key depend upon the distance and signal of the nodes. The random key aimed to secure the communication. Second stage is cluster head selection, The LEACH algorithm has two phases. First phase is Setup and second is Steady phase. In the setup phase, The cluster formed with numerous number of nodes, and the cluster head (CH) was also selected. Each node in the cluster could potentially be selected as the CH through a process of engendering a random precedence value between 0 and 1. For instance, if the number for the member node is less than the threshold assessment $T_{(n)}$, then the node will robotically be the CH. Whereas, if the value of the threshold $T_{(n)}$ is given by Equation (1), then the CH is responsible for assigning the TDMA schedule for the particular corresponding cluster members.

$$T_n = \frac{1}{1-p\ (r \bmod 1/p)} \qquad \forall n \in$$

Where ρ is the proportion of the sensor nodes that would be CH, r donates the existing round.

The mitigation of the attack between the FU and FS is achieved by determining the $FU - FS$ secret key $K_{FS}{}^{Fu} = H(ID_F, ID_{FS}, kFu)$ which is utilized for encrypting and decrypting the session key K_s, $E\ K_{FS}{}^{(Fu)}$, (r,FS,K_s) *by Fu and D* $K_{FS}{}^{(Fu)}$, $K_{FS}{}^{(Fu)}$, (r,FS,K_s) *by FS.*

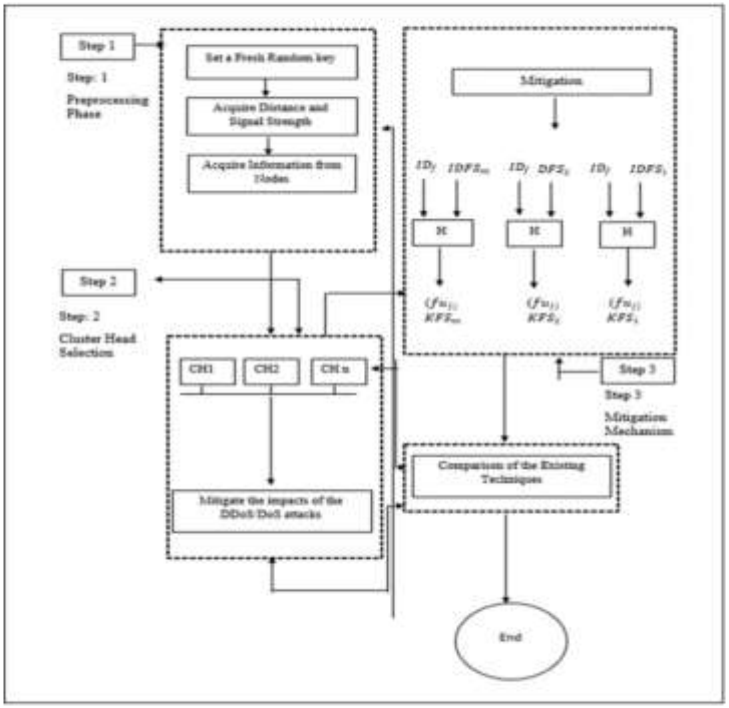


Figure: 2.2 Proposed Hybrid Method

2.3 Towards Detection of DDoS Attacks for Next – Gen Industrial Internet of Things [TDDIIT]

In this work, base station is conscientious for propagating traffic and architecture differentiates the traffic as 0 and the attack is 1. Enormous correlation of devices for the industrial scenario or IIoT is portico with security issues. Deep Neural Network developed the detection system with accuracy of 96%.

2.4 DDoS Attack in IoT: Vulnerabilities and Mitigation Techniques [DIOTV]

In this work provides an assortment of security facet of IoT setup and proposes security elucidation for Mitigation. It provides enhanced security access to IoT devices against DDoS attacks. This system includes two types of users which are admin user and IoT user. Admin user can access framework1 and framework 2. IoI user can access framework3. Secret keys are used to access the frameworks. Layer seven of the OSI model operated the proposed security design by using unique URL**.** It uses one skeleton at a time thereby limiting the resource and memory requirements. The proposed scheme used SHA 256 algorithm for encryption which is light weight security methodology. This following diagram [2.3] represents the secure communication system using Framework structure. Using the framework admin user and IoT user reacts against the DoS attacks based on the secret key.

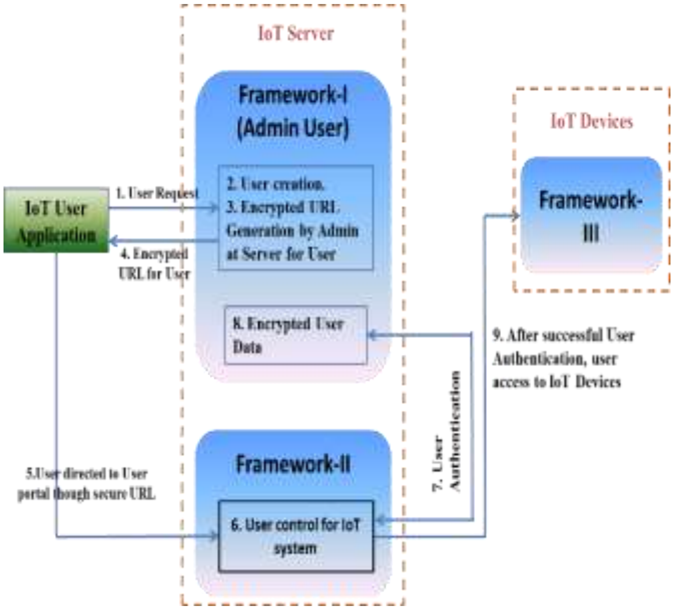

IoT Server
Framework-I (Admin User)
2. User creation.
3. Encrypted URL Generation by Admin at Server for User
8. Encrypted User Data
IoT Devices
Framework-III
IoT User Application
1. User Request
4. Encrypted URL for User
5.User directed to User portal though secure URL
Framework-II
6. User control for IoT system
7. User Authentication
9. After successful User Authentication, user access to IoT Devices

Figure: 2.2 Framework Structure

2.5 Performance Analysis of Denial of Service and Distributed DoS attack of Application and Network layer of IoT [PADAN]

The proposed research work introduced Distributed Denial of Service attack algorithm. In this DDoS attack, the network traffic arrives from different attacking sides. The solution for this attack is blocking single IP address makes it not probable to thwart the attack. In typical DDoS attack, the aggressor started through exploiting a susceptibility in one system and by creating it the DDoS master .The master attacking system concedes diverse exposed systems and gained management on them either by infecting different systems through bypassing the authentication controls that's by approximation default parole on a wide used device or with malware. A system or a networked device underneath the management of an attacker is understood as a bit or a zombie. botnets master controls a larva net. Botnets will comprise any range of bots; in botnets, there's no higher limit to their size as a result of, in present days DoS are also exemplified by the method that the attack uses.

2.6 Detection and Prevention Algorithm of DDoS Attack over the IOT Networks [DPAD]

This research paper provided the detection and prevention algorithm against DDoS attack. This work suggested two parts which are for detecting the DoS attack in the IoT devices and other mitigating the impact of DDoS attack. It provides the architecture of DDoS Defense Architecture. The Hybrid Defense methodology is utilized in proposed DDoS defense works. The two algorithms

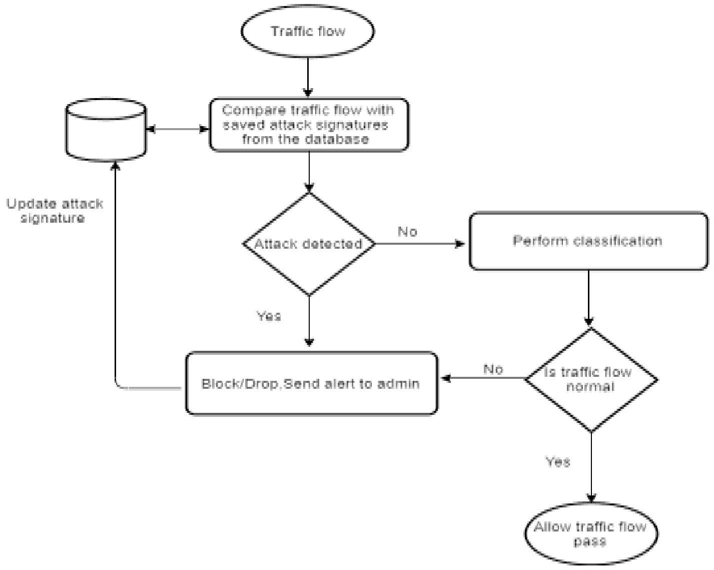


Figure: 2.3 Block diagram of KNN

collaborate with each other to accomplish best defense approach where the detection algorithm is distributed in excess of the End-nodes (victims) to distinguish the attack and discriminate attack type. Then, it will throw a warning to the mitigation algorithm which is established on the scrutinize agent to mitigate the blow of the DDoS attack. The boundary router and gateway of the IoT network supervised by the software based agent. PDDA algorithm detects the arriving traffic whether which is normal or DDoS traffic and also detect whether the attack rate is high or low. PDDA propel the caution message enclosing with the address of the attacker, port number and the type of the attack to monitor agent. PDDA utilized a table for counting the received packets from every client throughout a predetermined time called detection time.

2.7 A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing [DAMFF]

This research paper suggested DDoS mitigation skeleton for IoT using Fog computing to assured accurate DDoS detection. The Intrusion Detection Method is used to alleviate the attacks. The detection scheme utilizes a K-Nearest Neighbors (K-NN) classification algorithm for perceiving the DDoS attacks. The operational procedure suggested which is used to scan the network traffic against attack signature, If an attack is discovered, the flow is blocked/drop and an alarm is sent to the administrator. Otherwise, the traffic flow is agreed through a classifier. The classifier discriminates between the normal and abnormal network traffic flow by comparing the traffic flow with a model of a normal traffic flow formed. Normal traffic flow is allowed to pass into the IoT network, on the other hand, an abnormal network traffic flow is considered as an attack. Hence, it is blocked or dropped, an alarm will send to the administrator. The signature of the abnormal traffic is updated in the database to ensure an up-to-date database. This will ensure a faster response when the same attack is performed in the future. The DDoS mitigation framework utilizes a K-Nearest Neighbors (k-NN) classification algorithm [22] for the detection of DDoS attacks due to its simplicity, efficiency, and accuracy in classification [23]. Although, K-Nearest Neighbors (K-NN) algorithm has been utilized for DDoS detection in traditional networks , intrusion detection in Wireless Sensor Networks (WSN) [24] and detecting attacks such as U2R and Remote to Local attacks in IoT networks [25][26]. We employ K-Nearest Neighbors (K-NN) on the fog for DDoS attack detection in IoT networks. The K-Nearest Neighbors (K-NN) classifies unknown databy observing the k data points in a training set that are near to it in the input space. Thus, it requires a distance measurement technique like Manhattan or Euclidean distance measuring technique [27]. The diagram 2.3 shows the basic operation of the K-Nearest Neighbors Algorithm

2.8 SDN Based DDoS Mitigating Approach Using Traffic Entropy for IoT Network [SDNMTE]

SDN based Entropy model introduced Block chain Enabled Protocol. It consists of two components SEN and SND controller [28]. Inbound traffic received by SEN module with the help of packet capturing module. Inbound and outbound traffic calculated by entropy calculation. Block chain stores the entropy information and correlation of entropy information. Using the language of Python3, BEP protocol is defined. The protocol defined that the rules for transmission of data and block. BEP is an application layer protocol works based on client server model. The following diagram 2.4 represents the SDN (BEP-SEN) scenario.

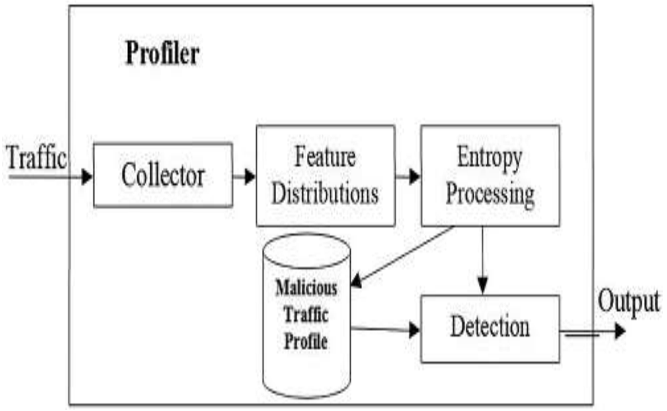


Figure: 2.4 Workflow of Traffic

Comparison of Existing Research methodologies and Performance metrics

S.No	Title	Author & Year	Protocol	Algorithm/ Techniques	QoS Parameters	Method Used	Protocol Performance	Issues/ Future Enhancement
1.	**DMS DN-IoT**	Deepak Chouhan,Lokesh Parashar	Entropy based Algorithm	Entropy based algorithm for detecting and mitigating DoS and DDoS attacks in IoT Scenerio	1.Throughput 2.Entropy variation for DDoS attack	1. Monitoring 2.Detecting Mitigating	**Entropy mechanism is developed the Open State method, that exploits in-switch competence and has been proved to be a promising approach for network monitoring attacks**	**Different statistical methods necessitate to detect the protect the IoT Devices**
2.	**FMD EHA**	Abdulrahman Aminu Ghali, Ahmad and Hitham Alhussian	1.Random key 2.LEACH protocol 3. Data exfiltration	1.Pre processing phase 2. Cluster head selection based on LEACH protocol 3. Mitigation	1.Energy Consumption 2. Improved network lifetime 3.Throughput	Pre processing phase	First stage is preprocessing phase. In this stage, random key is mitigating that attacks occurred by intruders, especially DDoS and DoS attacks. The determination of the key depends upon the detachment and signal of the nodes. It follows LEACH protocol algorithm to find the cluster head.	Various algorithms needed to reduce the DoS and DDoS attacks of Data exfiltration

							Mitigation mechanism leads to data exfiltration	
3.	**TDDIIT**	Gabriel Chukwunonso Amaizu, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim	Deep Learning Approach model	1. Deep Neural Network 2.Detection Framework	1.Accuracy 2.Data Loss	DNN Model	**The DNN model performed based on the accumulation of data in the base station.** All the network traffic is sent through base station. When the traffic gets to the base station, the detection model ensure for any DDoS attacks in real time	To pigeonhole each individual DDoS attack and also attain a higher detection accuracy
4.	DIOTV	Sanjay Kumar Gupta Sandeep Vanjale	Multilevel Cryptographic Hash function based Security Framework for Internet of Things	Framework1 Framework2 Framework3	CPU utilization Execution Time Thermal Analysis	MCHSFIOT	It consists of Admin user and IoT user. Admin users access Framework 1 &2 IoT user access the Framework3Security keys are used to obtain the frameworks .	This attempt has been achieved by theoretically. The same may be evaluated y practically. To develop algorithms to achieve the secured network devices against DDoS attack
5.	**PADAN**	Hanumat Prasad Alahari, Suresh Babu, Yelavarthi	DDoS Algorithm	It provides the algorithm to secure the servers	Distributed Denial of Service algorithm prevents the servers from the crashes	It provides routing path ,Delay and loss of packets	It prevents server from crashes when it overloaded with many users data	Algorithms needed to accomplish the better results in QoS

6.	**DPAD**	Mohammed Ridha Nsaif , Mohammed Falah Abbood , Abbas Fadhil Mahdi	PDDA and PDMA Algorithm	It suggests the algorithm to secure the network	Proposed Defense DDoS Algorithm Proposed DDoS Mitigation Algorithm	**PDDA maintains a storage as table for calculating the each client's packets at a particular time.** **It maintains three tables : WhiteList, GreyList and BlackList**	The proposed proceed includes two algorithms, one for detection of the attack and the other is to mitigate the collision of DDoS.	To discover different algorithms to protect the IoT network from DDoS attackers
7.	**DAMFF**	Muhammad Aminu Lawal [1], Riaz Ahmed Shaikh, Syed Raheel Hassan	K-NN Classification Algorithm	The algorithm provides the algorithm to secure the network against DDoS attack	K-NN Algorithm	Binary Classification False positive rates of the classifiers	The k-NN classifies unknown data by observing the k data points in a training set that are near to it in the input space. Thus, it necessitates a distance measurement performance like Manhattan or Euclidean distance measuring technique	To provide the framework on available fog computing platforms to further to evaluate the approach

8.	**SDN MTE**	Muhammed Ibrahim, Muhammed Hanif, Shabir Ahmad	BEP Protocol	BEP has two components SEN and SDN controller	BEP based Client/Server Model	Self Exposing Nodes Blockchain Enabled Protocol	SEN accepts the incoming traffic BEP stores the traffic data and compares with entropy calculated values The two modules helped to trace the botnet	Need to develop the algorithm for detecting the botnet and botnet's controller

III. CONCLUSION

DDoS is a cyber-attacks which affected the service by disrupting the facilities of a resource temporarily or permanently. Security protection has motivated intruders to perform serious attacks on the IoT devices. These attacks are leading financial loss and data filtration. This is main challenge to the researchers. In future, intend to develop many algorithms and scenario to prevent the network and nodes from DoS attacks with balanced energy and battery life of the nodes.

REFERENCES

1. N. B. Long, H. Tran-Dang and D. Kim,"**Energy-Aware Real-Time Routing for Large-Scale Industrial Internet of Things**," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2190-2199, June 2018, doi: 10.1109/JIOT.2018.2827050.
2. R. Abubakar et al.,"**An Effective Mechanism to Mitigate Real-time DDoS Attack Using Dataset**," in IEEE Access, doi: 10.1109/ACCESS.2020.2995820.
3. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, "**A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoTDevices**". IEEE Internet Things J. 2019, 6, 8182– 8201. [CrossRef]
4. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7
5. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. "**Security of the Internet of Things: Perspectives and challenges**". *Wirel. Net.* **2014**,*20*, 2481–2501. [CrossRef]
6. Patel, C.; Doshi, N. "**Security Challenges in IoT Cyber World**". In Proceedings of the International Conference TRANSBALTICA, Vilnius, Lithuania, 2–3 May 2019; pp. 171–191.
7. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. "**Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges**". *Futur. Gener. Comput. Syst.* **2019**, *92*, 265–275. [CrossRef]
8. azi, H.H.; Gonzalez, H.; Stakhanova, N.; Ghorbani, A.A. "**Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling**". Comput. Networks **2017**, 121, 25–36. [CrossRef]
9. Smith, T.; Aznarez, O.; Tsarou, A. "**The Dangers of Underestimating DDoS Attacks**". Available online: https://www.corero.com/ blog/the-dangers-of-underestimating-ddos-attacks/ (accessed on 4 February 2021).
10. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. "**Internet of things (IoT) security: Current status, challenges and prospective measures"**. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
11. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. **A Review of Security in Internet of Things**. Wirel. Pers. Commun. **2019**,108, 325–344. [CrossRef]

12. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. **Internet of Things security: A survey**. J. Netw Comput. Appl. **2017**, 88, 10–28.

13. Deepak Chouhan,Lokesh Parashar, "**Detection and Mitigation of DoS and DDoS Attacks in IOT-based Stateful SDN: An Experimental Approach**", International journal of Science,Engineering and Technology , ISSN No:2348-4098,An open Access Journal, 2020**.**
14. **https://www.temjournal.com**
15. Abdulrahman Aminu Ghali *, Rohiza Ahmad and Hitham Alhussian,"**A Framework for Mitigating DDoS and DoS Attacks in IoT Environment using Hybrid Approach**" in Hybrid Approach. *Electronics* **2021**, *10*, 1282. https://doi.org/10.3390/ electronics10111282.
16. https://www.mdbi.com
17. Gabriel Chukwunonso Amaizu, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim," **Towards Detection of DDoS Attacks for Next-Gen Industrial Internet of Things**", Korean Institute of communications and Information Sciences, Summer conference pp.1230-1231, Vol-72, August 2020
18. Sanjay kumar Gupta, Sandeep Vanjale**,"DDoS Attack in IoT: Vulnerabilities and Mitigation Techniques",** International Journal of Engineering Research in Computer Science and Engineering, ISSN.No : 2394-2320,Vol 8, Issue 3, March 2021
19. Hanumat Prasad Alahari, Suresh Babu, Yelavarthi , " **Performance Analysis of Denial of Service (DoS) and Distributed (DDoS) attack of Application and Network Layer of IoT"** in International Journal of Innovative Technology and Exploring Engineering(IJITEE), ISSN:2278-3075,Volume-9,Issue-4, February 2020.
20. Mohammed Ridha Nsaif, Mohammed Falah Abbood , Abbas Fadhil Mahdi," **Detection and Prevention Algorithm of DDoS Attack Over the IOT Networks"**, in TEM Journal , Vol-9, Issue-3,Pages 899-906,ISSN.No:2217-8309, DOI:10.18421/TEM93-09, August 2020.
21. https://www.irjmets.com
22. Fix, E. and Hodges JL.(1951) "**Discriminatory analysis. Nonparametric discrimination; consistencyproperties**". Technical Report 4, USAF School of Aviation Medicine Randolph Field, TX, USA.
23. Prasath VBS, Haneen Arafat Abu Alfeilat ABAH, Lasassmeh O, Lasassmeh O, Ahmad S. Tarawneh, Mahmoud B Alhasanat, Hamzeh S. Eyal Salman.(2017) "**Distance and Similarity Measures Effect on thePerformance of K-Nearest Neighbor Classifier -- A Review.**" arXiv preprints 1708.04321:1–39.
24. Nguyen HV and Choi Y.(2009) "**Proactive detection of DDoS attacks utilizing k-NN classifier in an anti- DDos framework.**" *International Journal of Computer, Electrical Automation, Control and Information Engineering* **39**(**3**): 640–645.
25. Li W, Yi P, Wu Y, Pan L, Li J.(2014) "**A new intrusion detection system based on KNN classification algorithm in wireless sensor network.**" *Journal of Electrical and Computer Engineering*.

26. Aljawarneh SA and Vangipuram R.(2018) "GARUDA : Gaussian dissimilarity measure for feature things."Journal of Supercomputing.
27. Pajouh HH, Javidan R, Khaymi R, Dehghantanha A,Choo Kim-Kwang R.(2016) "**A Two-layer DimensionReduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks.**" IEEE Transactions in Emerging Topics in Computing **7**(**2**):314-323
28. Mohammed Ibrahim, Muhammed Hanif, Shabir Ahmad," **SDN Based DDoS Mitigating Approach Using Traffic Entropy for IoT Network**", Computers, Materials & Cntinua,DOI:10.32604/mc.2022.017772