INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 5 - V8I5-1180)
Available online at: https://www.ijariit.com

DDoS Detection in Internet of Medical Things through Ensemble Learning with Clustering

Reena Devi
sparky.fragy66@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

Avni Sharma
avnisharma910@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

ABSTRACT

A direct or indirect means of attack modes have been found in the literature and the various types of attacks and their unique features have been extensively studied from the literature. Since the proposed evaluation is based on 119 evolutionary algorithms, the features of the attacks are extremely important to make the system learn and hence self-adapt to varying input attack patterns thus making the system to be intelligent. The last part of this chapter brings out the various defense and attack response mechanisms that have been developed in recent times and the merits and loopholes in existing system have been recorded. The literature survey has been extremely useful in proposing constraint featured defense mechanisms for the incoming DDoS attacks.

Keywords: *Internet of Medical Things, DDoS Attacks, Remote Patient Monitoring*

1. INTRODUCTION

The advent of Internet of Medical Things (IoMT) has enhanced remote patient monitoring. It reduces unnecessary hospital visits and the burden on health care systems by connecting patients to their physicians and allowing the transfer of health data over a secure network. Healthcare professionals can monitor patients' key biometrics in real-time, access healthcare data in remote locations, and keep track of any potential issues that might occur, thus help preventing any future complications. IoMT has the potential to give more accurate diagnoses, less mistakes and lower costs of care through the assistance of technology, allowing patients to send health information data to doctors. Currently, this is essentially necessary due to the effect of the global pandemic, COVID-19, reducing in-person medical visits which prevents the spread.

IoMT has enhanced Remote Patient Monitoring (RPM) which helps in monitoring patients' vital signs such as heart activities and glucose level - the doctors can then be automatically alerted when necessary. IoMT can also help in triggering emergency responses and keep chronic diseases in check. For instance, wearables can help monitor heart rate and glucose levels. Those living in remote areas can share activity tracker information with a remote health provider with the use of smart devices and get a medically informed recommendation. IoMT has revolutionized the operations of health sector. For example, a report from Forbe states "The Internet of Medical Things (IoMT) is poised to transform how we keep people safe and healthy especially as the demand for solutions to lower healthcare costs increase in the coming years".

IoMT has the potential for more accurate diagnoses, improved efficiency, improved patient care, and lower costs of care. It is capable of monitoring, informing and notifying not only care-givers, but also provide healthcare providers with specific data to help identify issues for earlier invention before they become critical .

IoMT helps insurance companies to view patient data more quickly and make the processing of claims faster and accurate. In fact, all stakeholders including the pharmaceuticals and insurance companies greatly benefit from IoMT due to improved quality of patient care.
According to Kamalanthan et al. [2], IoMTs are divided into 4 categories which are listed below:

- Wearable devices: Smartwatches, temperature and pressure sensors, heart monitoring and muscle activity sensors, and glucose and biochemical sensors.
- Implantable devices: Swallowable camera capsule for visualization of the gastrointestinal tract, embedded cardiac pacemakers, and implantable cardioverter-defibrillators (ICD).

- Ambient devices: Motion sensors, door sensors, vibration sensors, etc.
- Stationary devices: Imaging devices like CT (Computerized Tomography) scan and surgical devices.

BSN, called BSN-Care, which can efficiently accomplish those requirements.

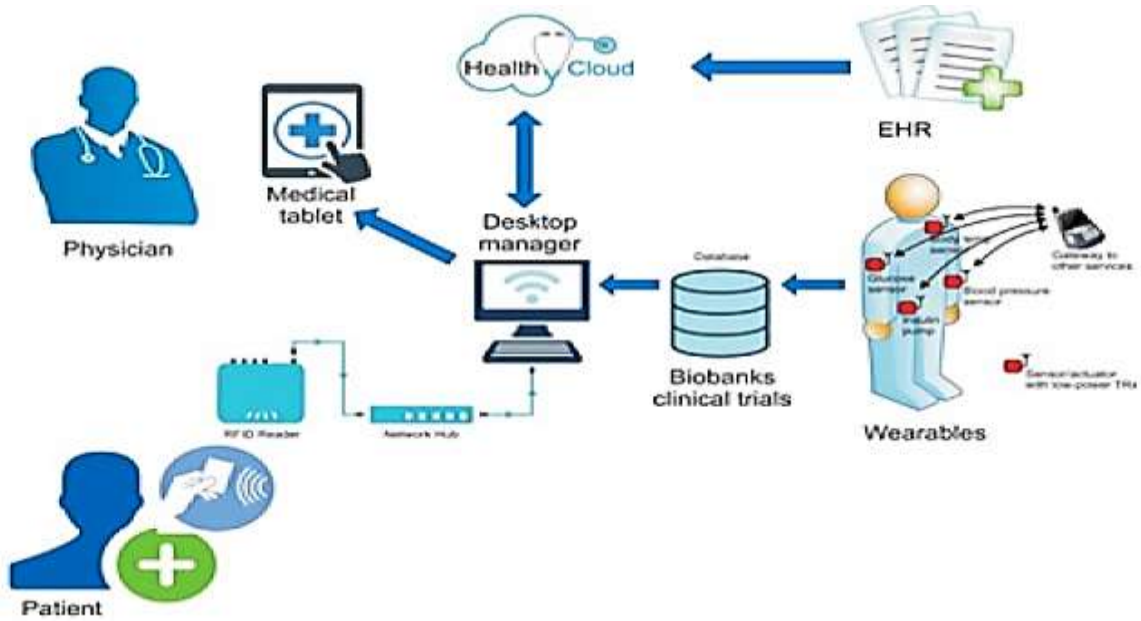

Fig.1.1. A typical IoMT System [63]

2. LITERATURE REVIEW

Mohammed Irfan and Naim Ahmad [7] reviewed and proposed the architectural model to implement IoMT. Moreover, using Carley's eight step content analysis technique, motivational factors for the adoption of IoMT have been identified. Finally, the paper sheds light on the major impediment such as security and privacy issues. This work will help the medical professionals to smoothly integrate the IoMT in their domain and avoid the major pitfalls.

Vankamamidi S. et al. [8] provides a review of IoT in the healthcare domain by first describing the enabling technologies for delivering smart healthcare, followed by some of the key applications of IoT in healthcare. Next, a fog-based architecture consisting of three layers for IoT-based healthcare applications is proposed. Finally, the researchers focus on some of the open challenges of IoT in healthcare, like fault tolerance, interoperability, latency, energy efficiency, and availability. Existing solutions for these challenges are also discussed.

T. Muhammed et al. [9] proposes a ubiquitous healthcare framework, UbeHealth, that leverages edge computing, deep learning, big data, high-performance computing (HPC), and the Internet of Things (IoT) to address the aforementioned challenges. The framework enables an enhanced network quality of service using its three main components and four layers. Deep learning, big data, and HPC are used to predict network traffic, which in turn are used by the Cloudlet and network layers to optimize data rates, data caching, and routing decisions. Application protocols of the traffic flows are classified, enabling the network layer to meet applications' communication requirements better and to detect malicious traffic and anomalous data. Clustering is used to identify the different kinds of data originating from the same application protocols. A proof-of-concept UbeHealth system has been developed based on the framework. A detailed literature review is used to capture the design requirements for the proposed system. The system is described in detail including the algorithmic implementation of the three components and four layers. Three widely used data sets are used to evaluate the UbeHealth system.

Bahar Farahani et al. [10] discuss applicability of IoT in healthcare and medicine by presenting a holistic architecture of IoT eHealth ecosystem. Healthcare is becoming increasingly difficult to manage due to insufficient and less effective healthcare services to meet the increasing demands of rising aging population with chronic diseases. The researchers propose that this requires a transition from the clinic-centric treatment to patient-centric healthcare where each agent such as hospital, patient, and services are seamlessly connected to each other. This patient-centric IoT eHealth ecosystem needs a multi-layer architecture: (1) device, (2) fog computing and (3) cloud to empower handling of complex data in terms of its variety, speed, and latency. This fog-driven IoT architecture is followed by various case examples of services and applications that are implemented on those layers.

Hilaire et al. [11] shows how DDoS attacks can exhaust controller resources and provides a solution to detect such attacks based on the entropy variation of the destination IP address. This method is able to detect DDoS within the first five hundred packets of the attack traffic.

Thamilarasu et al. [12] design and develop a novel mobile agent-based intrusion detection system to secure the network of connected medical devices. In particular, the proposed system is hierarchical, autonomous, and employs machine learning and regression algorithms to detect network level intrusions as well as anomalies in sensor data. The researchers simulate a hospital network topology and perform detailed experiments for various subsets of Internet of Medical things including wireless body area networks and other connected medical devices. The simulation results demonstrate that we are able to achieve high detection

accuracy with minimal resource overhead.

Gaganjot Kaur, and Prinima Gupta [13] improve attack detection accuracy by using the DPTCM-KNN approach. The DPTCMKNN technique outperforms support vector machine (SVM), yet it still has to be improved. For healthcare systems, this work develops a unique approach for detecting DDoS assaults on SDN using DPTCM-KNN.

Mario Di Mauro et al. [14] offer basically three contributions: 1) the authors introduce an abstract model for the aforementioned class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment; 2) the authors devise an inference algorithm that is shown to provide a consistent (i.e., converging to the true solution as time elapses) estimate of the botnet possibly hidden in the network; and 3) the authors verify the validity of the proposed inferential strategy on a test-bed environment. The tests show that, for several scenarios of implementation, the proposed botnet identification algorithm needs an observation time in the order of (or even less than) 1 min to identify correctly almost all bots, without affecting the normal users' activity.

Booth, Todd, and Karl Andersson [15] have created a new Internet services network security surface attack mitigation methodology. The novel design patterns will help organizations improve the price/performance of their anti-network reflection solution by 100 times, as compared to common on-premise solutions. The analysis and results confirm that our solution is viable. The novel solution is based on stateless IP packet header filtering firewalls (which can be implemented mostly in hardware due to their simplicity). The researchers have reduced and, in some cases, eliminated the need for researchers to even try and find new ways to filter the same traffic via more complex, software driven stateful solutions.

Da Yin and Kun Yang [16] proposed an algorithm which compares the packet-in rate of real time traffic with the threshold value of cosine similarity of the vectors of packet-in rate at the ports. If any anomaly or inconsistency is detected from the packet-in rates, then it blocks source.

Seyed Mohammad and Marc St. Hilaire [17] proposed a method which is based on comparing entropy of repeated packet from the traffic which results in classifying the variations in their randomness. A threshold value is calculated to compare with the entropy of the traffic. The entropy is estimated based on the destination IP address of a window of 50 packets each and if the entropy is less than the threshold, the device is considered to be compromised and it is reported.

Surender Singh and Sandeep Jain [18] proposed a distributed framework, to analyze the behaviour of the packets in traffic. To distinguish between the malicious traffic and legitimate traffic from network traffic, this method uses traceback algorithm and entropy.

Mohan Dhawan et al. [17] proposed a SPHINX framework which detects DDoS attack in SDN with less performance overheads. This framework spots both known and potential attacks on network. This is based on approximation of real time network traffic into a flow graph to detect threats in a network traffic.

3. PROPOSED METHODOLOGY

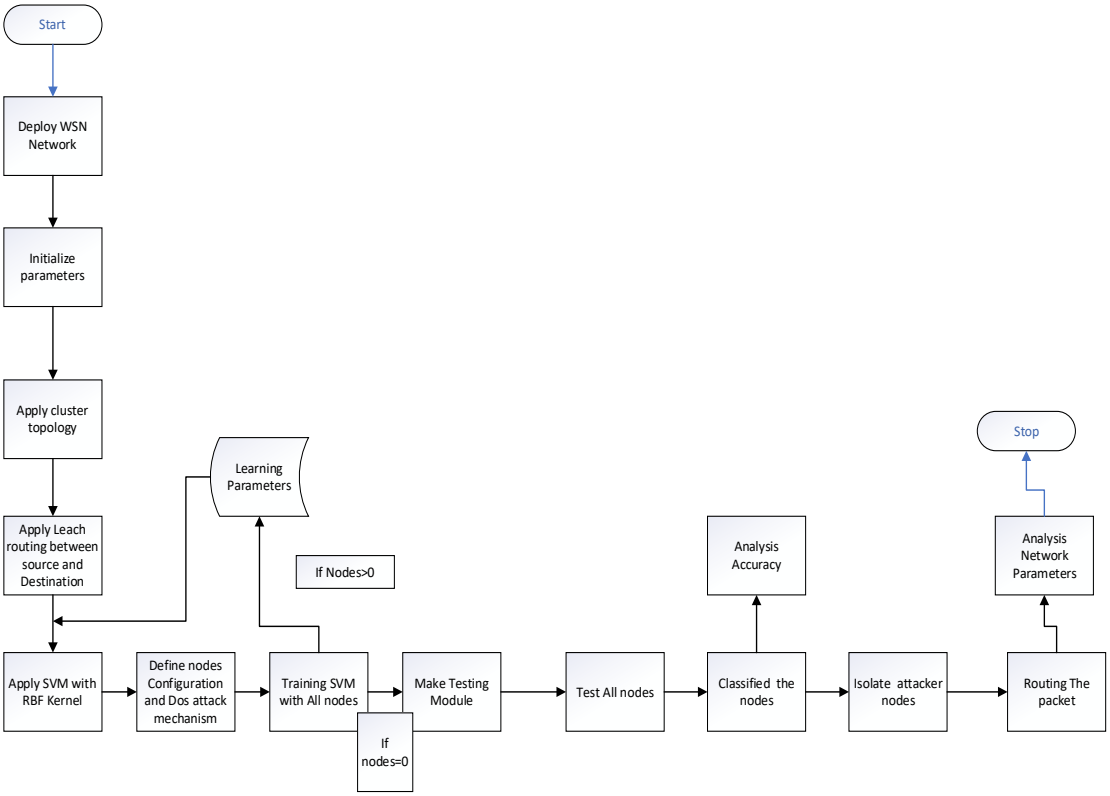

Fig. 1. Proposed Flow chart

In fig4.1 show the proposed flow chart which have following step:

Step1: In first deploy IOMT network with initialize parameter with number of nodes, energy, area and number of rounds with time of simulation.
Step2: In next step apply clustering base topology apply. By clustering topology every node has own cluster head where send message and then communicate to base station.
Clustering
Energy consumption and network consistency is a serious task in IOMT. Clustering in IOMT is well recognized and has long been in use. Clustering over centralized technologies is increasingly evolving to resolve concerns such as longevity of the network and energy saving. Clustering in sensor nodes is quite essential to fix the several issues of sensor networks such as scalability, energy as well as lifetime difficulties. Clustering algorithms restrict connectivity in a local environment and therefore only transmit required information via the relay nodes to the rest of the network. A group of nodes form a cluster in which cluster head manages the local transmissions among cluster members. Cluster head coordinate with the members of the cluster, as it aggregates the gathered data and compress it to save energy. Until CH deplete their energy, they choose new CH to automatically replace itself after the complete drainage of their energy (46).

Clustering strategies for homogeneous and heterogeneous networks are focused on sensor node features as well as functionality within a cluster. In homogeneous networks, all the sensor nodes have identical processor and storage capacities. In addition, every node could be a CH depending on different parameters like excess energy level and distance from a cluster's centre. The position of CH is rotated regularly to achieve energy conservation as well as load balancing whereas in heterogeneous networks, there are typically 2 types of sensor nodes that is nodes with higher potential as well as storage capacities are generally used as CH inside a cluster, which act as data collectors or may even be seen as backbones within the network while nodes with lower abilities are general sensor nodes which sense the attributes of the chosen field (47).
Step3: Randomly select DDOS attacker nodes and apply routing algorithm LEACH its base is clustering topology.

4. RESULT AND ANALYSIS

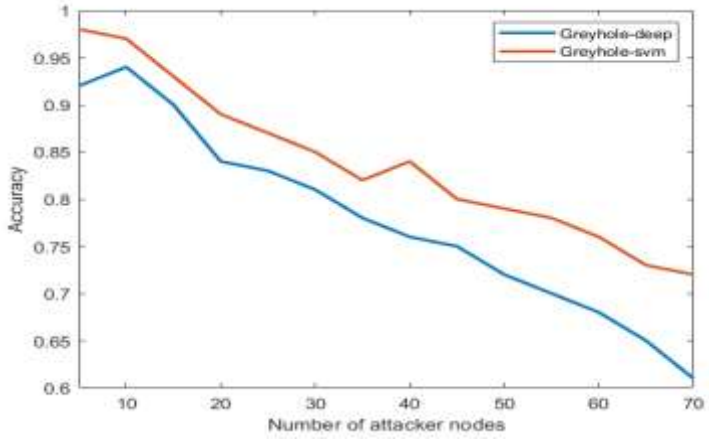

Fig. 2. Comparison of attacker node detection between proposed and existing approach

Figure 2 depicts a comparison of the proposed grey hole with SVM and the existing grey hole with deep learning as a basis in terms of accuracy. As Deep Learning requires non-linear features, the accuracy of attacker nodes increases in the SVM approach. When there are 10 attacker nodes, the proposed system has an approximate accuracy of 0.90, while the existing method has an accuracy of 0.94. The existing proposal has an accuracy of 0.85 when the number of attacker nodes is 40, whereas the existing method has an accuracy of 0.75. The existing method has a significant downfall, bringing its accuracy to 0.6 as opposed to 0.74 in the case of the proposed method. The use of the proposed approach to detect the network attack path may substantially increase the defensive performance of network node attacks and the information security coefficient.

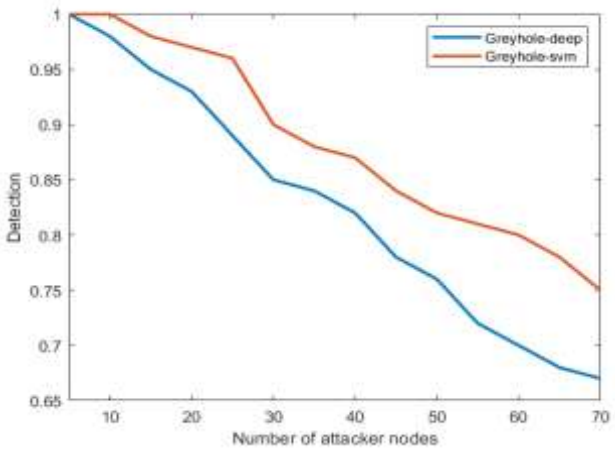

Fig.3: Comparison of attacker node detection between proposed and existing approach

Figure 3 depicts a comparison of the proposed grey hole with SVM and the existing grey hole with deep learning as a basis in terms of detection. As Deep Learning requires non-linear features, the accuracy of attacker nodes increases in the SVM approach. When there are 10 attacker nodes, the proposed system has an accuracy of 1.0, while the existing method has an accuracy of 0.98. The existing proposal has an accuracy of 0.82 when the number of attacker nodes is 40, whereas the existing method has an accuracy of 0.87. The existing method has a significant downfall, bringing its accuracy to 0.68 as opposed to 0.75 in the case of the proposed method. It is possible that the proposed approach to detecting the network attack path would improve the defensive capabilities of network node attacks and the security coefficient significantly.

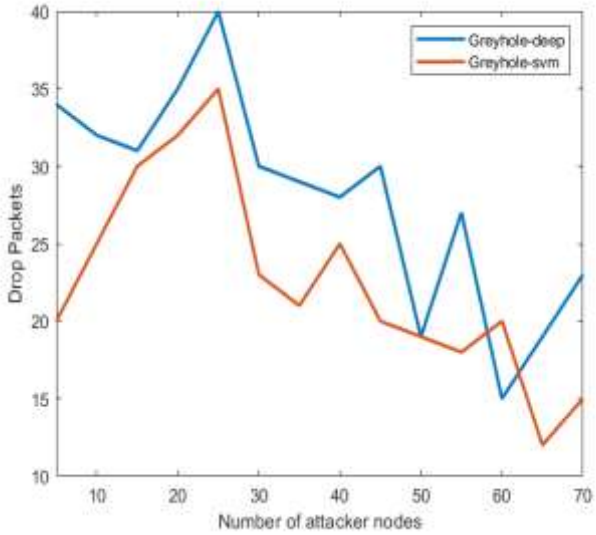

Fig. 4: Comparison of drop packet between proposed and existing approach

Figure 4 shows a comparison of drop packets between the proposed grey hole with SVM and the existing grey hole with deep learning as a basis. Figure 4 depicts the number of lost packets when attacker nodes are present. As depicted in the graph, fewer packets are lost with grey hole SVM than with grey hole-deep technique for varying numbers of attacker nodes. Therefore, the proposed method (grey hole-SVM) is more resistant to security threats in wireless sensor networks and can defend itself well against many types of attacks.

5. CONCLUSION

The work embodied in this dissertation has addressed the problem of an effective and optimal evaluation of evolution-based algorithms for effectively defending against distributed denial of service attacks on a network. The rapid increase in communication protocols has invoked a great deal of internet usage day by day and at the same time attracted a wide range of online and offline attacks being carried out to illegally extract or tamper with the data over the network. This chapter presents the summary of the work done with emphasis on the findings from the experimentations. The chapter concludes briefing the limitations and future scope of this research work. The objective of the thesis is to design, implement and test an optimal and robust defense mechanism to detect and resist against a specific class of attacks known as distributed denial of service (DDoS). To start with, an extensive literature survey has been carried out starting from research contributions defining the various attributes of cloud. The survey of literature has been carried out in a very systematic manner by outlining the different modes by which the attacker engages with the target or victim system.

6. REFERENCES

[1] S. Vishnu, S.R Jino Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview, 2020 5th International Conference on Devices," in *Circuits and Systems (ICDCS)*, 2020.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of- Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine,* vol. 55, pp. 16-24, 2017.

[3] A. S. El-Wakeel, J. Li, A. Noureldin, H. S. Hassanein, and N. Zorba, "Towards a Practical Crowdsensing System for Road Surface Conditions Monitoring," *IEEE Internet of Things Journal,* vol. 5, p. 4672–4685, 2018.

[4] Nipuni Nanayakkara, Malka N. Halgamuge and Ali Syed, "Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review," in *International Conference on Advances in Business Management and Information Technology, Research Gate,* 2019.

[5] K. Ngo Manh, S. Saguna, M. Karan and A. Christer, "IReHMo: An efficient IoT-based remote health monitoring system for smart regions," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom), IEEE*, Boston, 2015.

[6] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal,* vol. 16, pp. 1368-1376, 2016.

[7] Mohammed Irfan, Naim Ahmad, "Internet of Medical Things: Architectural Model, Motivational Factors and Impediments," in *2018 15th Learning and Technology Conference (L&T) IEEE,* 2018.

[8] Vankamamidi S. Naresh, Suryateja S. Pericherla, Pilla Sita Rama Murty and Sivaranjani Reddi, "Internet of Things in Healthcare: Architecture, Applications, Challenges and Solutions," *Computer Syst Sci & Eng,* vol. 6, pp. 411-421, 2020.

[9] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ube-Health: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities," *IEEE Access,* vol. 6, p. 32258–32285, 2018.

[10] Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Nicholas Constant, Kunal Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems,* vol. 78, p. 659–676, 2018.

[11] Hilaire, Seyed Mohammad Mousavi and Marc St., "Early Detection of DDoS Attacks against SDN Controllers," in *International Conference on Computing, Networking and Communications, Communications and Information Security Symposium*, 2015.

[12] Thamilarasu, Geethapriya, Adedayo Odesile, and Andrew Hoang. "An intrusion detection system for internet of medical things." *IEEE Access* 8 (2020): 181560-181576.

[13] Kaur, Gaganjot, and Prinima Gupta. "Detection of Distributed Denial of Service Attacks for IoT-Based Healthcare Systems." *Computer Assisted Methods in Engineering and Science* (2022).

[14] Matta, Vincenzo, Mario Di Mauro, and Maurizio Longo. "DDoS attacks with randomized traffic innovation: Botnet identification challenges and strategies." *IEEE Transactions on Information Forensics and Security* 12, no. 8 (2017): 1844-1859.

[15] Booth, Todd, and Karl Andersson. "Network security of internet services: eliminate DDoS reflection amplification attacks." *Journal of Internet Services and Information Security (JISIS)* 5, no. 3 (2015): 58-79.

[16] Da Yin, Lianming Zhang and Kun Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," *IEEE Access,* 2018.

[17] Seyed Mohammad Mousavi and Marc St. Hilaire, "Early Detection of DDoS Attacks against SDN Controllers," in *International Conference on Computing, Networking and Communications, Communications and Information Security Symposium*, 2015.

[18] Jain, Surender Singh and Sandeep, "A Review of Detection of DDoS Attack Using Entropy-Based Approach," in *IJCST*, 2013.

[19] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan and Vijay Mann, "SPHINX: Detecting Security Attacks in Software-Defined Networks," in *BM Research*, 2009.

[20] Haopei Wang, Lei Xu and Guofei Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks," in *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'15*, 2015.

