IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study on Intrusion Detection System for IoT Environment Based on Machine Learning

Laiby Thomas[1] , Subrahmanya Bhat [2]

[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangaluru, India, and Assistant Professor, Dept. of Computer Science, NIMIT, Pongam,Kerala, India

[2]College of Computer Science and Information Science, Srinivas University, Mangaluru, India.

Abstract

IoT, Internet of Things is now becoming an inevitable part of everyone's life. IoT connects many devices, sensors, applications via wireless or mobile networks to fulfill the required tasks. IoT invests interest in various fields like agriculture, healthcare, smart cities, homes, cars, transportation, etc. Today IoT is being used extensively to lessen the burden of humans. Even though IoT eases human life but also opens to different security challenges. Security must be a priority while across the value chain from the device manufacturers, IoT Service providers, Retailers and consumers. Adopting IoT in a sensitive environment is really a challenging task because of subtle data. This may cause hazards for the nourishment of IoT in the coming days. In light of this, we try to examine the various factors that contribute to the challenges of IoT security. Intrusion Detection System can be used for the security of data as well as devices over the internet. In recent years Machine Learning techniques are applied in the detection of threats in IDS. This research, therefore, focuses on Machine Learning Techniques applied in Internet-of-Things and Intrusion Detection for IoT security. Denial of Service (DoS) is one of the most catastrophic attacks against IoT. In this paper, we investigate the prospects of using machine learning algorithms for securing IoT against DoS attacks.

Keywords: IoT, IDS, Machine Learning, Vulnerability,DDoS

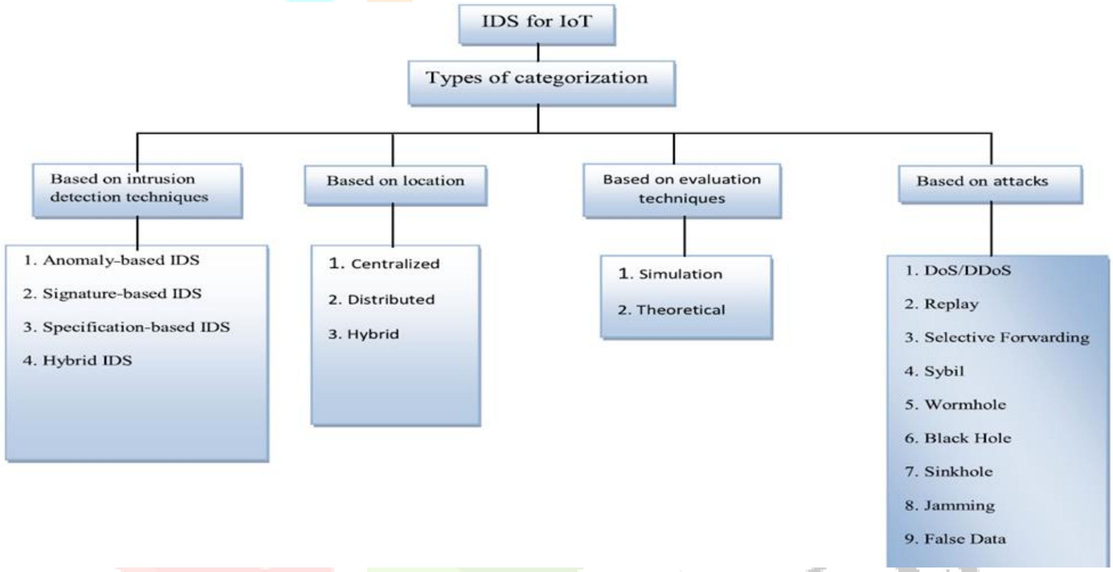
Introduction

The Internet of Things (IoT) has received increased attention in recent years as a result of its unique applications and assistance for a variety of areas, including industrial processes, medical care, automation, smart environments, and so on [1]. Despite the fact that the IoT offers a diverse set of services and applications, it is vulnerable to cyber-attacks. Because the Internet of Things is a diverse ecosystem with a lack of interoperability, traditional security solutions are ineffective [2]. However, other aspects of IoT security, such as data authentication, confidentiality, and access controls, are improved. These security mechanisms are designed in collaboration between the user and the IoT, yet they still have security flaws. These security mechanisms are designed in collaboration between the user and the IoT, yet they still have security flaws. As a result, a separate module is required to provide IoT network security. Intrusion detection systems (IDS) are an example of a notion that is already being used in wireless networks [3, 4]. Adding IDS features to wireless networks will aid IoT in protecting the network from assaults and other issues.

IDS in IoT

An unauthorised activity or action that harms the IoT ecosystem is known as IoT Intrusion. In other words, an intrusion is an attack that results in any kind of destruction to the confidentiality, integrity or availability of information. While using the traditional firewalls, it is not possible to identify unauthorised computer usage and malicious network traffic. So the main aim of IDS is making the computer systems which is highly protective against the malicious actions that compromise the availability, integrity, or confidentiality of computer systems.

The four types of IDS categorization is shown in Figure[5]. The first one is based on intrusion detection techniques. The second one is based on the location, including centralized, distributed, and hybrid. The third one is based on evaluation techniques such as simulation and theoretical. The fourth one is based on potential attacks.



I. Classification based on detection systems

a. Specification-based IDS in the IoT

In the IoT, anomaly-based and specification-based IDSs are similar because both of them recognize intrusions when a change occurs from normal behaviour. However, specification-based methods do not depend on machine learning techniques.[5] In these schemes, specifications are physically developed and captured legitimate system behaviours. A Service Oriented Architecture (SOA) presented by Misra et al. is a system model for the detection of attacks in the IoT environment using learning automata concepts. The SOA acts as a middleware which delivers a platform for developing numerous applications for IoT. According with different layers and objects the amount varies. In this step, the system senses the attacks on any object in the IoT. If the number of requests is greater than the defined value for each layer uses a DDoS alert (DALERT). DALERT is directed to all nearby neighbours of objects that will distribute this alert to other nodes[6]. In nutshell, this phase recognizes a DDoS attack and is carried out entirely on the servicing device i.e. server. During this phase, other objects keep their normal performance.

b. Anomaly-based intrusion detection system (AIDS)

Because of AIDS feature to overcome the limitation of SIDS became an area of researches. A normal model of the behaviour of a computer system is created using machine learning, statistical-based or knowledge-based methods are used in AIDS. Any major deviation between the observed behaviour and the model is regarded as an anomaly, which can be deduced as an intrusion[7]. These techniques work on the fact that typical user behaviour is different from malicious behaviour. An intrusion is defined as the behaviour of abnormal users that distinguishes from the standard behaviour. The training phase and the testing phase are the two phases in the development of AIDS, the normal traffic profile is used to learn a model of normal behaviour is used in the testing phase. Also a new data set is used to develop the system's capacity to generalise to previously unseen intrusions.

Based on the methods used for training, AIDS is sub-categorized. They are statistical based, knowledge-based and machine learning-based. The main difference between SIDs and AIDS is that, SIDS can only detect previously known intrusions whereas AIDS can discover zero-day attacks. Because of anomalies may just be new normal activities rather than genuine intrusions results in high false-positive rate.

c. Hybrid IDS in the IoT

In order to identify the usual behavior of a node, the anomaly based IDS employs a training process to reach a high detection rate. The disadvantages of the anomaly-based IDS is High false positive rate and computation cost, the disadvantages of signature based IDS is high storage cost and a limited number of attack detection[8]. For overcoming these disadvantages, a hybrid scheme was suggested. A signature based scheme has been used to spot the known attacks and anomaly detection scheme has been used to spot the unknown attacks, these two methods are used in the hybrid scheme.

High computational overhead and high resource consumption are some disadvantages of hybrid scheme. Some of hybrid scheme have a high delay. The merits of this method are the false alarm rate, lightweight implementation, and low memory consumption, and the demerits are the high computational overhead and high delay.

d. Signature-based intrusion detection systems (SIDS)

To find a known attack, Signature intrusion detection systems (SIDS) use pattern matching techniques are used this is also known as Knowledge-based Detection or Misuse Detection. In SIDS, to find a previous intrusion matching methods are used. An alarm signal is triggered when an intrusion signature matches the signature of a previous intrusion that is already exists in the signature database. For SIDS, the host's logs are inspected to find sequences of commands or actions which have previously been identified as malware[9]. SIDS has also been considered in the literature as Misuse Detection or Knowledge-Based Detection.

Build a database of intrusion signatures and to compare the current set of activities against the existing signatures and raise the alarm if a match is found is the main idea of this method. SIDS provides excellent detection accuracy for previously known intrusions .The SIDS is unable to identify zero-day attacks as the database does not contain a matching signature until the signature of the new attack is extracted and stored. SIDS is employed in a number of common tools, such as Snort and NetSTAT.

II. Based on Location

a. Distributed IDS

In distributed placement, the IoT devices could be responsible for checking other IoT devices. In Distributed IDS a big IoT ecosystem is made up of several IDS, all of which communicate with each other, or with a central server that assists advanced intrusion detection systems, packet analysis, and incident response. Distributed architectures are organised by several IDS. This includes a subset of network which checks the other nodes[6]. Distributed IDS have many advantages over centralized IDS. The capability to identify attack forms across a whole IoT ecosystem is the main advantages of this. This might increase prompt IoT attack prevention and detection. The other advantages are to allow early detection of an IoT Botnet creating its way through corporate IoT devices. This data is used to detect and clean systems that have been infected by the IoT Botnet and stop further spread of the Botnet into the IoT ecosystem consequently take down any IoT devices damaged that would otherwise have occurred. The advantage of distributed IDS rather than centralized IDS computing resources also implies reduced control over those resources.

b. Centralized IDS

The centralized IDS is placed in central devices, for instance, in the boundary switch or a nominated device. All information's that the IoT devices collect and then send to the network boundary switch passes through the boundary switch. The IDS located in a boundary switch can check the packets switched between the network and the IoT devices. In spite of this, checking the network packets that pass through the boundary switch is not suitable to identify anomalies that affect the IoT devices. In centralized IDS the network traffic is monitored.

This traffic is take out from the network through different network data sources such as packet capture, NetFlow, etc. The computers connected in a network can be examined by Network-based IDS. NIDS is also able to observing the external malicious activities that could have been originated from an external threat at earlier stage, before these threats expand to other computer systems. NIDS have some drawbacks such as its restricted ability to inspect the entire data in a high bandwidth network because of the volume of data passing through modern high-speed communication networks)[7,8]. NIDS installed at several positions within a particular network topology, together with HIDS and firewalls, can provide a concrete, resilient and multi-tier protection against both external and insider attacks.

Data source consists of system calls, application program interfaces, log files, data packets that are extracted from well-known attacks. These data sources can be useful to classify intrusion behaviours from abnormal actions[9].

III. Based on Evaluation Techniques

The third type is based on evaluation techniques such as simulation and theoretical.

IV. Based on attacks

Well-known types of attacks which can be detected by IDS are as follows[25]:

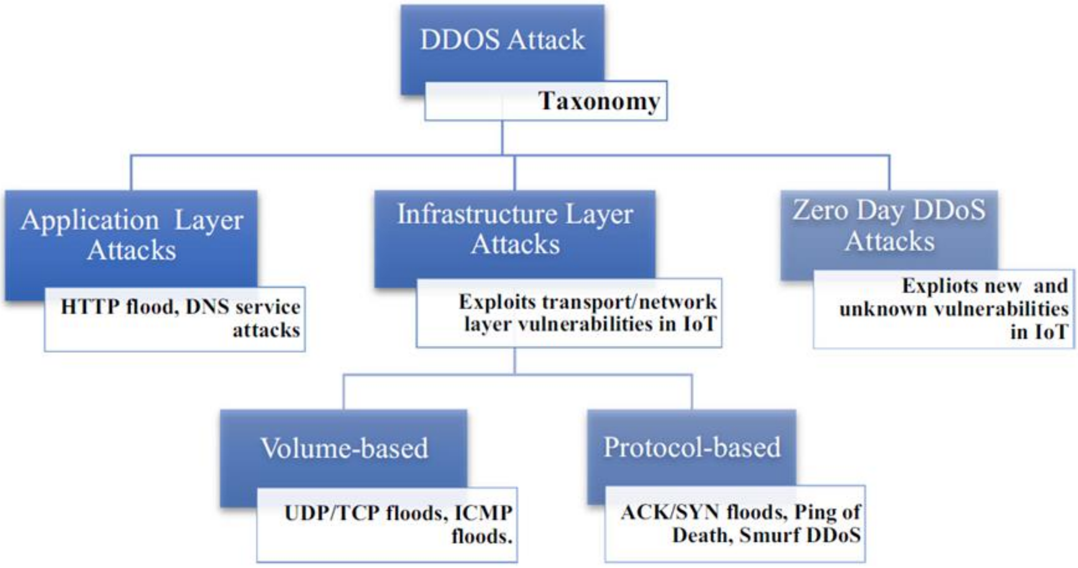
- **DoS attack:** Presence of DoS/DDoS attacks can disorder the usability of the networks by sending data in specific samples over the network, or by simply flooding packets. It is often possible for attackers to hinder the remote service.
- **Sybil attack**: In this type an adversary presents faked identities to legitimate nodes. An adversary may make such identities with disabling the legitimate nodes permanently.
- **Replay attacks**: In the first step, the attacker performs an intrusion from time t0 until tn and collect data, then replaying the collected data.

- **Selective forwarding attack**: In selective forwarding attacks, some of the specified packets (not every packet) are refused to forward or dropped by the malicious attacks. The adversary ensures that the packets are never propagated.
- **Sinkhole attack:** In a sinkhole attack, attracting the data from all neighbouring nodes is the goal of the compromised node.
- **Wormhole attack:** An attacker gets the packets at the one side of the network, tunnels them to another side, and then relays them into the network from that point.
- **Black hole attack:** In the black hole attack, an attacker listens to the request packets using the dynamicity of the routing protocol in order to abuse it by replying with a faked reply packet

Different DDoS attacks in IoT

In the case of simple DoS attack, the targeted server or device rejects serving any request from its clients due to excessive flooding of data through the communication channel consuming all the bandwidth unnecessarily and as an effect, makes the server inaccessible for additional requests. This overflow of data is purposefully targeted by the attacker against the server in the form of false requests due to this a valid request also get suffered and are dropped before completion[25,10]. But in DDoS Attack, the transfer of data is carried out between different network devices distributed across the network without having any centralized control. The DDoS Attacks take place at both application layer and infrastructure layer (i.e., Network and Transport layers) of the network architecture.

DDoS attacks have a number of variations in their attacking methods in past years and still getting experimented with a number of possibilities[11]. There is not much difference between traditional DDoS attacking methods and IoT specific DDoS attacking methods. They use similar techniques to exploit the susceptibilities that exist either in an IoT device or in conventional systems. IoT specific DDoS attacks are more diverse and sophisticated due to heterogeneity involved in IoT devices. On the basis of their attacking techniques, this is categorized into three types of attacks. This classification based on DDoS attacks is completely depends upon the impact of the attack on the server site in an IoT network. Except considering the corresponding network architecture as a reference model, IoT specific DDoS attacks are similar to the traditional DDoS attacks. According to the way of generating number of pseudo codes requests from an IoT source to the targeted server, we have another class of DDoS attack types[12]. The only way that has been discovered yet to trigger such a huge number of false requests that utilises the power of IoT network is based on malwares and bots.


DDOS Attack
Taxonomy
Application Layer Attacks
HTTP flood, DNS service attacks
Infrastructure Layer Attacks
Exploits transport/network layer vulnerabilities in IoT
Zero Day DDoS Attacks
Expliots new and unknown vulnerabilities in IoT
Volume-based
UDP/TCP floods, ICMP floods.
Protocol-based
ACK/SYN floods, Ping of Death, Smurf DDoS

The basic IoT network layered architecture is used to classify the DDoS attacks, where each layer can be targeted explicitly to conquer the security of an IoT network-based application server. Thus, the attacks are classified into Application layer attacks and Infrastructure layer attacks[13].The attacks which try to invade application layer of IoT network infrastructure where the packets are dropped at the rate of request per second due to flooding of application or web server by HTTP(Get/Post) requests, and other requests that target the system software like Windows, Apache, OpenBSD, etc. is known as Application layer attacks. These attacks are harder to detect and diminish as they tend to generate the traffic at a lower rate and the request generated seems to be authentic but they actually trigger the back-end process that makes the resources unavailable, which include HTTP flood, DNS service-based attacks, etc[14].

Infrastructure layer attacks render the target system inaccessible by exploiting the weaknesses present at the network layer or transport layer of the IoT architecture. These attacks can be of two types, protocol-based and volume-based attacks. They usually employ amplification or reflection techniques to fire the attack. The attacker uses IP address spoofing to reflect the sent request as an unrequested reply to the victim that leads to the congestion at the victim network. Amplification is also a reflection having larger replies for smaller requests which unnecessarily consumes the bandwidth. Protocol-based attacks, also known as Resource Depletion attacks, are responsible for consuming the actual server resources along with intermediate communication equipment’s like firewalls, load balancers, etc.[15]. They are measured in packets per second (Pps). SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, etc. are some of the examples of this. Saturate the bandwidth of the target system by generating excessive traffic in bits per second (Bps) is known as Volumetric attacks also known as Bandwidth Depletion attacks. These are simplest to service as they use amplification and reflection techniques to launch the attack. The studies prove that up to 65% of attacks are only volume-based attacks, such as UDP/TCP floods, ICMP floods.

In spite of having such a classification, attacks can take the integrated form of forementioned infrastructure layer attack types. Now a days IoT network intruders are becoming smarter enough and have started experimenting with new ways to launch the attack to defeat the security of even some well-known web servers too[16]. Recent examples of such a case was Dyn DNS Outage, which was a combination of an application and protocol-based attack on DNS service that was prolonged into a volumetric attack. Followings are some well-known DDoS attacks that become common these days[20].

DDoS defence mechanisms in IoT network

From other attacks, Denial-of-service attacks behaves differently as it often does not show any initial signs on the targeted device of its failure, rather, it gradually depletes all the available resources consuming whole network bandwidth that results into a server shut down.

There has been a number of proposals on defence mechanisms against DDoS attack from traditional defences to IoT based, specifically after seeing its wide range of variations in the recent past years[21]. All such defence mechanisms for defending DDoS can be categorized into Traditional DDoS defences and IoT specific DDoS defences. Traditional DDoS defences are applied on the target server and the conventional systems basically homogeneous systems. IoT-specific defences are applied to the IoT devices that are vulnerable to several IoT threats. These defence mechanisms are more sophisticated as they compromise of heterogeneous IoT devices distributed across the network. On both types of defence mechanisms to find out any abnormal activity either on the host or in the network a defence techniques are applied. IoT specific defence is more focused towards the detection of intrusion by a malware which results into formation of IoT botnets[22]. The presence of any such malicious software responsible for converting the host into a compromised host are also detected by the traditional DDoS defence. They also detect the unusual network traffic that leads to flooding in the network. for detecting the unusual traffic, Honeypots-base and anomaly detection-based defence mechanisms employ host-based detection schemes whereas Learning automata and software-defined networking methods are used. Prevention based defence mechanism is concerned towards avoiding any malicious intrusion into the IoT device[23].

The examples of prevention based DDoS defence are IoT middleware solution and regulatory solutions. Mitigation techniques intend to reduce the effect of flooding of the network. They do not focus on the origin of the problem, hence do not employ any sophisticated detection technique rather concentrates on lessening the problem size by elimination[18,19].

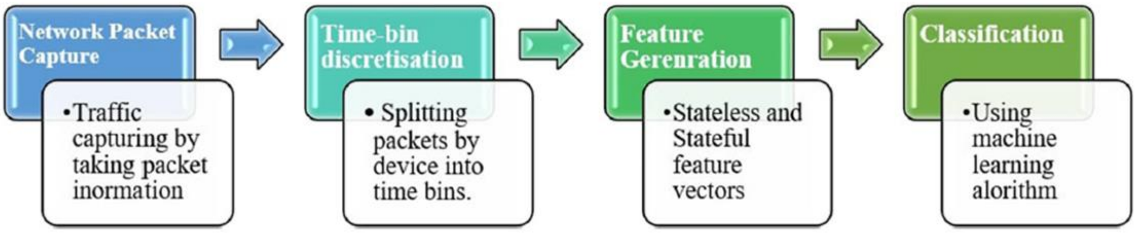
The first phase detects the attacks by defining a maximum value of servicing capability determined as per the computational resource availability (threshold value). a DALERT (DDoS Alert) is issued when the number of service requests exceeds the limit, which gets propagated with help of immediate neighbours[24]. After this next phase get started, which identifies the attacking device by finding out the device id sending a greater number of requests than others. Using a packet, the hacker’s entire information’s are transmitted which embarks the next phase to defend it against the attack. after having all the information about the attacker, all the incoming packets from the attacker’s device easily get discarded if it fails to be legitimate during sampling.

Machine learning based DDoS

Due to advance benefits of using machine learning approaches for classification, it’s now has become one of the most prominent detection techniques used for malware detection in DDoS.

Defending against an DDoS attacks, Machine learning based defence models have become a new trend. Due to their ability to detect and predict against millions of network intrusions accurately with compared to other mitigation and prevention-based defence mechanisms, they are capable enough to deal even with IoT vulnerabilities effectively.

Machine learning solution for defending DDoS has incorporated smart Home LAN with a gateway router (middlebox) to observe the traffic between the consumer IoT devices and the internet. It has utilized IoT specific network behaviors like the limited number of endpoints, the regular time interval between packets, etc. to perform feature selection process to achieve the higher accuracy in detecting DDoS in IoT network traffic with the assistance of various machine learning algorithms, including neural networks[26,27].


Network Packet Capture
•Traffic capturing by taking packet inormation
Time-bin discretisation
• Splitting packets by device into time bins.
Feature Gerenration
•Stateless and Stateful feature vectors
Classification
•Using machine learning alorithm

Conclusion

The process of detecting intrusion has grown considerably more difficult since the attack behaviour and medium of propagation used by malwares such as email and social networking platforms have become much more complicated.In this paper, we have presented, in detail, a review of IoT intrusion detection system methodologies, deployment strategy, validation strategy, and technologies. Also we reviewed Several intrusion detection systems have been proposed to detect IoT attacks. Such approaches may have the difficult to detect all IoT attacks due to IoT architecture. Even though the research development under DDoS mitigation in IoT is progressing with a good pace and researchers are coming up with their much more efficient and innovative ideas, there are still open issues and challenges that have been discussed above to provide an ideal picture of a DDoS Defence System[29,30]. In a nutshell, now the defence in IoT has to get smarter enough than the IoT itself.

References

[1].Sarkar, S., Chatterjee, S. and Misra, S., 2015. Assessment of the Suitability of Fog Computing in the Context of Internet of Things. *IEEE Transactions on Cloud Computing*, *6*(1), pp.46-59

[2].Chowdhury, A., Karmakar, G. and Kamruzzaman, J., 2019. The co-evolution of cloud and IoT applications: Recent and future trends. In *Handbook of Research on the IoT, Cloud Computing, and Wireless Network Optimization* (pp. 213-234). IGI Global.

[3].Saha, H.N., Mandal, A. and Sinha, A., 2017, January. Recent trends in the Internet of Things. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1-4). IEEE.

[4].Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), pp.1-22.

[5]. Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), 3-25.

[6].Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111(4), 2287-2310.

[7].Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 160, 165-191.

[8].Wanda, P. (2020). A survey of intrusion detection system. International Journal of Informatics and Computation, 1(1), 1-10.

[9].Choudhary, S., & Kesswani, N. (2019). A survey: Intrusion detection techniques for internet of things. International Journal of Information Security and Privacy (IJISP), 13(1), 86-105.

[10].Santos, L., Rabadao, C., & Gonçalves, R. (2018, June). Intrusion detection systems in Internet of Things: A literature review. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-7). IEEE.

[11].Tabassum, A., Erbad, A., & Guizani, M. (2019, June). A survey on recent approaches in intrusion detection system in iots. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 1190-1197). IEEE.

[12].Gendreau, A. A., & Moorman, M. (2016, August). Survey of intrusion detection systems towards an end to end secure internet of things. In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) (pp. 84-90). IEEE.

[13].HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. Future Generation Computer Systems, 85, 88-96.

[14].Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

[15].Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

[16].Sherasiya, T., Upadhyay, H., & Patel, H. B. (2016). A survey: Intrusion detection system for internet of things. International Journal of Computer Science and Engineering (IJCSE), 5(2), 91-98.

[17].Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[18].Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE communications surveys & tutorials, 20(4), 3496-3509.

[19].Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.

[20].Yang, K., Ren, J., Zhu, Y., & Zhang, W. (2018). Active learning for wireless IoT intrusion detection. IEEE Wireless Communications, 25(6), 19-25.

[21].da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks, 151, 147-157.

[22].Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analyses of intrusion detection system for IoT environment. Journal of Information Processing Systems, 16(4), 975-990.

[23].Amin, S. O., Siddiqui, M. S., Hong, C. S., & Lee, S. (2010). Implementing signature based IDS in IP-based sensor networks with the help of signature-codes. IEICE transactions on communications, 93(2), 389-391.

[24].Sedjelmaci, H., Senouci, S. M., & Al-Bahri, M. (2016, May). A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In 2016 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.

[25].Three Types of DDOS Attacks. https://blog.thousandeyes.com/three-types-ddos-attacks/. Accessed 04 December 2018.

[26].Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). Bigdata analytics framework for peer-to-peer botnet detection usingrandom forests. Information Sciences, 278, 488–497.

[27].Mergendahl, S., Sisodia, D., Li, J., & Cam, H. (2017, November). Source-End DDoS Defense in IoT Environments. In Proceedings of the 2017 workshop on internet of things security and privacy (pp. 63-64).

[28].Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011, October). A learning automata based solution for preventing distributed denial of service in internet of things. In 2011 international conference on internet of things and 4th international conference on cyber, physical and social computing (pp. 114-122). IEEE.

[29]Ahmed, M. E., & Kim, H. (2017, April). DDoS attack mitigation in Internet of Things using software defined networking. In 2017 IEEE third international conference on big data computing service and applications (BigDataService) (pp. 271-276). IEEE.

[30]. P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based internet of things, in: Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 600–607