IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

DDoS ATTACK PREVENTION FOR IoT DEVICES

Manjunath N R[1], Naveen Kumar R[2], S Karpaga Murthy[3], Sacheth K[4], Prof. Lavanya M C[5]

UG student, Dept. of CSE, Vidyavardhaka College of Engineering, Mysore, India[1-4]

Assistant Professor, Dept. of CSE, Vidyavardhaka College of Engineering, Mysore, India[5]

Abstract: The rising frequency of Distributed Denial of Service (DDoS) attacks is mostly due to botnets, as their weaknesses in the Internet of Things (IoT) make them an excellent target for these attacks. As DDoS attacks have become more frequent, it is critical to address the implications they have for the IoT industry, which is one of their primary causes. The purpose of this study is to offer an examination of attempts to stop DDoS attacks, mostly at the network level. These solutions effectiveness in addressing IoT risks serves as a gauge of their sensitivity. This analysis makes it clear that there isn't yet a perfect answer for IoT security and that there are still lots of prospects for research and development in this area.

Keywords— Denial of Service (DoS), Distributed Denial of Service(DDoS), Internet of Things (IoT), Attacks, Technology, Botnets**.**

I. INTRODUCTION

The Internet of Things is a new type of network that has emerged as a result of the growth of technology, which has brought about a time when more devices are linked to the Internet than people. The Internet of Things is a new type of network that has emerged as a result of the growth of technology, which has brought about a time when more devices are linked to the Internet than people. Most of such items are implanted monitoring and sensory devices into specific physical surroundings with the goal of presenting the real world as a smooth data flow to the digital world. IoT network components include computing platforms, individually addressable data communicating and gathering items, data transmission networks, and specialised user applications. IoT devices, just like their forebears, outdated desktop PCs and even contemporary laptops, have security flaws that make them prime targets for hackers. IoT security flaws have had a number of negative privacy and data leakage effects for health and safety organisations. Because they are a reality of everyday life, security concerns in the IoT cannot be disregarded.

A distributed denial of service (DDoS) attack seeks to temporarily reduce genuine users' bandwidth while interfering with legitimate requests. This is frequently accomplished by flooding the targeted host server with malicious requests. [9]. The attack on February 9, 2000, resulted in significant financial losses for numerous businesses that rely heavily on online commerce, including Amazon, Yahoo, and eBay. At a peak pace of 10 GB/s later in 2006, around 1500 IP addresses were attacked. Additionally, users of IoT devices paid a high price for the power and bandwidth they consumed. Several technologies have been put up to prevent and detect DDoS assaults in the IoT. [8] presents a technique to identify and counteract DDoS assaults against the Constrained Application Protocol (CoAP). [5] proposes a technique that leverages the pace of grouped messages at the boundary to assess whether DDoS attacks have occurred. This algorithm is based on the Software Defined Networking (SDN) in IoT framework. Similar to this, [7] presents a real-time DDoS assault detection method based on network time synchronisation service information.

1.1 Distributed Denial of Service (DDoS) Attacks

DDoS attacks try to consume resources or bandwidth and block access to services for genuine users. DDoS attacks against the three layers of the IoT architecture were discussed by several researchers. To prevent reading RFID data, there are jamming, kill command, and desynchronizing attacks for the perception layer. Layer-3 assaults try to deplete the victim's resources using a variety of techniques at the network layer, such flooding attacks, reflection-based flooding attacks, amplification-based flooding attacks, protocol exploitation flooding attacks, etc. Compared to layer-3 attacks, application-level DDoS attacks (Layer-7 attacks) are thought to be more complex and difficult for filters to identify. IoT devices are becoming more and more common, and because they are continually connected to the Internet with minimal security configurations, have significantly increased the vulnerability of these networks to attackers. These networks have

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

consequently emerged as the new most vulnerable link in a network's security chain in the current day. Therefore, the IoT devices have drawn many negative actors, especially those planning for large-scale DDoS assaults, due to their distributed nature, pervasiveness, and extreme vulnerability.

1.2 Internet of Things (IoT)

The IoT has gained enormous attention from the research and academic communities and has become a significant component of our daily life. Business as a result of the increasing use of IoT devices in daily life. The International Telecommunication Union defines the Internet of Things as a combination of hardware and software components(ITU) that may run many services simultaneously using both TCP/IP and non-TCP/IP protocols according to the definition provided by the Internet Engineering Task Force (IETF). The Industrial Internet of Things (IIoT), the Internet of Anything (IoA), the Internet of Everything (IoE), the Social Internet of Things (SIoT), the Web of Things (WoT), and the Internet of Medical Things (IoMT) are just a few examples of IoT applications and deployment scenarios. Multiple issues, including how to handle the massive amounts of data effectively, are brought on by the rise in connected devices and the problems with Big Data management, privacy and provenance, mobility management and handover, and privacy and security challenges. Interoperability between diverse hardware and software platforms. We observe that the research community is making a variety of attempts to enhance the functionality and scalability of IoT networks e.g., the use of edge computing to complete resource-intensive tasks and the usage of SDN for programmability and flexible management A new mix of Software-Defined Internet of Things (SDIoT) architecture was introduced, as well as flexible network programmability, for effective management.

II. LITERATURE SURVEY

Due to worries about security flaws, there have been many arguments against the Internet of Things since it first emerged. Networks, operating systems, software, and hardware are all susceptible to violations. Hackers have successfully taken advantage of various systems and devices to access resources, damage them, and bar legitimate users from using them.

A. The Vulnerability of IoT Devices:

TABLE 1:PRESENTS THE LIST OF VULNERABILITIES ON IOT DEVICES [2]

Vulnerability	Weak points
Insufficient validation and authorization	• Poor password • Weak password recovery systems • Unsecured credentials
Untrusted user interfaces	• Low login credentials, plain text credentials • In the absence of encryption, data can be compromised.
Network is not reliable	• Sensitive network facilities can be used to attack target.
Privacy problems	• Untrustworthy end points, not strong authentication,non-encrypted transmitting, and exposed network facilities that let attackers access poorly protected data .

Fig 2.1 Vulnerabilities list

B. Protocols on IoT:

1) There are many researches that have been mentioned as protocols for Internet of things with different advantages and disadvantages.

2) Constrained Application Protocol(CoAP):

- It is a deployment protocol designed for lightweight machine-to-machine connections in restricted networks.
- Easy interaction with HTTP.
- **No Sec:** It is presummated that the transmitted message lacks security.
- **Pre shared Key**: support Programmed sensors using Symmetric cipher keys.
- **Raw Public Key** for devices requiring authentication using the public key.
- **Certificates.**

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

3) Routing Protocol Low Power and Lossy Networks (Routing-RPL):

- Network layer using IPv6.
- Assures message integrity and secrecy.

4) 6LoWPAN:

- It is open source and utilised in the network layer for direct Internet connectivity.
- Alternative for IPv6.
- The layer has numerous vulnerabilities that can be used by attackers since it lacks safety.
- In research showing IPSec is employed in the suggestion solution.

5) 4. 802.15.4 Protocol

- It works in the physical layer and mac layer.
- It provides protection and security by using encryption Cryptography.

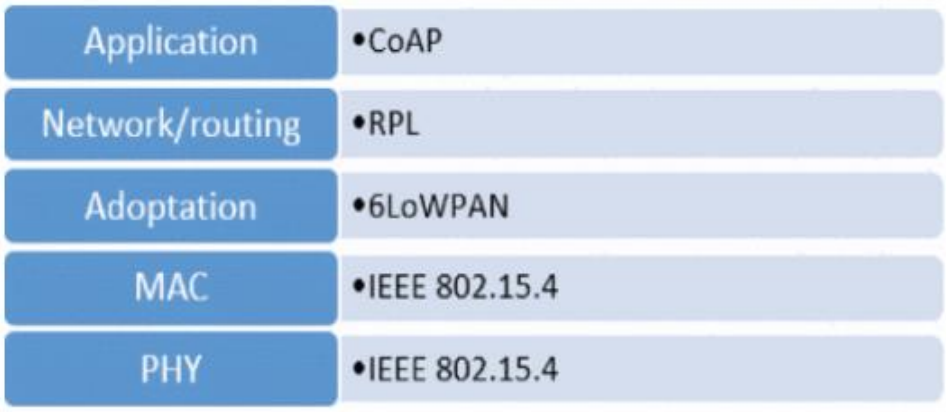

Fig 2.2 Protocols

C. DDoS Attack Classification on IoT:

IoT is divided into the three essential layers of observation, network, and application, and DDoS assaults vary depending on the layer:

1) DDoS on Observation Layer:

- RFID: A method for obtaining and reading data from sensors included in Internet of Things devices, without any direct human influence, and this is where potential attacks like jamming, kill command attacks, etc., could happen.
- To restrict access to services, Confusion is used as a layer relay.

2) DDoS on Network Layer:

Attacks against wired and wireless networks at the network layer, where massive amounts of data are fed to carry out the assault, are most likely to occur. The data-receiving system continues to make efforts to stall the processing of requests and the resources until there are no direct connections, the necessary resources can be made, which ultimately results in the service being stopped.

- DDoS on Application Layer:In the application layer, which includes the fundamental user interface (smart cities, smart governments, smart devices, etc) via which it utilises applications. Reprogramming Attacks and DoS based on a path are two sorts of attacks that can happen in this layer.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

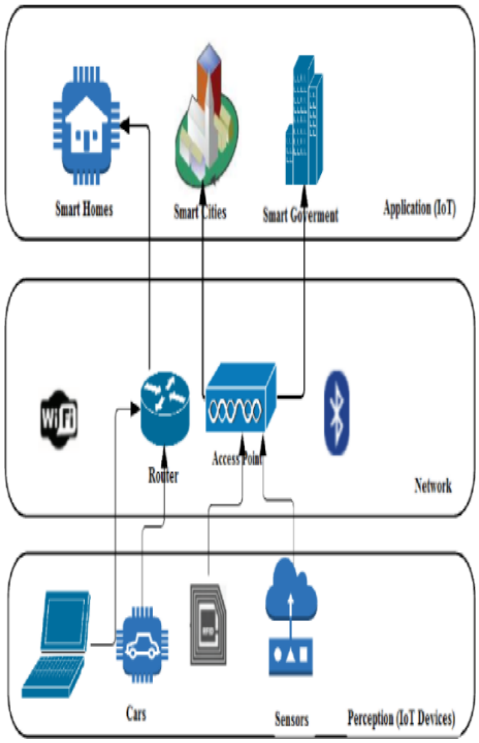

Fig 2.3 IOT architecture.

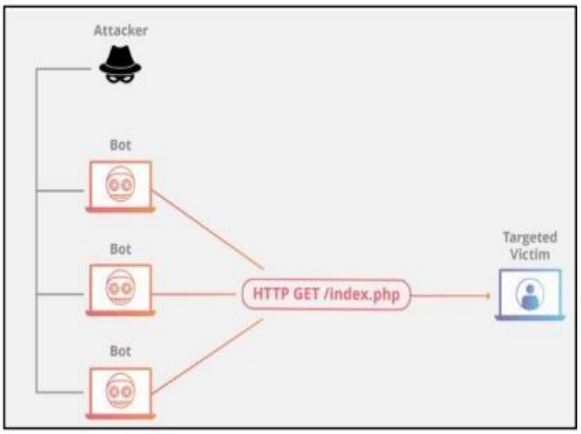

Fig 2.4 DDoS attack.

D. Example of DDoS Attack on IoT Devices:

Due to the interconnectedness of Internet of Things (IoT) devices, a favourable environment will be created for the occurrence of distributed denial-of-service (DDoS) assaults, and because of this, malware (such as bots and zombies) can be readily implemented and spread on it.

1. Mirai:

Infects the Linux systems.

2. Wirex:

Infects Android mobile phones.Google fixed the issues by removing several applications from the Play Store.

3. Reaper:

Major firms like Cisco and Linksys have been impacted by this bot's capacity to search for weaknesses and vulnerabilities in Internet of Things devices.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

4. Torii:

Recently, Torii has been covered. It can target the majority of today's most modern PCs, smartphones, and tablets with architectures like (64-bit), x86, ARM, MIPS, etc.

E. Defend DDoS Attack on IoT Devices classification:

1. Classical DDoS Detection:

- Mitigation flooding:

This defence, which uses technology to route the destructive deluge through a middleman and onto an external server, includes a fee-based arrangement for the mediator to safeguard Internet of Things devices. This method is employed in attacks with a huge scope.

- Detecting Intrusions:

1. Network traffic detection:

It was regarded as one of the more traditional methods of preventing distributed denial of service attacks on Internet of Things networks, which employ a model to cross all system layers or which are directed towards the system layer model. To stop these attacks across all network and system architectural layers. This method consists of a series of processes that start with capturing the attack, continue with identifying the hacker type, and end with the defence operation. When it determines in the first phase that the amount of traffic to be served is very large by measuring and comparing with the capacity of traffic, the defence procedure is comprised. The compromised gadget that sends a lot of requests that are greater than usual is then located and may be easily destroyed.

Machine learning was utilised to gather additional data on the attack rate with the usual traffic rate due to the mechanism's inability to stop all attacks using this technique.

2. System workflow detection [9]:

It is also one of the more traditional methods for identifying attacks, and it involves building a honeypot (database) to hold questionable packets and system workflow. In the suggested plan, honeypots are employed as a trap for intruders hoping to compromise the system's security. A honeypot is designed to lure in attackers with the intended purpose, as its name suggests that to watch and examine how they initiate an assault by gathering data about the attacking agent, such as malware [8]. Therefore, it examines each request that comes to the server. When a request raised suspicion, In order to safeguard the main server from intrusion, it routes this request to the honeypots. Additionally, it checks the IP address of the machine that launched the attack and keeps the information in a different database from the main servers.

Each request is thereafter analysed and compared to the honeypots content based on these records.Based on these records, each request is then examined and contrasted with the information in the honeypots.

2. Modern DDoS attack Detection:

1) Malicious software Detection:(Using machine learning)

Many learning machine algorithms that can recognise distributed denial of service threats have been discovered. Because of the extensive testing this mechanism undergoes, it is possible to determine how different Internet of Things device networks behave.

In a research paper published after these algorithms were evaluated by Princeton University, [6] "We evaluated five machine learning algorithms to separate legitimate IoT packets from packets used in DoS attacks: closest K neighbours KD Tree algorithm, linear kernel support vector machine, Gini impurity scores are used in a decision tree, random forest, and neural network (NN) systems".

When they claimed in their research that these algorithms produced results that were worthwhile and inspired them to keep going to further develop them and keep an eye on IoT device networks. Implementing this will enable accurate numbers to be reached in a more realistic setting. It is possible to deduce statistics that aid in the detection of distributed denial of service attacks.

DOI: 10.17148/IJARCCE.2023.125132

2) Prohibition Techniques:(Using Middleware like SDN) [7]:

It is a technology where software with the goal of defending (SDN) is specifically designed to interact well with IoT devices. One of the most difficult issues in network security is identifying malicious packets on a given network path. We contend that the introduction of Software Defined Networking (SDN) presents an exceptional chance to efficiently detect and counteract DDoS attacks[8]. SDN middleware then its primary goal is to reduce attack damage by utilising the features of the software. While it is operating, it gets data from the IoT environment and stores all information pertaining to user interactions with IoT devices.

Alerts are given when unexpected interactions are found so that the necessary blocks can be made later. That was developed by software, whose task it is to identify any transmissions that are not balanced: such as boosting the quantity of messages, sending noticeably more packets, detecting malicious entries at ports, and after the programme has found these exploits, it sends the work to another instrument to stop them. At this time, online services and apps using algorithms can successfully enforce prohibition against DDoS attacks. We discovered a method used to put this concept into practise at Georgia Institute of Technology. They presented - an architecture they named "ShadowNet" that makes the edge defending the first line of defence against IoT-DDoS and meets its goals in the attack defence .

3) Blokchain Defense [2]:
As organised data are maintained in the blockchain, the process employed to safeguard IoT devices is a modern defence strategy. IoT devices are connected to servers in a sequence. Launched applications for IoT devices integrated into this blockchain, with the status being reported each time a server and IoT device interact.

It would be preferable to monitor and secure IoT devices using blockchain when they are located in significant buildings and cities.

F. COMPARING AND CLASSIFYING IOT DDOS SOLUTIONS:

Any system must guarantee the confidentiality, accessibility, and integrity of data in terms of information security. DDoS is by definition an attack on the accessibility of data or services. Utilising availability attacks initially involves having access to private resources. It is only an assault on the privacy of data. Data integrity is completely compromised because it is also unknown what an attacker's goal is when unauthorised access happens. Simply put, an information security semantics-compliant IoT network must be in place. IoT was formerly divided into three layers in section II: an application layer, By all ways, a network layer and a perception layer that provide security on all of these tiers and more would be the ideal answer. Sadly, to the best of our knowledge, there isn't yet a perfect answer. The prior study has largely focused on network technology rather than the physical or software components of IoT, making it difficult to categorise. As a result, the only comparison that can be drawn is regarding the IoT's vulnerabilities and whether or not they have been fixed.

We have observed that the majority of the suggested DDoS solutions are network-focused and employ SDN techniques. The preceding methods have a significant flaw in that they did not take into account all IoT vulnerabilities before being implemented. The advantages of SDN and virtualization, as well as how they could safeguard networks more generally, have received all of their attention. IoT is a little bit different from traditional networks, thus theory does not apply. The information that these devices process and the environment in which they are used are the only factors that make IoT unique. IP tracking is not illegal or unethical in this situation, but if the suggested approach is used in a hospital, any traces coming from outside the facility will be viewed as malevolent. Trace redirection for healthcare data would be absurd and raise serious ethical concerns regarding data protection. It is quite difficult to determine whether only one solution can be modified due to the diversity of IoT devices.

SDN and NFV together have produced superior results in terms of reducing vulnerabilities. Due to the separation of the data planes, they have been able to provide trace and port analysis as well as enhanced authentication and authorisation. In Table 1, altering the default access privileges and passwords resolved the issue of insufficient authentication and authorisation. It is unclear how the authors came to this result as this has nothing to do with networks.

It is clear from this situation that consumers of IoT, not IoT providers, must handle the application layer solution. The implementation of SDN with IoT and the integration of SDN and NFV in IoT have not differed much from one another. In order to address IoT security challenges, all vulnerabilities must be eliminated, decreasing to zero percent the likelihood of dangers and vulnerabilities. IoT is not the solution to this problem.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125132

It takes a combined effort from the two, neither from manufacturers nor from network users. Better port and trace monitoring can only be achieved by concentrating on the network architecture, nd claiming additional benefits is not possible. Data encryption across the envisioned network was one significant issue that was left out. A hopeful supposition would be that because establishing an HTTPS connection is so typical, it would be disregarded when recommending a network configuration.

CONCLUSION

This study's goal was to examine the DDoS attacks in IoT and IoT security flaws enable DDoS attackers to carry out their objective. The problems with IoT were discovered to include; insecure networks, lack of encryption, insecure software, and authentication and authorisation. In this paper, existing strategies for preventing DDoS in the Internet of Things were listed, and the majority of these solutions involve the use of NFV and SDN, two types of network technology. These two network technologies were combined to create the most reliable solution. In order to anticipate a DDoS attack, this method placed a strong emphasis on automated traffic analysis. It was also suggested to use Fast Entropy methods to enhance traffic analysis. After that, a review of the unfinished business and remaining voids.

REFERENCES

[1] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.
[2] Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): 71
[3] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security 19.5 (2017): 653-659.
[4] Pajila, P.B. and E.G. Julie. Detection of DDoS Attack Using SDN in IoT: A Survey. in Intelligent Communication Technologies and Virtual Mobile Networks. 2019. Springer.
[5] Doshi, R., N. Apthorpe, and N. Feamster. Machine learning ddos detection for consumer internet of things devices. in 2018 IEEE Security and Privacy Workshops (SPW). 2018. IEEE.
[6] Biswas, Kamanashis, and Vallipuram Muthukkumarasamy. "Securing smart cities using blockchain technology." High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE, 2016.
[7] Alison DeNisco Rayome. 2017 (accessed April 9, 2018). 33% of businesses hit by DDoS aŠ ack in 2017, double that of 2016. hŠ ps://www.techrepublic.com/ article/33-of-businesses-hit-by-ddos-aŠ ack-in-2017-double-that-of-2016. (2017 (accessed April 9, 2018)).
[8] Lee, Boohyung, and Jong-Hyouk Lee. "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment." The Journal of Supercomputing 73.3 (2017): 1152-1167
[9] Dorri, Ali, et al. "Blockchain for IoT security and privacy: The case study of a smart home." Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on. IEEE, 2017