*I.J. Wireless and Microwave Technologies,* **2022, 3, 18-32**
Published Online June 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2022.03.02

# Analysis and Detection of various DDoS attacks on Internet of Things Network

**Atika Bansal, Divya Kapil, Anupriya, Sagar Agarwal**
School of Computing, Graphic Era Hill University, Dehradun, Uttarakhand, India

**Vishan Kumar Gupta**
Dept. of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
Email: vishangupta@gmail.com

Received: 03 February 2022; Revised: 10 March 2022; Accepted: 05 April 2022; Published: 08 June 2022

**Abstract:** Internet of Things is used for those devices, which are connected over a network, once the devices are connected to the internet they are known as smart devices. These devices share information and communicate with each other to influence our day to day lives. Due to the rise in these devices, security is compromised. Malware is malicious software that can damage the computer, server, or network intentionally. Malware can also exploit the confidentiality, integrity, availability (CIA) triad. Rather than the traditional malware, IoT malware can damage different internet connected devices such as routers, DVRs, CCTV, or many internets connected devices. The IoT devices are more vulnerable due to weak passwords, missing authentication schemes, backdoor entries, lack of high-security algorithms, and plug and play services. There is no widespread survey available about IoT malware in an efficiently organized manner, publicly. In this article, we have classified the IoT malware according to their release and provide on the basis of their functionalities, growth, revolution, and their detection mechanism. We perform DDoS attack on Raspberry PI to hamper the home automation system. We employ Wireshark to monitor network traffic and demonstrate the service unavailability.

**Index Terms:** IoT, Malware, Malware family, DDoS attack, IoT Botnet, Threats to the IoT.

## 1. Introduction

IoT helps the traditional “dumb” objects to become smart by giving them a platform to talk to each other and take collaborative decisions to benefit humans [1]. The idea looks very exciting when we think of gathering and controlling our day-to-day objects that are remotely available. As the idea flourished, the firms started to compete which each other to take market share that made these businesses develop IoT devices as quickly as possible [2]. All the vendors started making quantity, because of this the security was compromised, which could lead to several severe consequences. The spreading of more and more connected ensure devices means more possibilities for attacks, the hackers can hack our devices, gather the information, control our devices which means controlling our life. A large amount of connected IoT devices soon became a target for many malwares, building a malicious army (termed as “botnet”) [3].

It is known that the internet is full of insecurities, with some threats which have little consequences to others which may be life-threatening [4]. One of these threats is a new family of threat called Botnet, which is considered the most pernicious one. When several internet-based devices such as computers, routers, CCTV systems, DVRs are infected and operated by a common attack, such as flooding, DDoS, phishing come together, called a botnet.

These botnets are different from other malware because the hold a channel of communication with the attacker who controls and issues commands to the network of bots to perform malicious actions. The most common attack that is popular and common amongst this malware is DDoS (Distributed-Denial-of-Service) attack. The DDoS attack works by attempting to exhaust resources like bandwidth, CPU, etc. of the devices on the internet to downgrade the services for example, it may overwhelm a web server by issuing junk commands that lead to dropping in the legitimate once. The attacks launched from the distributed environment are more damaging because they can use distributed resources to overload the target and they require advanced techniques to overcome. Botnets include a C&C server (Command-and-control) which keep continuous contact with the active bots and allows its operators to issue commands [5]. In addition, the malware involved in IoT, which is responsible to make it network of vulnerabilities uses, a common type of method to make their way into the devices. Many of them use weak credentials brute forcing to penetrate the devices. Once the make their way inside, they start downloading malicious binaries to infect the device for which they may carry

downloaders as well. Due to such a boom in the demand of IoT devices the security has been compromised, but it is advised to the users that they must change the default passwords as soon as they start using the device [6].

In this paper, we have performed literature review in Section 2, Section 3 presents a classification of IoT malware according to the year in which they were launched and a brief introduction of the malware is given with the target devices and the method that they use to get into the system. Section 4 presents a threat model on which we have tried out the experiment. Section 5 demonstrates the methodology of the work. Section 6 discusses the experiment setup, tools, and technique used for the execution. It also presents the results that produce after experiments. Finally, conclusion is exhibited in Section 7.

## 2. Literature Survey

Ankush R Kakad et al. suggested that the signature-based approaches are the simplest to execute and identify the main kinds of viruses but this method cannot detect the novel attack. In this research article, they have classified the viruses as transient and resident. Here transient means the virus is dependent on the life cycle of the host i.e., this malware terminates when the life of the host ends, whereas resident malware attaches itself to the memory of the system and works as a separate application even when the program terminates [33].

Savan Gadhiya et al. proposed that there can be two methods of detecting malware static and dynamic. Dynamic detection is considered the best one for malware analysis because it executed the malware code in a controlled environment and then analyzes it. Here also, mostly the emphasis is given to sandboxing method of malware detection. In sandboxing technique, a virtual environment is created which isolated the malicious code to run so that the rest of the system functions properly [34].

Rabia Tahir shown the classification of the malware which are threats to the computer world. Two main analysis techniques, static and dynamic are discussed in the paper. The results show that static analysis function better, and its accuracy is higher in multipath malware when compared to dynamic analysis. Whereas dynamic analysis can analyze complicated and polymorphic malware, its accuracy is not that good. Three malware detection techniques are also discussed: signature-based, heuristic, and specification-based detection. Dues to the rapid advancement in polymorphic malware, the heuristic approach is combined with machine learning to get more accurate and efficient results [35].

Amin kharaz proposed a system UNVEIL: which is a novel approach to detecting and analyzing malware. The study detects the typical behavior of malware such as encryption and folder lock. The system was able to correctly detect 13,637 malware samples from different origins in real-world data with zero false positives. UNVEIL prototype was developed on top of the open-source malware analysis framework Cuckoo sandbox [36].

Sonali Sharma et al. stated that different viruses can damage the system by manipulating the vulnerabilities. The attacks of malware like the “WannaCry” malware manipulated many vulnerabilities and caused damaging effects on the money and property of the public. It also gives knowledge about creating a system that can safeguard the system by constantly monitoring it and keeping it updated about upcoming vulnerabilities [37].

Samuel Ndichu et al. proposed that there are three main areas that are of concern in remote access security namely, remote devices, access method, and target resources. There are factors that play an important role when exhaustively securing the system such as tunneling. The encrypted traffic technique provides an immense advantage in terms of data privacy and security of data transit. Though the very basic thought and benefits of encryption technology are used by attackers to prevent, detect, and respond, thus negotiating privacy, integrity, and availability of data [38].

Jagsir singh et al. proposed a deep-learning approach for malware classification problems. On Malimg dataset, the CNN model is combined with data preprocessing and enlargement techniques and obtained results which are much better than the existing approaches. Another hybrid approach is performed where CNN is combined with L2-SVM and it boosts the performance by 1.56%. The proposed model accomplishes more precise results with negligible amount of misclassification in less time and computational resources [39,40].

## 3. IoT Malware Classification

The attacker finds a way to get into several connected IoT devices utilizing brute-forcing the general credentials and the devices which are not having the common credential changed to get into the class of vulnerable devices. Once the attacker finds such devices it attacks those devices by majorly the DDoS attack. Figure 1 discusses the scenario for the attacker, where is a pool of all the IoT devices and an attacker. Here we are going to discuss some malware related to IoT infrastructure from the year 2014 to 2019 and a summary is tabulated in Table 1.


Fig.1. Scenario for attacker

### *3.1. Linux.Wifatch*

An open-source piece of software which is also known as Zollard and Reincarna introduced in November 2014 and comes under the malware which does not harm other devices rather they secure the devices from other malware. The thing that is uncommon with this malware is instead of launching any malicious code for attempting a DDoS attack; it has hardcoded subroutines that were implemented to secure the target devices. It infects the target by cracking the same weak telnet credentials, once entered it removes all the malware, offers code for debugging, and disables the telnet after that by flashing the message to change telnet credentials. "Telnet has been closed to avoid further infection of this device. Please disable telnet, change telnet passwords, and/or update the firmware". Not only it removes the malware, but it also reminds the user to update the router's firmware whenever it sees an incoming request for a telnet connection.

Linux.Wifatch code is written using Perl language that could be obfuscated but the author chose not to. The DVR it infected were Dahua DVR CCTV systems and Wifatch has a module dahua.pm, which has the configuration to automatically reboot the devices every week (maybe to kill the infection).

Despite the actions, which it does to protect the devices, we should also take into consideration that Linux. Wifatch is a piece of code that enters the system and infects it without consent and so it is the same as other malware. Most of such activities are happening because of loose Telnet connections using weak credentials. It can be removed by resetting the device, but the device can become infected again over after some time. It is advised that the users must keep the firewalls up-to-date and should practice changing the default credentials [3] [7]. The malware allows the user to download and run the malware themselves by issuing the below commands to download:

**wget -O .net_bn ***
**wget -O .net_pl ***
**to run:**
**chmod 700 .net_bn**
**. /.net_bn -run**
**To kill the bot:**
**. /.net_bn -bnkill**

If internet access is there then it will connect to the P2P network, and download modules, which are an extension to upgrade the bot. It might be connected to other nodes to disinfect, but it comes with no guarantee, etc.

### *3.2. TheMoon*

The Moon is an IoT botnet that appeared in around 2014 and its major mode of infection was to get over the vulnerable IoT devices and routers within broadband networks. The main devices it targeted were Linksys, D-Link, ASUS, and MikroTik routers. The attacks carried out by this malware were typically brute force attacks, DDoS attacks, and some other malicious actions. This malware continuously senses the other vulnerable devices and influences them to spread from one device to another creating an army of botnets.

Another interesting thing about this malware is that after acquiring home routers and modems it creates a proxy and uses it to rent the network. That allows it to be sold-as-a-service to other malicious actors, which intend to use it for unwanted actions like launching DDoS attacks or launching suspicious YouTube videos to generate a large amount of revenue from advertising. TheMoon botnet module was only deployed on MIPS based devices which is a common microprocessor architecture that is mostly found in home gateways and modems. Once the routers are compromised,

they scan port 80 and 8080 as fast as possible to engage the whole bandwidth available. The malware works by first requesting the firmware and model of the router by issuing HNAP (Home network administration protocol), which is used to collect the identification, management, and configuration of network devices, and once it finds a vulnerable device it executes a CGI (Common Gateway Interface) script to get control over accessing the local commands over the device. TheMoon botnet can also bring down servers and their web offerings by prodigious them through service requests, which they cannot handle. Also, it can be used to obfuscate the transfer of online information or setting up some illegal sites or methods to make money.

The malware brute forces the common credentials, gets a way to get inside the device, they transfer the malware, and that malware gets installed on the computer. This malware turns the infected device into SOCKS5 proxy which was used to filter the internet traffic which allows the botnet authors to sell these proxies to sold-as-a-service to other actors [8]. To detect whether the system is under the influence of this malware you can execute the below command:

**echo [-e] "GET /HNAP1/ HTTP/1.1\r\nHost: test\r\n\r\n" | nc routerip 8080**

If you get an XML HNAP reply that means your system is under influence of the malware and some actions need to be taken. The users are advised to disable the remote administration of their device or to allow the rights to a few trusted IP addresses.

*3.3. Spike/Doofloo*

Spike is also known as MrBlack, it is a type of malware that affects routers, PCs, Servers, and IoT devices and eventually spreads from one device to another. Majorly the actors to launch a DDoS attack on the mentioned devices use it. The toolkit has several DDoS payloads including DNS query flood, GEET flood, UDP flood, etc.

This specific malware not only affects Linux based systems but also affects Windows and ARM architecture-based devices. The victim devices are exploited by using the weak credentials to enter the system and infectious binaries are then dropped. Spike toolkit can create three types of binaries:

- 32-bit Linux Binary
- 64-bit Linux Binary and
- 32-bit ARM-based Binary.

Once these binaries are configured, they run on the victim device. DDoS attacks that exploit IoT devices are very trending these days because they lack security in their devices and their software are hard to update. Spike botnets can be avoided by using access control lists, also SNORT signatures (the rule assumes that the host header and domain not more than 58 bytes) are issued which can help the administrators to avoid such attacks.

*3.4. BASHLITE*

A kind of IoT malware that is responsible for launching a DDoS attack introduced in 2015. It is also known as Gafgyt, Lizkebab, Qbot, Torlus, and LizardStresser and it victimizes mainly the Linux Operating System. Earlier the malware used to be called under the name of BashDoor also; the speed up to which it can launch the attack is 400 Gbps. At first, it used a bug in the bash shell to exploit, which is the ShellShock software bug in which the attacker can cause the bash to execute some arbitrary commands and obtain unauthorized access to the internet-based services and devices that use Bash to process the request. The tool which was used is BusyBox which is a software suite that has many Unix Utilities in a single executable file. It runs on many operating systems such as Linux, Android, FreeBSD, and many of the tools provided by it were designed to run on Linux Kernel provided interface.

The major portion of the targeted devices were CCTV cameras and DVRs which were mainly located in Taiwan, Colombia, and Brazil. The capability to stream videos means a lot of available bandwidth which makes the devices a powerful tool for attackers to use for DDoS. A DDoS attack can flood the web servers with some unwanted requests which in turn causes the legitimate ones to be dropped [3][9].

BashLite is written in C and has to capability to cross-compile on any architecture, but the most common feature is that it can launch several types of DDoS attacks, which includes sending several strings of meaningless characters to TCP or UDP ports, occupy TCP connections, or continuously send TCP packets. It uses a Client-server architecture to command the bots and control them where the protocol used is a lighter version of IRC (Internet Relay Chat). The total ecosystem of Bashlite consist of six agents:

a) Command and Control Server (C&C): The interface interacts with the bots. It accepts the instructions from the attacker and controls the malware-ridden devices to broadcast malicious commands.
b) Bots: These infected devices collectively form a botnet. They receive the commands from C&C and executes them.
c) Malware Servers: it has all the resources used by the botnet such as shell scripts and binaries.

d) Loaders: After successful login to vulnerable devices, the loader downloads and run the botnet malware, converting the device into a new bot.
e) Scanner: This is an agent that continuously senses the Telnet and SSH servers to attempt to login and find the vulnerable devices.
f) Database: to stores the information that a botnet gathered.

The prevention method of this malware is to disable the telnet and SSH services [10]. Besides, the user must change the admin password for Telnet.

*3.5. Mirai*

Mirai is the most powerful malware that affects IoT devices. Mirai means "the future" in Japanese and was launched by Paras Jha to make a profit. The speed with which it launches the attack is up to 1Tbps. The working scenario of this malware is that rather than making use of complex techniques to track down different IoT devices on the internet, it scanned a big chunk of the internet for open Telnet ports and then attempt to login using the default username and password combination which were never changed. It works by scanning the IP addresses with the open ports 23 and 2323. By doing this it was able to create an army of bots or zombies which mainly targets CCTV cameras, routers, and home appliances and then collect a large amount of data from them, which in turn was then sent to the targets (in case of Mirai it was large web hosting companies which were responsible for taking offline many popular websites). Initially, this only infected Linux based systems but now there is also a version which can affect windows machine, increasing the threat. It is, therefore, necessary for you to practice safe web-browsing and use some internet security programs.

The device which is infected will continue to function normally except for some occasional sluggishness and extra use of bandwidth. Though a reboot will disinfect the device for a while, it needs a quick change of the admin password, otherwise, the device will become infected again within minutes. Also, the user must change the default username and passwords of the devices on the internet for security purposes, as you may not even know that your system or device is under the influence of some malware, or it is one among the botnet army and is instructed to launch Malware activities. The standard detection methods of the malware are traffic analysis, NetFlow, honeypot data, open/closed ports, etc. With the source code leak, hackers have found many new ways to upgrade it to avoid detection and go deep into the systems. New versions of this malware can be seen almost every day e.g., AirDropBot and GUCCI were discovered recently in October 2019.

Mirai botnet is different from the rest as the scale is larger than anything seen before, this allows it to generate a large amount of traffic to be launched. These attacks can take down the best-defended services like Twitter, Facebook also.

*3.6. KTN-RM/Remaiten*

KTN-RM has gained its functionality from two malware

- Tsunami and
- BASHLITE.

It inherits the DDoS attack launching capabilities from the Tsunami and from BASHLITE it inherits the Telnet scanning feature and also has some extra improved features above both of its predecessors [3].KTN-RM is an infection that infects Linux on embedded devices utilizing brute-forcing the set of username & password used previously. The techniques it uses for spreading itself is by carrying a downloader along with itself which checks the underlying architecture and drops the executable, which in turn downloads extra software in infected machines & executes them. Once executes it changes its name to look legitimate one. When executed on the victim machine it connects to the bot's command and control server and sends matching architecture commands. C&C responds with bot binaries on whose success bots run in the background. Randomly bot is connected to C&C server which accepts bots request to connect & send instructions to perform malicious actions such as flooding. Remaiten is a type of bot that does not let others know of its presence, it can hide in the system and secretly perform its actions. There are many IRC commands which are supported by this bot which includes "PRIVMSG" which is used to instruct the bot to do some malicious actions like downloading unnecessary files, flooding, Telnet Scanning, etc. Some of the features which have been seen on this malware are the capability to kill other processes, this majorly includes killing other malware instances [11]. This malware penetrates themselves into the network because of the vulnerabilities in security routers, with the help of which it gains access to the complete network.

*3.7. Linux/IRCTelnet*

This malware is the successor of Mirai and was discovered by the security researchers at MalwareMustDie.org. The major task of this malware is to create fresh botnets that could be used for conducting a DDoS attack on vulnerable IoT devices. The devices include CCTV cameras, DVRs, and routers. It is built on the core code of Aidra, which was previously known to launch DDoS attacks. It inherited some of the properties from its predecessor as BASHLITE (Telnet

scanner and malicious piece of code injection) and Mirai (leaked credential list). The techniques used are TCP flood, UDP flood, and both IPv4 and Ipv6. The malware targeted IoT devices by using telnet scanner function, which means it brute force the known credentials by the command sent through CNC malicious IRC server. The malware infected 3500 devices within 5 days of its first detection. This botnet attack first came from countries like Turkey, The Philippines, and Moldova. The message that was hardcoded in the malware was in the Italian language, which suggests that the author is an Italian speaker. The researchers suggest that the working of the malware can be as follows:

- The source of the attacker was all the infected IoT devices (routers and modems), and the attack was started by brute-forcing the credentials.
- On successful login, the commands were executed: "shell"," sh" and "free", then one-liner shell command to download and install the malware.
- Now, the attacker executes "/etc/firewall stop" command to close the connection.

*3.8. IoT Reaper*

IoT Reaper is the successor to the most damaging malware, Mirai that took down the world's top online websites by enslaving the IoT devices such as routers, CCTV systems, and DVRs. After Mirai, a far more powerful malware of IoT attack appeared which was names "Reaper" or "IoTroop" which did not try to get inside the devices using loose credentials but spread via loose security points in IoT hardware and software. The difference between both the malware is that one is checking for an open door to get inside, and the other is intelligently picking up locks. It is also declared that over 2M devices were already attacked by it, and its rate of spreading is also very high. The potential of this malware is far more than that of Mirai because it does not use the weak credential list, but it has 9 (to be precise) parameters with which it can penetrate. Its target devices are D-Link routers, Netgear, Linksys, and internet-connected devices which include CCTV cameras, etc. This malware has been seen operating on MIPS variants and ARM variants architectures [12]. The working of the malware is:

a) Initializing itself by obfuscating the String, ensuring the malware runs all the time, and preventing the device reboot.
b) It kills any open Telnet process using port 23/TCP and scans the memory for any existing malware.
c) For vulnerability scanning, random IP addresses are generated, and then a set of vulnerability test is executed on these IP's.
d) Command and Control communication: A list of all the vulnerable IoT devices after their weaknesses have been identified is collected by the server.
e) The infected devices continuously sense the channel for any command issued by the controller. Once the command is received, the device performs the action which has been instructed.
f) Downloading the binaries.
g) Execution

It is advised every user must think of security whenever using an IoT device, keep your router's firmware up to date.

*3.9. BrickerBot*

BrickerBot is a type of malware that claims at permanently destroying the vulnerable/insecure IoT devices. It attempts to log into insecure IoT devices and run certain pernicious commands to disable them completely [10]. This malware is retired after being attacked by the Radware honeypot (honeypots are the security mechanisms that are used to detect and clean the attackers). The attack used by this malware was Telnet brute-forcing- the same which Mirai used to log into the victim device. How this malware is different is that it does not download the binaries, this is the reason Radware was not able to generate the list of attempted username/password pair. Once logged in successfully, the bot performs the Permanent Denial-of-service attack by issuing a series of Linux commands, which leads to corrupting the storage, internet connectivity, deletion of all the files [13]. The target of these devices is Linux/BusyBox based IoT devices, which have an open Telnet port and are publicly connected to the internet. The devices which are exploited by BrickerBot needs to be reinstalled or replaced in some cases when the firmware is rewritten by the malware. To protect the devices from these types of attacks, one must take the following steps:

a) Disable Telnet access.
b) Network Behavioral Analysis can analyze the traffic and detect anomalies.
c) Change the default credentials.
d) User/Entity Behavioral Analysis.

*3.10. JenX*

JenX is a new type of IoT botnet, which came and started spreading in early 2018. It started recruiting the devices on the internet and offered a speed of 300Gbps attacks. Hosted servers were used to find and infect the IoT devices and

used the one out of two popular vulnerabilities in IoT botnets: CVE-2014-8361 and CVE-2017–17215. It was based on the code of its predecessor (BrickerBot) and customized it accordingly. The origin of JenX came from game server operates who compete to get the clients by launching attacks against each other. The new and different thing in this malware is that it uses servers to scan and exploit, whereas all the other malware used the distributed form of attacks where a victim device will perform its search for a new victim. It works by executing its binaries which are called "Jennifer" and these binaries were seen in almost all the downloaded occurrences from the same servers which were hosted with different providers. Once the binaries are executed, it initiates 3 obfuscated processes entries in the process table. The localhost bound port is being listed by all the processes except the one which opens TCP socket at port 127 to the C2 server at obfuscated 80.82.70.202. Once the connection has established the bot and the C2 server sends 2 bytes packets to each other to keep the session alive. We can detect this by the sha256 and md5 Jennifer present for each MIPS, ARM, and x86 architecture [14].

Table 1. Classification of malware

| **Malware Family** | **Year** | **Target** | **Architecture** | **Type of Attack** | **Protocols** | **No. of Devices affected** | **Recovery** | **Detection** |
|---|---|---|---|---|---|---|---|---|
| **Linux.Wifatch[15]** | 2014 | CCTV, home routers | ARM, MIPS and SH4 | White DDoS | Telnet | more than 200000 | Resetting the device | - |
| **TheMoon [16]** | 2014 | Linksys routers | MIPS | DDoS, Video ad frauds | SOCKS5, HNAP | 1000 | Deleting the malware | 80 and 8080 logs |
| **Spike/Dofloo [17]** | 2014 | PC, Servers, Routers an IoT Devices | Linux, MIPS, ARM, Windows | DDoS | - | - | - | Presence of malicious binaries |
| **BASHLITE [18]** | 2015 | IoTDevices (CCTV and DVR mainly) | Linux | DDoS | IRC | 1000000 | Device Reboot | NetFlow, Packet Analysis, |
| **Mirai [19]** | 2016 | IP cameras, home routers | ARM, MIPS | DDoS | Telnet | 600000 | Device Reboot with a quick change of password | NetFlow, Packet Analysis |
| **KTN-RM/ Remaiten [20][21]** | 2016 | Routers and embedded devices | Linux | DDoS/Various UDP, TCP floods | IRC | - | Device Reboot with a quick change of password | - |
| **Linux/IRCTelnet [22]** | 2016 | Routers, DVRs, and IP cameras | Linux | DDoS | IRC | 420000 | - | - |
| **IoT Reaper [23]** | 2017 | CCTV, D-Link routers | MIPS and ARM | DDoS | - | 2M | Device Reboot | Attack Simulation |
| **BrickerBot [24]** | 2017 | BusyBox based devices such as webcams, smart bulbs, toys etc. | Linux | PDoS | Transmission Control Protocol (TCP) | 2 000,000 | Device Reboot | Network Behavioral Analysis |
| **JenX [25]** | 2018 | Gaming Servers | MIPS, ARM, ARM7 and x86 | DDoS | - | - | - | sha256 and md5 Jennifer presence |
| **Silex [26]** | 2019 | IoT devices | ARM, Linux, UNIX | Brute force | Telnet & SSH | 2000 in 2 hours | Reinstallation | System halt |

*3.11. Silex*

Silex is an IoT malware, which is found recently in mid-June 2019. It was developed by a 14-year-old hacker, which created a new tension and started targeting and destroying the IoT devices using weak passwords. This malware could only survive for a day or two but proved to be damaging for the IoT firms in such a short period. It is assumed that the C&C server is down, but the malware is still running on the infected machines. The malware proved to be catastrophic removing over 2000 devices in just an hour and required a complete reinstallation of the firmware to remove it from the victim machine. The basic entry point for the malware was the default username password of the devices that comes with it. The target machines fall under ARM majorly also covering Unix and Linux systems. The flow in which it behaves is first wrecking the storage, deleting the firewall rules in the second step, cutting down the network configuration in the

next step, and then finally stopping the device entirely. The victim machine shows a hardware failure behavior and does not give any sign of the malware. It is assumed that the hacker doesn't have any monetary reasons behind it because the malware runs with a note that it is just bricking the device so as they do not fall prey to any other malicious codes.

Table 1 shows all the malware discussed in this paper and bring them all together in sequence according to the years in which they appeared. It also defines the target devices of these malware systems along with the architecture in which they operate.

## 4. Threat Model

The picture given below is created to show the threat model. Here the threat at each layer (Perception, Network, Support, Application, Business) [27] of IoT is shown. The model describes what each layer of the architectures does and what are the possible attacks which can be there on these layers.

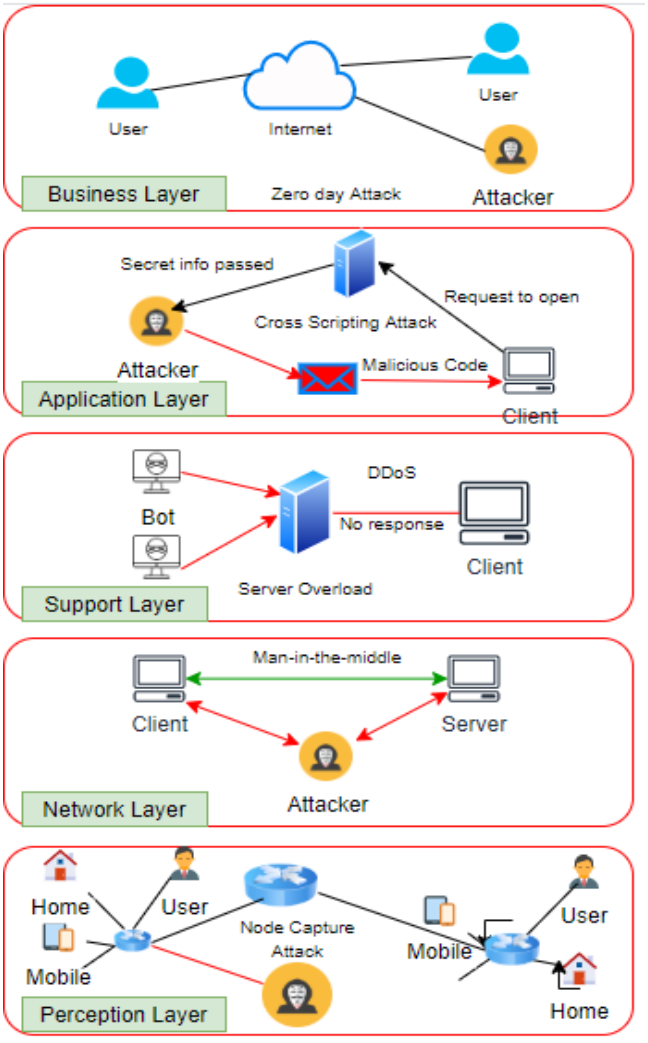



Fig.2. Threat model

The figure shows the threat model at each layer:

- **Node Capture Attack (Perception Layer):** This is the lowest layer of IoT architecture whose responsibility is to collect information from the environment or the object. The threat which is defined here is node capture which is one of the many in this layer. This attack defines that the attack gets hold of any of the nodes in the network and can perform any type of operation in that compromising the whole network [28].
- **Man-in-the-middle Attack (Network Layer):** The next layer in the architecture is the network layer whose main job is to connect the smart devices in the IoT environment and is also responsible for processing and transmitting the sensor data. The common attack here is the man-in-the-middle attack in which the intruder intercepts the conversation between the two systems. The attacker here is having the original communication,

which was going on and, in that way, he succeeds in making the recipient think that the communication is genuine [29].

- **Server Overload Attack (Support Layer):** It is the 3rd layer of the architecture whose task is to provide a connection between the application and the network layer. The attack that can be launched here is the Server overload or the DDoS attack where the intruder tries to make Bots, which continuously sends some commands to the server at a very high rate. The server gets busy taking the commands which are meaningless ignoring the ones which are useful [30].
- **Cross-Scripting Attack (Application layer):** The second layer of this architecture is the Application layer which has the responsibility to provide the interface between the end device and the network. The attack launched is a cross-scripting attack where the malicious code is injected into genuine and trusted sources. It is generally sent from the medium of web applications [31].
- **Zero-day Attack (Business Layer):** It is the top layer which is an extension to the application layer and has a responsibility to manage the whole system. The attack here is the Zero-day attack which is launched once the vulnerability in the software/hardware is exploited and the attacker uses this as an opportunity to release the malicious code before anything could be done about it [32].

## 5. Methodology

- In this section, we show some core aspects of our study. The IoT malware and embedded devices relatively recently gained headlines and achieved public attention due to huge damage and large-scale attacks. We emphasize known attacks at the layers of the IoT architecture. We also present a distributed denial-of-service attack at the support layer of IoT. For the DoS attack, we create an IoT environment using RASPBERRY PI and a virtual machine with Kali Linux that plays an attacker role. For this, first, network traffic among devices is sniffed. Then the network is scanned for finding the active hosts. Using the DoS tool, the access point is jammed and RASPBERRY PI is not accessible. In figure 3, we show the work flow of attack on IoT environment.

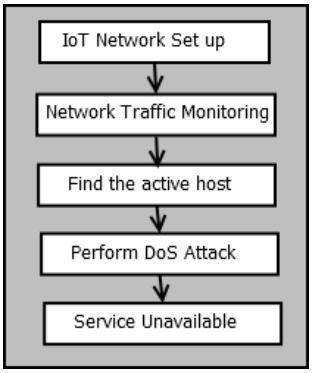



Fig.3. Work flow

## 6. Experiment and Results

The experiment and Results section consists of objective, tools, attack scenario, and steps of experiment with result. The major contribution of this paper is the experiment that we have performed. The attack is the de-authentication attack on IoT devices (Raspberry PI) and after the success of attack the home automation system will not work. The attack scenario explains to launch a DDoS attack on the home automation system to check whether it is launched successfully, and all the home automation services should be stopped, if it is successfully launched. For this experiment we use the following tools: Raspberry Pi: A compact single-board computer has no peripherals attached to it. AIRMON-NG, AIRODUMP-NG, AIREPLAY-NG: it is a tool that was used for accessing the Wi-Fi network security. This tool comes with the bundle of Kali Linux, and we need not install it separately. Wireshark: An open-source tool is used to analyze the network traffic state. The experiment is performed in a system with 16GB RAM, 512 GB SSD and Intel processor with 2.80 GZ. We use a virtual machine with Kali Linux as an attacker. We have a IoT devices network that is under DDoS attack. Using Wireshark, the network traffic is monitored and live host are identified using Nmap tool. The Wi-Fi adapter is set to the monitoring mode using Airmon-Ng tool. As the wireless adapter is in monitoring mode, we can analyze the traffic using Airodump-Ng tool. Aireplay-Ng tool is used to launch the DDoS attack. Attack is launched and successfully executed shutting down all the services.

*6.1. Objective*

The major contribution of this paper is the experiment that we have performed. We tried to launch the DDoS attack on an IoT device which in our case is a Raspberry PI. The attack is the de-authentication attack on IoT devices (Raspberry PI). The main objective is to launch a DDoS attack after which the home automation system will not work.

*6.2 Tools*

The tools used for the experiment in this research experiment are as follows:

1. Raspberry Pi: A compact single-board computer has no peripherals attached to it.
2. AIRMON-NG, AIRODUMP-NG, AIREPLAY-NG: it is a tool that was used for accessing the Wi-Fi network security. This tool comes with the bundle of Kali Linux, and we need not install it separately.
3. Wireshark: An open-source tool is used to analyze the network traffic state.

*6.3 Attack Scenario*

The attack scenario in Figure 3 explains that there is an actor, who acts as an attacker and sends the packets to the Raspberry PI that is connected to the router. The raspberry PI on receiving the messages that are flooded to it suffers from DDoS attack shutting down all the services, which it was providing to its connected devices.

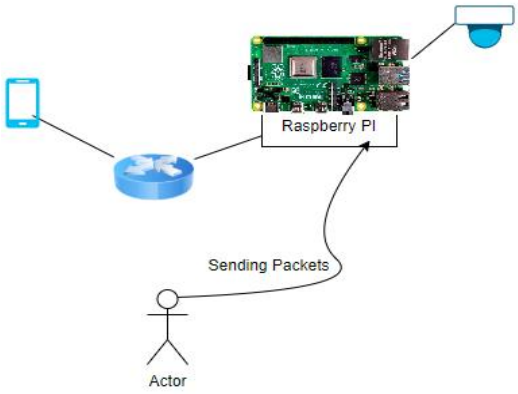
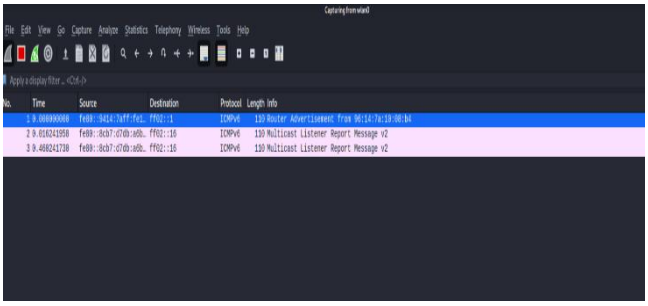


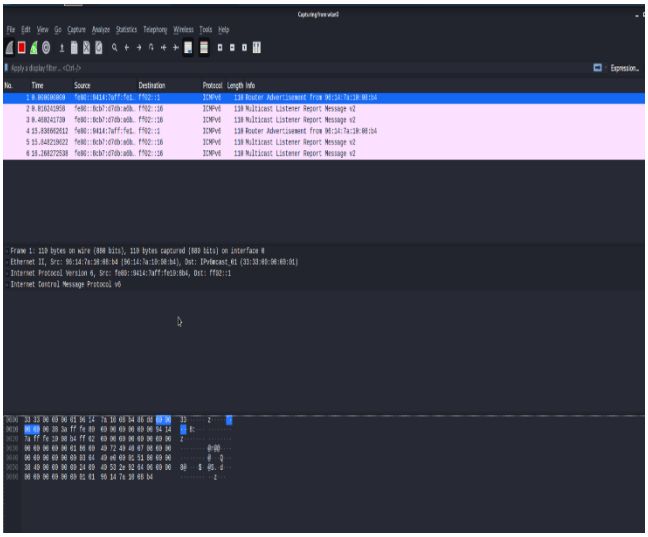

Fig.4. Attack scenario

*6.4 Steps of Experiment*

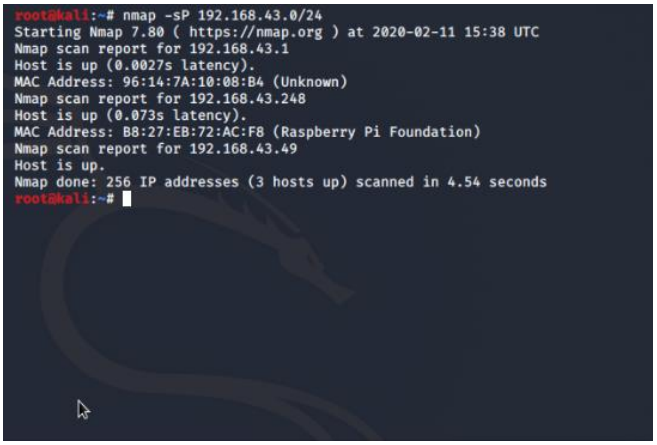
The steps of this experiment are given below:

**Step 1:** Checking the initial traffic of the network using Wireshark tool.

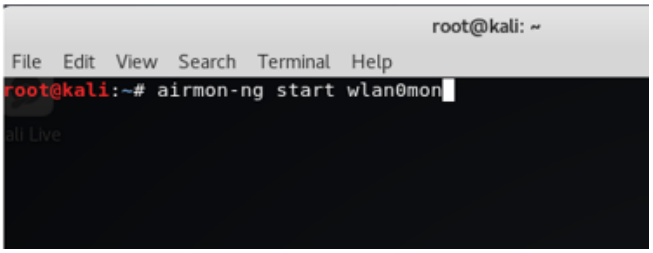




**Step 2:** Checking the live host in the network of IoT devices.



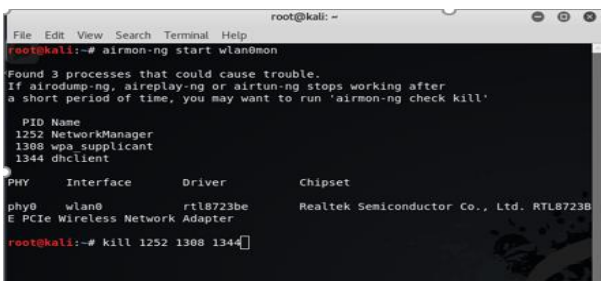

**Step 3:** Put Wi-Fi Adapter in Monitor Mode with Airmon-Ng tool.




**Command: airmon-Ng start wlan0mon**

The command tells you the name of the wireless interface, and you won't be able to connect to Wi-Fi because you are in monitoring mode.

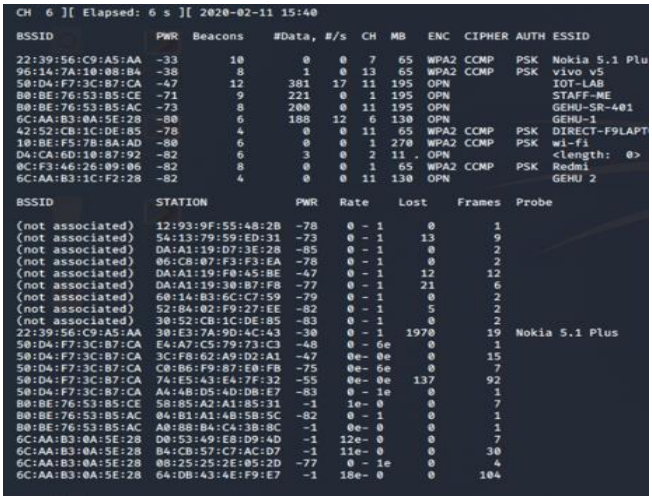
**Step 4:** Killing the process: We will see different running processes; we must kill them for no interruption in the attack.



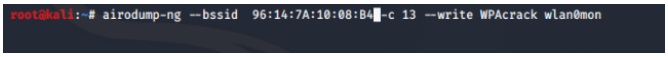
**Command: kill 1252 1308 1344(Where 1252 1308 1344 are the PID).**

**Step 5:** Capture traffic with Airodump-Ng tool: As the wireless adapter is in the monitor mode, we can now see all the wireless traffic that is being passed. We can capture that traffic by simply using Airodump-Ng tool.


**Command: airodump-ng wlan0,** where wlan0 is an interface. The output of the command is shown:

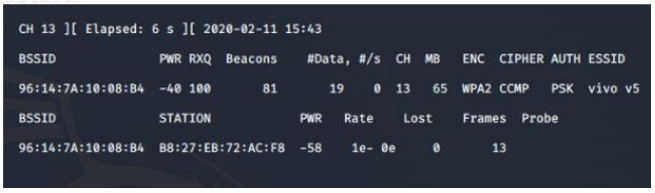



focusAirodump-Ng tool on One AP (target access point) on One Channel: Focus on the access point and get the critical data from it. We need the BSSID and channel to do this. We require getting the MAC ADDRESS of the RASPBERRY PI that is connected to the TARGATED ACCESS POINT. Open another terminal and write




**Command: airodump-ng --bssid 96:14:7A: 10:08: B4 -c 13 wlan0mon**

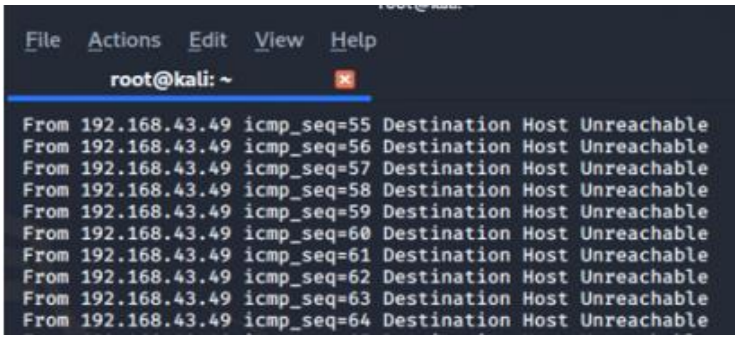
Where Bssid = mac address of Access Point and C= channel number
The output of the above command is:




**Step 6:** Aireplay-Ng Deauth attack (Dos tool): Now we have to jam the access point with DDoS attack. In this case, we will use MAC ADDRESS of the RASPBERRY PI and MAC ADDRESS of the ACCESS POINT which is B8:27: EB:72:AC: F8 and 96:14:7A:10:08:B4 respectively.


**Command: aireplay-ng –deauth 100 –a 96:14:7A: 10:08: b4 wlan0mon,** where -a= MAC Address of Access Point, -c= MAC Address of Raspberry PI, -deauth= De-authentication attack and 100= 100 number of packets which I will send on the ACCESS POINT to jam it.

**Step 7:** Observation is that initially, we were able to get a reply from our RASPBERRY PI having the IP ADD**: command: ping 192.168.43.248**




However, after performing this attack we are not able to get a reply from the RASPBERRY PI because we have kicked it out of the network by performing a DOS ATTACK.

**Step 8:** Attack has been performed and the home automation system will not work now.

## 7. Conclusion

IoT is an umbrella term that is used to refer to the devices that are connected to a network and can respond by sensing the environment. Such devices are known as smart devices. There can be many security challenges for such types of devices as they are globally connected to the network. Anyone can hack and get access to the devices. Malware is the code which is most used by the attacker or hacker to perform attacks and steal information, harm the complete system, and software companies are continuously working on finding ways to identify these attacks early and mitigate them. A major attack that is seen amongst these is the DDoS attack. The discussion in the paper is about classifying the several types of malwares on the type of behavior and how they get into the device, because for developing an efficient malware detection model malware sample should be studied that can represent maliciousness. After that, we have also presented a threat model for the same which shows what different type of attacks are performed on different layers. An experiment is carried out to get access to Raspberry PI and launch the DDoS attack to shut down all the services attached to the device. Besides, the result has shown that the attack is launch successfully.

## References

[1] Maurya, S. and Ahmad, R., ‘Cloud of Things (CoT) based Smart Cities’, 7th IEEE International Conference on Computing for Sustainable Global Development (INDIACom 2020), New Delhi, India, 2020, pp. 94-97.

[2] Maurya, S. and Mukherjee, K., ‘An Energy Efficient Architecture of IoT based on Service Oriented Architecture (SOA)’, Informatica: An International Journal of Computing and Informatics, Vol. 43, No. 01, 2019, pp. 87–93.

[3] Donno, D.M. Dragoni, N., Garett, A. and Spognardi, A. ‘DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation’, Security and Communication Networks, 2018.

[4] Koroniotis, N. Moustafa, N. Sitnikova, E. and Slay, J. ‘Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques’, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST - Springer), Vol. 235, 2018, pp. 30–44.

[5] Bastos, G. Marzano, A. Fonseca, O. Fazzion, E. and Hoepers, C. 'Identifying and Characterizing Bashlite and Mirai C & C Servers', IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1–6.
[6] Weber, R.H., 'Internet of Things - New security and privacy challenges', Computer Law & Security Review - Elsevier, Vol 26, Issue 1, 2010, pp. 23–30.
[7] Donno, M.D. Dragoni, N. Giaretta, A. and Mazzara, M., 'Antibiotic: Protecting IoT devices against DDoS attacks', Advances in Intelligent Systems and Computing book series (AISC - Springer), Vol. 717, 2018, pp. 59–72.
[8] Costin, A. and Zaddach, A. 'IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies', BlackHat USA, 2018, pp. 01-07.
[9] Marzano A. et al., 'The Evolution of Bashlite and Mirai IoT Botnets', IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 2018, pp. 813–818.
[10] Elzen, I.V.D. and Heugten, J.V. 'Project Report on MSc System and network Engineering Techniques for detecting compromised IoT devices', submitted at Oregon State University, Cascades, CS 575, 2017.
[11] Angrishi, K. 'Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV)' IoT Botnets, 2020, pp. 1–17.
[12] Shouran, Z. Ashari, A. and Kuntoro, T., 'Internet of Things (IoT) of Smart Home: Privacy and Security', International Journal of Computer Applications, Vol. 182, No. 39, 2019, pp. 3–8.
[13] Shobana, M. and Rathi, S. 'IOT Malware: An Analysis of IOT Device Hijacking, International Journal of Scientific Research in Computer Science, Engineering and Information Technology', Vol. 5, No. 3, 2018, pp. 653-662.
[14] McDermott, C.D. Isaacs, J.P. and Petrovski, A.V., 'Evaluating awareness and perception of botnet activity within consumer internet-of-things (IoT) networks', Informatics, Vol. 6, No. 1, 2019.
[15] Schick, S., 'Linux.Wifatch: The Router Virus That May Be Secretly Defending You from Other Malware', https://securityintelligence.com/news/linux-wifatch-the-router-virus-that-may-be-secretly-defending-you-from-other-malware/., Accessed on 21 March 2020.
[16] Constantin, L., 'There's now an exploit for 'TheMoon' worm targeting Linksys routers', 2014. https://www.computerworld.com/article/2487778/there-s-now-an-exploit-for--themoon--worm-targeting-linksys-routers.html, Accessed on 22 March 2020.
[17] Bohio, M. 'Analyzing a Backdoor/Bot for the MIPS Platform', SANS Institute, Technical Report, 2015. https://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902. Accessed 22 March 2020.
[18] Spring, T. 'BASHLITE Family of Malware Infects one Million IoT Devices', 2016. https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/. Accessed 22 March 2020].
[19] Antonakakis, M. April, M. and Bailey, M. 'Understanding the Mirai Botnet, in 26th USENIX Security Symposium', Vancouver, British Columbia, pp. 1093-1110, 2017, https://www.usenix.org/conference/usenixsecurity17/ technical-sessions/presentation/antonakakis, Accessed 22 March 2020.
[20] Malik, M. and Léveillé, M., 'M-EM.: Meet Remaiten – a linux bot on steroids targeting routers and potentially other IoT devices', 2016, https:/ /www. welivesecurity.com /2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/. Accessed 22 March 2020.
[21] Paganini, P., 'The Linux Remaiten malware is building a Botnet of IoT devices.' 2016. http://securityaffairs. com/wordpress/45820/iot/linux-remaiten-iot-botnet.html. Accessed 23 March 2020.
[22] Cyware Hacker News, 'Meet Linux/IRCTelnet malware, the successor to Mirai!' 2016. https://cyware.com/news/meet-linuxirctelnet-malware-the-successor-to-mirai-2863deb8. Accessed 23 March 2020.
[23] Greenberg, A., 'The Reaper IoT Botnet Has Already Infected a Million Networks', 2017. https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/. Accessed 23 March 2020.
[24] Threat advisories and attack reports, 'BrickerBot Results in PDoS Attack,' 2017. https://security. radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/. Accessed 24 March 2020.
[25] Seals, T., 'JenX Botnet Emerges to Target IoT Devices and Grand Theft Auto, Info Security Magazine,' 2018. https://www.infosecurity-magazine.com/news/jenx-botnet-emerges-to-target-iot/. Accessed 24 March 2020.
[26] Cimpanu, C. and Day, Z. "New Silex malware is bricking IoT devices, has scary plans," March 2019. https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/. [Online; accessed 24 March 2020].
[27] Madakam, S. Ramaswamy, R. Tripathi, S., 'Internet of Things (IoT): A Literature Review, Journal of Computer and Communications,' Vol. 03, No. 05, 2015, pp. 164–173.
[28] Patel, K.K. Patel, S.M., 'S.M.: Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges', International Journal of Engineering Science and Computing, Vol. 6, No. 5, 2016, pp. 1–10.
[29] Bhushan, B. Sahoo, G. and Rai, A.K. 'Man-in-the-middle attack in wireless and computer networking - A review', 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), Dehradun, India, 2017, pp. 1-6.
[30] Yuan, B. Zou, D. Yu, S. Jin, H. Qiang, W. and Shen, J. 'Defending Against Flow Table Overloading Attack in Software-Defined Networks', IEEE Transactions on Services Computing, Vol. 12, No. 2, 2019, pp. 231-246.
[31] Pranathi, K. Kranthi, S. Srisaila, A. and Madhavilatha, P., 'Attacks on Web Application Caused by Cross Site Scripting', Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1754-1759.
[32] Sajjad, H. and Arshad, M.J., 'Evaluating Security Threats for each Layers of IoT System,' pp. 0–6, 2020. https://www.researchgate.net/publication/336149742_Evaluating_Security_Threats_for_each_Layers_of_IoT_ System, Accessed 21 March 2020.
[33] Kakad, A. R., Kamble, S. G., Bhuvad, S. S. and Malavade, V. N. 'Study and Comparison of Virus Detection Techniques', in conference proceeding, 2014.
[34] Gadhiya, S. and Bhavsar, K. 'Techniques for Malware Analysis', International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, 2013.

[35] Tahir, R. 'A study on malware and malware detection techniques.' International Journal of Education and Management Engineering, Vol. 02, 2018, pp. 20-30.
[36] Kharza, A., Arshad, S., Muliner, C., Robertson, W. and Kirda, E. 'UNVEIL: A large-scale automated approach to detecting Ransomware', USENIX security symposium, Northeastern university, 2016.
[37] Sharma, S. and Mahajan, S. 'Design and implementation of security scheme for detecting system vulnerabilities', International journal of computer network and information security, Vol.9, 2017.
[38] Ndichu, S., McOyowo, S., Okoyo, H. and Wekesa, C. 'A Remote Access Security Model based on Vulnerability Management'. International Journal of Information Technology and Computer Science, Vol. 05, 2020, pp. 38-51.
[39] Singh, J. and Singh, J. 'A survey on machine learning-based malware detection in executable files.' Journal of Systems Architecture, Vol. 112, 2021, pp. 101861.
[40] Lad, S. S. and Adamuthe, A. C. 'Malware Classification with Improved Convolutional Neural Network Model.' International Journal of Computer Network and Information Security (IJCNIS), Vol. 12, 2020, pp. 30-43.

## Authors' Profiles

**Atika Gupta** is pursuing Ph.D. degree in Computer Science and Engineering Department, Graphic Era Deemed to be University, Uttarakhand, India. She has received her MCA and BCA degree from Graphic Era Deemed to be University. Currently, she is working as an Assistant Professor in Graphic Era Hill University, Dehradun, Uttarakhand, India. Her area of research is Data Mining, and Machine learning.

**Anupriya** is pursuing Ph.D From graphic era hill University Dehradun, She is an Assistant Professor in graphic era hill University. She is MCA and M.Tech in CSE from Uttarakhand technical university, Dehradun. Her area of interests are Moocs, Software engineering, data mining.

**Divya Kapil** is Working as an Assistant Professor in Graphic Era Hill University, Dehradun. She has received M.Tech degree in Computer Science and Engineering from Graphic Era Deemed to Be University, Dehradun, India in 2013. She is currently pursuing Ph. D from Graphic Era Deemed to be University, Dehradun, India. Her research interest includes Security in cloud computing and virtualization.

**Dr. Vishan Kumar Gupta** has received his Ph.D. degree in Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India. He has received his M.Tech degree in Information Technology from ABV-Indian Institute of Information Technology and Management, Gwalior, MP, India and Bachelor of Engineering in CSE from Rajiv Gandhi Technical University, Bhopal, MP, India, Currently, he is working as an Associate Professor in Graphic Era Deemed to be University, Dehradun, Uttarakhand, India. His areas of research are Computational Biology, Data Mining, and Machine learning.

**Sagar Agarwal** is an internal IT engineer, system engineer, BAU activities coordination, participated in various network shutdown activities, trained students how to be aware of online cybercrime. He is working in Graphic Era Hill University, Dehradun, India.

**How to cite this paper:** Atika Bansal, Divya Kapil, Anupriya, Sagar Agarwal, Vishan Kumar Gupta, " Analysis and Detection of various DDoS attacks on Internet of Things Network", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.12, No.3, pp. 18-32, 2022.DOI: 10.5815/ijwmt.2022.03.02