International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

Cyber Security Measures for Internet of Things Devices

Sanjay Kumar Gupta[1] and Sandeep Vanjale [2]

[1] *Faculty of Multidisciplinary Studies, Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra, India.*

[2] *Department of Computer Engineering, College of Engineering, Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra, India.*

Abstract

The Internet of Things (IoT) is a new paradigm that integrates the Internet and physical objects belonging to different domains such as home automation, industrial process, human health and environmental monitoring. It is intended for ubiquitous connectivity among different entities or "things". It can be seen as a pervasive network of networks: numerous heterogeneous entities both physical and virtual interconnected with any other entity or entities through unique addressing schemes, interacting with each other to provide/request all kinds of services. It deepens the presence of Internet-connected devices in our daily activities, bringing, in addition to many benefits, challenges related to security issues. The number of devices connected along with the ad-hoc nature of the system further exacerbates the situation. Therefore, security and privacy has emerged as a significant challenge for the IoT. This research work focuses on the security aspects of IoT and proposes security solutions for mitigation of the concerns.

Keywords: Cyber-attacks, DDoS, Internet of Things (IoT), IoT security, Vulnerabilities

1. INTRODUCTION

Internet of Things (IoT) represents amalgamation of different technologies that are interconnected with the aim of providing innovative services [1][2]. In the recent years, the rapid development of access technologies has acted as a catalyst for growth of on-demand services for the end -users [3].It has become possible to regulate the room temperature, lights, PCs etc from anywhere with the help of rudimentary devices connected to internet resulting in evolution of IoT[4]. With millions of such devices being deployed every day, as per conservative estimates it can be stated that by 2020 IoT environment will comprise of 26 billion connected devices[5].Presently IoT applications can be observed in wide variety of critical applications viz. home security, hospital management, waste management, industrial automation, traffic management, resource management, etc to provide new services to citizens, companies and public administrations.[6].

A classic example of IoT in the day to day life of the people can be studied with the help of the modern concept of "Smart Cities". It assimilates the concept of seamless connectivity with the modern global urbanization. Smart City can be defined as the platform for use by information and communication technologies to enhance the quality of urban-life with reduced cost resource consumption [7]. The applications of smart city includes [7] Traffic Management, Electricity Grids, City Lighting and Surveillance, Public Transit, Public Health, Businesses, Water management, Sanitation etc.

Wifi or wireless last-mile technology is employed to network the IoT devices [8]. Evolution of 4G/5G technologies has resulted in better on-demand services with high quality and availability while reducing operational costs of the administrators [9]. This has opened up newer horizons for further IoT deployments. Field -trials are being conducted worldwide employing IoT devices in the fields of intelligent monitoring of hospitals, schools, community centres and air quality indices. Also encouraging results are observed in intelligent parking, vehicular-traffic management, dynamic resource allocation etc. defining the basic parameters of a smart city environments [7].

The exponential growth of IoT devices and the objective of retaining its cost effectiveness has resulted in the neglect of security measures by manufacturers [10]. This vulnerability has led to the avalanche of security breaches in the IoT setup resulting in catastrophic situations [11]. IoT security has now become a matter of critical importance in the recent security researches [12]. With the high dependency on IoT devices in a smart city, cyber-attackers on such devices may result in substantial impairment to the smart systems. Hence it is envisaged that security parameters should be an essential component of IoT setup [12].

The paper is structured in six sections. Section- 1 gives a brief introduction of the topic. Section 2 discusses about the Internet of Things in details and its needs in the modern world. Section -3 discusses the concerns of IoT and provides an analysis of major attacks faced by IoT setup. Section 4 deliberates about the existing security solutions and techniques and gives suggestions for improved network security. Section -5, concludes the paper with the summary of discussions. Section -6 provides future scope of study.

2. INTERNET OF THINGS

Internet of Things (IoT) is an interconnection of systems having sensors, network connectivity and limited processing power employed for exchange of collected information [11]. It can be said to comprise of the interdisciplinary union of different

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

branches of applied sciences viz. engineering, production, automation, health care, applied computation etc. [12].

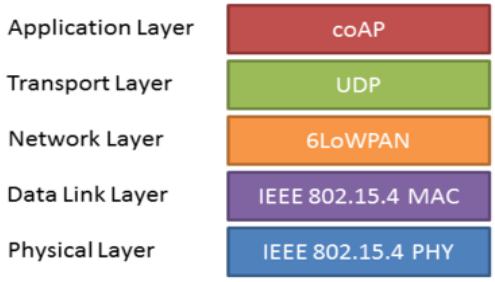


Figure 1. IoT Protocol stack[13].

For catalysing the deployment of IoT on the existing infrastructure, standardization is implemented in the IoT setup. The standardization is designed keeping in mind the unique features of IoT devices which include [13] limited processing power, limited bandwidth and low energy sensor devices. These standardizations enables IoT devices to interface the rudimentary devices with internet [14]. Figure 1[13] presents the standardized IoT protocol stack for interconnectivity with OSI protocol stack.

2.1. IoT Protocol Stack

The salient features of the IoT Protocol stack are presented below:

- IEEE 802.15.4[15][16] radio technology provides interconnect in Physical and Datalink layers of OSI.
- IPv6 Over Low Power Wireless Personal Area Network (6LowPAN) as defined in RFC4944[17], compresses IPv4 packets in IEEE802.15.4 frame; defines the interconnect of IoT devices on the existing IP network infrastructure.
- Due to the inherent low processing power, UDP protocol having lower overhead is used in the transport layer [13].
- Constrained Application Protocol (CoAP) as defined in RFC7252[18] , is an application layer protocol for low energy, low power and bandwidth limited network. It is used extensively in machine-to-machine applications [18]. CoAP supports TLS for UDP protocol[19] for the much needed security aspect.

2.2. Need of IoT

In recent years, concepts such as smart devices, smart cars, smart cities, and smart homes have received great interest from many different research communities. The combination of these concepts is considered as the future of Internet and it is called the Internet of Things (IoT) . Recent technological advances in electronics have enabled the development of all kinds of small-size devices with various degrees of sensing, computing, storage, and power capabilities, which has led to the opportunity of utilizing almost any object as a smart and communicating thing rather than an isolated entity, for the purpose of unlimited number of applications.

It is expected that IoT technology will pave the way for groundbreaking applications in a diversity of areas such as healthcare, security and surveillance, transportation, and industry, and that it will be able to integrate technologies such as advanced machine-to-machine communication, ,autonomic networking, decision-making, confidentiality protection and security, and cloud computing with advanced detection and actuation technologies. Technically speaking, IoT encompasses both static and dynamic objects of the physical world (physical things) and the information world (virtual world), which can be identified and integrated into communication networks . IoT is graphically presented in Figure 2[12].

The essential features of IoT include: (i) interconnectivity, (ii) things-related services such as privacy protection and semantic consistency, (iii) heterogeneity, (iv) support of dynamic changes in the state and the number of devices, and (v)enormous scale.

The importance of the context of scale is evident from the fact that, by the year of 2010, there were already 1.84connected devices per person; and it has been estimated that the number of connected devices will accomplish approximately 50 billion by 2020. Given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance; calling into question the whole future of IoT. IoT applications will affect many aspects of people's lives, bringing about many conveniences; however, if security and privacy cannot be ensured, this can lead to a number of undesired consequences such as violation of private information and other opportunities for foul play.

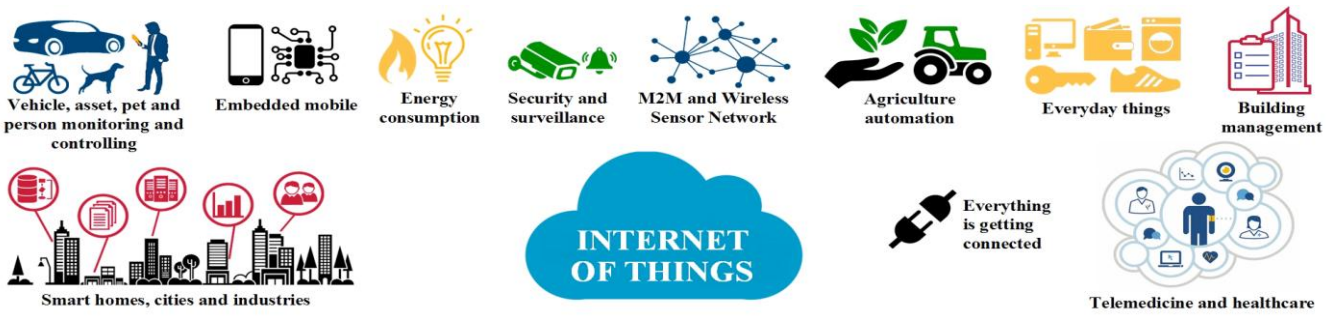


Figure 2. Internet of Things

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

3. CONCERNS OF IOT

Nowadays, IoT is widely applied to social life applications from smart homes, smart security, autonomous transports, smart grids to smart health, waste-management, automated attendance etc. [5].

IoT on one hand brings convenience to people, but puts a major risk on the personal privacy. Compromising the IoT devices may bring about catastrophic consequences. Hence, IoT security is of paramount importance. If IoT cannot have a good solution for security issues, it will largely restrict its development.

As more and more smart cities are being launched across the globe, users are getting accustomed to the usage of IoT in their day-today life. The sheer number of such devices and the environments they control, motivates a cyber-attacker [6]. Figure 3[6] highlights some of the possible motivations of a cyber attacker.

Generally, for an attacker, the above motivations act as inputs for malicious intents [6]. The goals of cyber attackers may be summarized as [13]:

- Launch of DDoS attack on internet by using the IoT devices as autonomous botnets.
- Unleashing extortion from users by breaching their privacy
- Data forgery
- Synchronized attacks.

In a smart environment, attackers may target [6] database of usernames and passwords, electronic sensors, CCTV setups, Access controls, personal electronic devices, biometrics stored in devices etc. From security point of view the confidentiality, integrity, availability, authentication, authorization of the IoT setup needs to be protected [6].

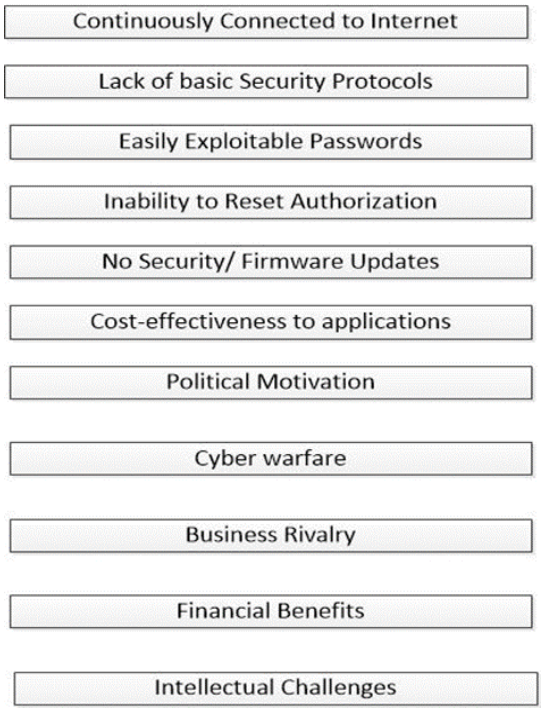


Figure 3. Motivation of attacks in IoT

3.1. Types of Attacks in IoT.

The most prevalent attacks on IoT devices are DDOS attacks [18]. DDoS attack is defined [18] as a cyber-attack originating from the internet in order to render a server in accessible to legitimate users. Let's consider 14 nodes of a network as shown in Figure 4. It may be noted that Node 13 acts a gateway to Node 14 which is the server. On the event of a malicious DDoS attack from the internet in which nodes 10, 11 and 12 are infected they send garbage data to node 13 thereby depleting its resources resulting the legitimate packets being dropped in node 13. This constitutes a DDoS attack and is graphically presented in Figure 5.

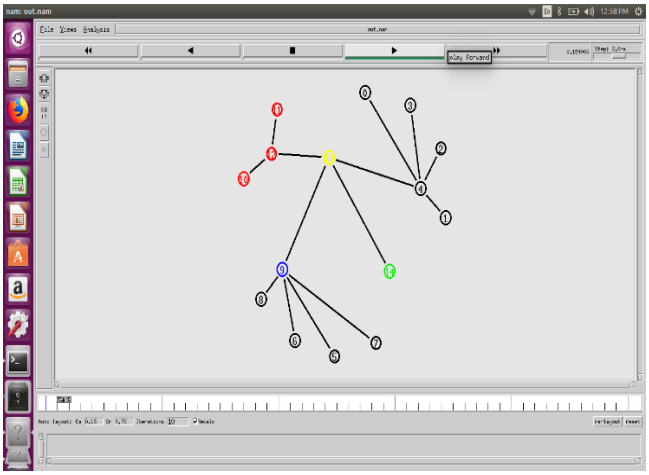


Figure 4. Network of 14 Nodes

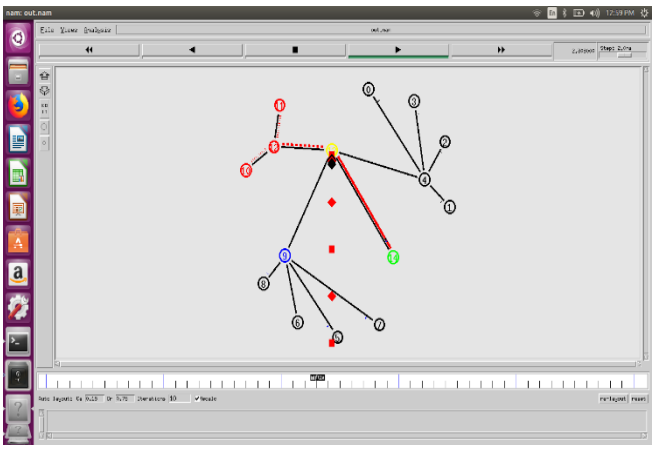


Figure 5. DDoS Attacks on IoT Network

IoT devices in general have web interfaces for administration. These can be easily compromised by attackers by attacks like SQL injections and cross website scripting [19]. These attacks tend to create privilege-escalation in the devices resulting in the compromised device acting as a Botnet for a DDoS attack. Further due to the constrained processing power and memory resources, the IoT devices may [18]:

- Store user credentials in plain text
- May employ weak authentication mechanism

- Channel of communication may be unencrypted communication between devices.
- No logical and robust zone management defined in the command structure.

The above vulnerabilities expose the IoT devices to cyber-attacks like [18]: Session hijack, Man-in-the Middle attack, data Compromise, Credential Fraud, Firmware corruption etc.

KRACK [20] may be exploited by a cyber attacker to gain access to the IoT devices through Wi-Fi medium and coupled with Sybil Attacks [21] can cause routing confusions in wireless domain causing severe drainage of allocated system resources. Similarly, a cyber attacker may exploit default credentials left unattended by users to launch a Mirai Botnet DDoS attack in the setup. Also, it is observed that software-updates are not available on time for IoT applications thereby exposing the devices with known limitations to cyber attackers [23]. Further the IoT devices are vulnerable to device cloning and un-authorized control [24]

Figure 6 presents possible attacks in the constrained protocol stack of IoT devices

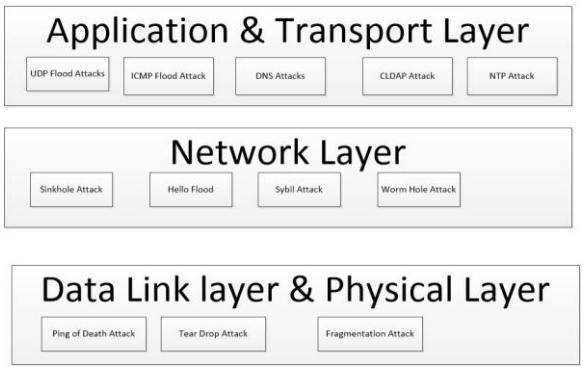


Figure 6. DDoS Attacks on various layers of Protocol Stack

Considering the number of IoT devices in a smart-city environment, even a small percentage of compromised device may generate an avalanche of malicious data, disrupting and depleting the system resources available to legitimate users and takes heavy tolls on performance metrics of the system for rectification. This may cause trespassing of user privacy & security and may even endanger the life of citizens. Table-1. provides a list of DDoS attacks on IoT devices.

Table 1. List of recent DDoS Attacks on IoT

Sr. No	Name	Year	Targeted devices	**Activity**
1	BashLite	2015	Cameras, DVRs	Transport layer flooding along with application layer tweaks resulting in huge volume of malicious request clocking up to 400 Gbps
2	Mirai	2016	Network devices and cameras	SYN and ACK, UDP Flooding, HTTP traffic, DNS attacks after brute force entry
3	Reaper	2017-18	General IoT environment.	Uses known vulnerabilities of the IoT devices and delivers code modules by LUA to launch DDoS Bots.

3.2. Analysis of IoT Security

The best way to analyse the threats in a IoT environment is to classify the components of IoT in terms of the general security characteristics of Confidentiality, Integrity, Availability, Authentication, Access Control and non-repudiation. The components of the IoT environment may be classified as Hardware, Network and Server [23].

3.2.1. Hardware

IoT devices have hardware which have a very limited processing power, operating frequency and power requirements; hence they form a distinct identity as compared to the hardware deployed in the internet.

3.2.2. Network

Compared to internet systems, IoT devices employs bandwidth limited, reduced complexity and minimal power devices. Generally, WiFi is used for interconnectivity of IoT networks, causing them to be prone to jitters. Also due to the limited processing capacity of IoT devices the internet protocols need to be tweaked to be operable in the IoT setups. This is also true for encryption and other security measures.

3.2.3. Server

The data collected by IoT devices and submitted to server are having highly privilege and privacy content and hence needs to be accessed by authorized users only. The main concern is to deal with rogue devices and spoofing attacks.

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

The Table-2. provides threat analysis of IoT environment.

Table 2. Threat Analysis of IoT Environment

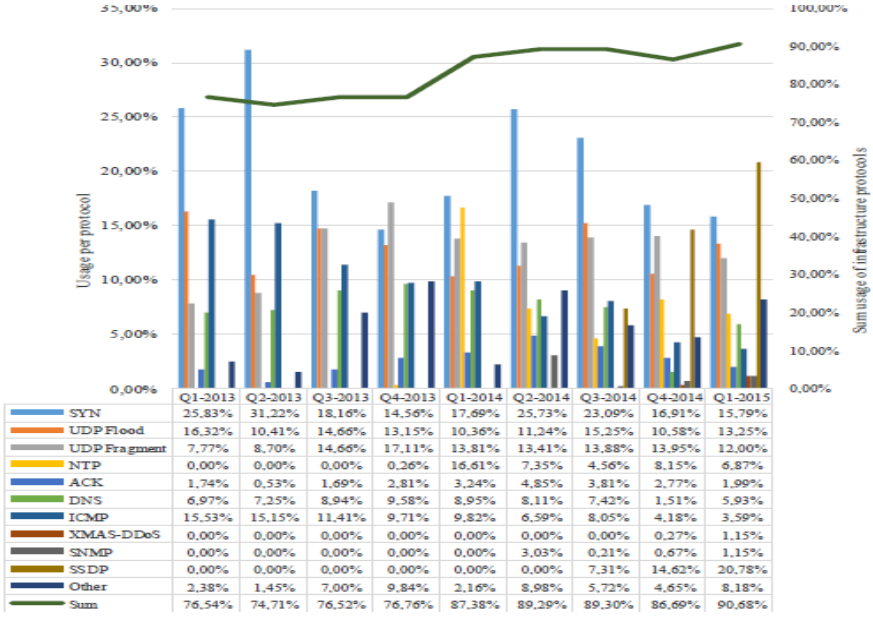
Security Characteristics	**Device**	**Network**	**Server**
Confidentiality	Hardware Attacks	Encryption Challenges	Privacy Data leaks
Integrity	Spoofing	Sybil attacks	No common device identity
Availability	Physical attacks	DDoS	DDoS
Authentication	Default password breach	Brute-force attacks	Insecure Data flows
Access Control	Authentication issues	De-centralized rule sets	Rogue Device connections
Non –Repudiation	No security at local storage level	No Signature hierarchy and verification capabilities	

3.3. Majority Attacks Type

With the sheer number of vulnerable devices being connected to internet in an IoT environment, these devices act as highly lucrative tools for launching Denial-of-Service (DoS) by the cyber –attackers from the internet. DoS is a cyber-attack in which the internet-based attacker seeks to make a machine or a network resource unavailable to its intended users by disrupting the services of the target connected to internet. It is performed by flooding the targeted machine or network resource with superfluous requests in an attempt to overload the systems and prevent the legitimate requests from being fulfilled. DoS originates from a single host or network in the internet

DoS when performed by flooding the targeted machine from many different sources is called as Distributed Denial of Service (DDoS) attack. The scale of DDoS attack makes it impossible to distinguish a legitimate traffic and attack traffic, complicating the security mechanism. A new augmentation of DDoS attack where the attacker spoofs the originating address with that of the victim and employing UDP protocol is the severest form of attack and is known as Reflection DDoS attack. DDoS attacker may forge the source address of the request packets pretending to be that of the victim and flood the requests to reflectors, who then direct their response to the victim, flooding its resources. Such type of attack is called Distributed Reflection DoS attack or DRDoS or simply Reflection attack. Reflection DDoS attack take advantage of publicly accessible UDP services to overload victims with response traffic. The attacker delivers traffic to the victim by reflecting it off a 3rd party, so the origin of the attack is concealed from the victim, making *Ingress Filtering Firewall* in-effective. The exponential growth of the IoT devices is making it a fertile field for Reflection DDoS attackers.

Denial of service attacks represent a growing problem therefore it is necessary to research and analyse trends of applied protocols and traffic volume and bandwidth of attacks with the aim of timely response to future attacks.Figure 7[25] presents an analysis of attacks employing network layer of IoT devices from Q1 2013 to Q1 2015.



	Q1-2013	Q2-2013	Q3-2013	Q4-2013	Q1-2014	Q2-2014	Q3-2014	Q4-2014	Q1-2015
SYN	25,83%	31,22%	18,16%	14,56%	17,69%	25,73%	23,09%	16,91%	15,79%
UDP Flood	16,32%	10,41%	14,66%	13,15%	10,36%	11,24%	15,25%	10,58%	13,25%
UDP Fragment	7,77%	8,70%	14,66%	17,11%	13,81%	13,41%	13,88%	13,95%	12,00%
NTP	0,00%	0,00%	0,00%	0,26%	16,61%	7,35%	4,56%	8,15%	6,87%
ACK	1,74%	0,53%	1,69%	2,81%	3,24%	4,85%	3,81%	2,77%	1,99%
DNS	6,97%	7,25%	8,94%	9,58%	8,95%	8,11%	7,42%	1,51%	5,93%
ICMP	15,53%	15,15%	11,41%	9,71%	9,82%	6,59%	8,05%	4,18%	3,59%
XMAS-DDoS	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,27%	1,15%
SNMP	0,00%	0,00%	0,00%	0,00%	0,00%	3,03%	0,21%	0,67%	1,15%
SSDP	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	7,31%	14,62%	20,78%
Other	2,38%	1,45%	7,00%	9,84%	2,16%	8,98%	5,72%	4,65%	8,18%
Sum	76,54%	74,71%	76,52%	76,76%	87,38%	89,29%	89,30%	86,69%	90,68%

Figure 7. Frequency of infrastructure layer protocol used in DDoS

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

For the entire analyzed period of time we can see continued growth. The overall increase from Q1 2013 to Q1 2015, a summary of all protocols, is 14.14% [25]. In Q1 2015, 90.68% of all recorded DDoS attacks used infrastructure layer protocols. The primary protocol used for the implementation of DDoS attacks from Q1 2013 to Q4 2014 was the TCP SYN [25].

Figure 8[25] shows the extent of DDoS attacks in the period from 2002 to 2014. In the last two years exponential growth of the attack volume is seen (measured in Gbps). Compared to the year 2012 the volume of DDoS attacks in 2013 increased by 475%, and in 2014 for 615% [25]. The result is the increasing availability of online services that offer the service botnets usable in conducting DDoS attacks, a growing number of connected devices that are potential agents in botnet networks which allows generating larger amounts of network traffic and finally the use of new protocols in the realization of attack and reduced levels of protection.

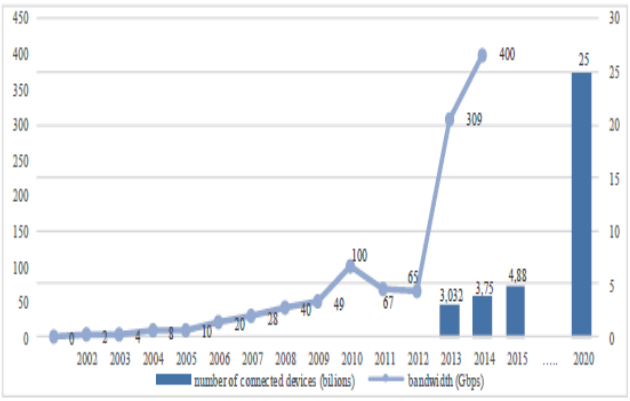


Figure 8: Increase in IoT Connected Device and DDoS attacks

Further as accelerated growth of the connected devices number based on the IoT concept is predicted. Currently in the world there are approximately 5 billion of these devices, and interpolation growth trend indicates a potential 25 billion connected devices by 2020. The same figure is shown that the increase in the number of connected devices is followed by an increase in DDoS attacks bandwidth. The sharp rise in the number of devices connected through the IoT concept offers the possibility of forming a botnet network that is able to generate significantly greater amount of illegitimate traffic than in previous years.

3.3.1. DDOS ATTACK Types in IoT [26]

As can be seen from the above, DDOS attacks forms the most voluminous attack involving IoT devices due to its sheer size of deployment. DDoS attacks affecting the various devices and Layers of the Iot protocol stack is presented below:

3.3.1.1. DDoS on Physical layer & Data-link layer

At this layer, automated reading of sensor-data by RFID is performed. The following attacks are prevalent in this layer. The details of attacks are presented in Table-3[27].

Table-3. Details of attacks on Physical and Datalink Layer

Sr. No.	**Name of the Attack**	**Activity**
1	Jamming	Prevention of RFID tag reading
2	Disabling	Tags are easily disabled causing disconnect in data
3	De-synchronizing	Permanent Disabling of RFID tags
4	Wide-band Denial & Pulse Denial	Blocks the entire RF spectrum causing DOS
5	Node-specific/ Message Specific Denial	Hijacking of legitimate information for launching specific attacks.

3.3.1.2. DDoS on Network Layer

The network layer follows the mechanism in sensors, which usually include Bluetooth, IrDA, Wi-Fi etc. and are prone to the following attacks as depicted in Table-4[26].

Table-4. Attacks on Network layer

Sr. No	Name of the Attack	Activity
1	Flooding Attack	Attacker disrupts the authenticating user's resources
2	Reflection-based flooding Attacks	Attacker sends malicious requests by employing Botnets, thereby exhausting victim's resources and making it difficult to block the attacker.
3	Protocol Misuse Flooding	Attacker exploits the known vulnerabilities of the victim's protocol for draining the available resources.
4	Amplification Attacks	Attacker compromises the genuine application to flood the victim's incoming traffic employing BOTNETs.

3.3.1.3. DDOS ATTACK on Application Layer

The attacks are presented in Table-5[26].

Table-5. Attacks on Application layer

Sr. No	Name of the Attack	Activity
1	Re-programming Attack	Attacker modifies the source code to make the application run an infinite loop making the network inaccessible.
2	Path based DoS	Attacker bombards the devices with spurious packets on communication paths.

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

3.3.1.4. Classical Example of DDoS attack on IoT

Mirai is a malware that targets un-secure IoT to launch DDoS attacks. The modus operandi of the attack is as follows:

- Devices infected by Mirai continuously scan the internet for the IP address of IoT devices.
- It then identifies vulnerable IoT devices for open telnet access using a table of default usernames and passwords to perform brute-force login and to infect them with the Mirai malware.
- Infected devices will continue to function normally, except for occasional slow response and an increased use of bandwidth. The device remains infected until it is rebooted. After a reboot, unless the login password is changed immediately, the device will be re-infected again.
- It will identify any "competing" malware, remove it from memory, and block remote administration ports of the infected device.
- Once infected, the device will respond to a command and control server which indicates the target of an attack.

The reason for the use of the large number of IoT devices is to bypass some anti-DoS software. Another reasons for targeting IoT devices is to accommodate more bandwidth for attack than the attacker can assemble alone, and to avoid being traced.

Mirai then launches the following 9 types of attack as described in Table-6, on the internet with the help of compromised IoT devices

Table-6. Attacks of Mirai

Sr.No.	Attack	Description
1	UDP Flood	Flood of spurious UDP packets
2	VSE Flood	Valve Source Engine Query Flood
3	DNS water torture	Recursive DNS query attack
4	SYN attack	SYN packet flood
5	ACK attack	ACK packet flood
6	STOMP attack	ACK flood with STOMP
7	GRE IP	GRE flood
8	GRE Ethernet	Ethernet encapsulated inside GRE flood
9	HTTP Flood	HTTP application layer flood

3.3.1.5. DDoS Attack Taxonomy

The sheer size and reach of the IoT devices and the fact that these devices are neglected in terms of security has made these devices susceptible to DDoS attacks. As per the security bulletin issued by Kaspersky for 2019[25] following can be observed:

1) The DDoS attacks are a worldwide phenomenon in the IoT environment and it effects both developed and developing countries.
2) The DDoS attacks contribute to the most economically and resource draining phenomenon in an organization.
3) Working days are seen to be mostly acting as fertile environment for DDoS attacks.
4) Most DDoS attacks are those which last less than 4 hours
5) The longest attack was observed for 116 days in the third quarter of 2019.
6) SYN flooding is the leading attack type with more than 79% attacks being SYN flooding followed by UDP flooding at 9.4%.
7) Linux Botnets constitutes 97.75% of all the botnets while windows botnets comprise to 2.75% this confirms the fact that more and more users are using Open Source Operating systems.

These reports are graphically presented in figures 9, 10 and 11[25].

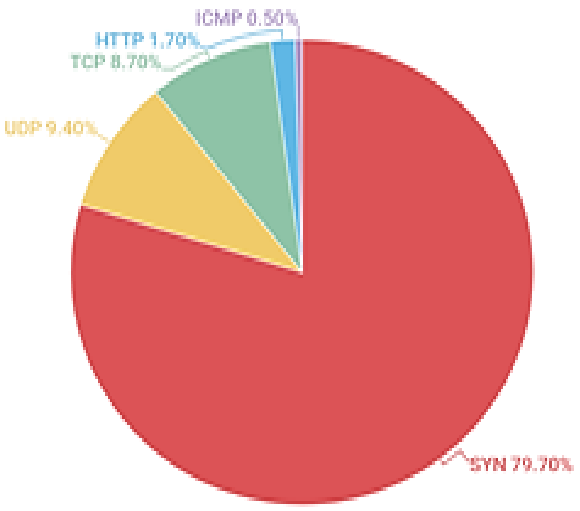


Figure 9. Types of DDoS Attacks

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

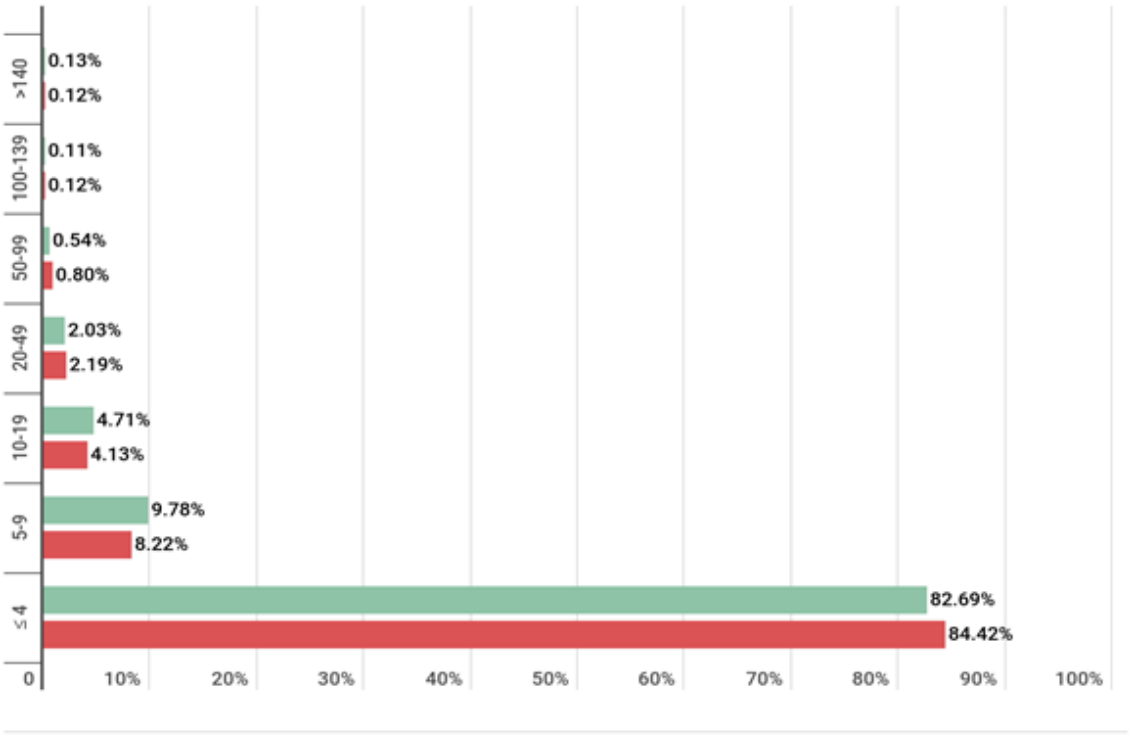


Figure 10. Duration of DDoS attacks

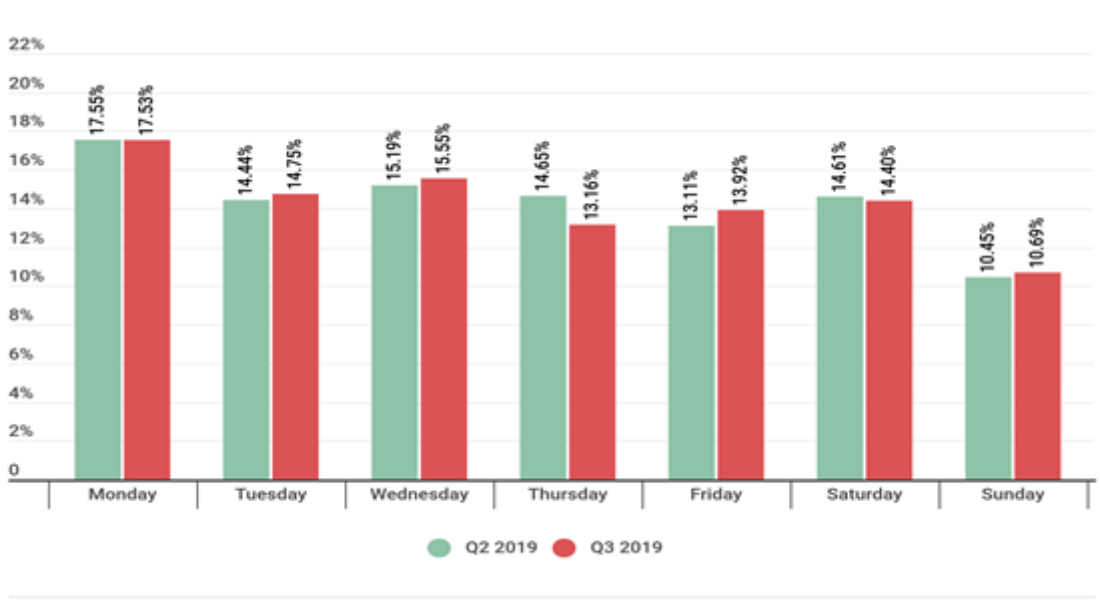


Figure 10. Percentage of DDoS attacks observed in days of the week

4. EXISTING SECURITY SOLUTIONS OR TECHNIQUES

The best way to protect an IoT setup is to implement a strict authentication mechanism for addition/ deletion and devices and their management. Further attack detection mechanisms may be implemented to proactively detect attacks and protect the IoT setups. The various techniques that are available to detect attacks are summarized below[26]:

4.1. NetFlow

It is a protocol developed by Cisco Systems to collect Ip traffic metrics on a Router/ Switch.It characterizes traffic flows and patterns and can locate the potential attackers

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 8 (2020), pp. 1830-1839
 https://dx.doi.org/10.37624/IJERT/13.8.2020.1830-1839

4.2. Packet analysis

Packet analysers/ sniffers captures and interprets the data that flow through the network eg. Tcpdump, Wireshack. They can check the network interfaces of a device and analyse any packet flowing in the network irrespective of the fact weather the packet is destined to a specific host or not.

4.3. Monitoring Darknets

It allows network administrators to capture and analyse any packet in the network.

4.4. Honeypots

These are systems designed to entice attackers to attempt to gain access to the systems. It is used to deflect the attackers and analyse the techniques used by the attackers.

IoT devices are controlling important applications. In order to secure such devices care may be taken to secure the attributes viz. Secrecy, Veracity, Accessibility, Verification /Validation, Permissions are of key importance [6]. The first step towards implementing the security is the drafting of a Security policy for the network. The policy may include the following activity list [23]:

- Removal of the default passwords and time frame for regular password updation
- Application of Software updates as and when available
- Allow Plug and play after proper authentication.
- Permit only predefined services in the network
- Encrypt communication between devices
- Filter based firewall implementation

Current IoT deployments uses data protocols without any security considerations. A possible solution is to develop a new data-security protocol conforming to the IoT protocol stack for universal acceptance. For implementing future-ready IoT systems, it is recommended to set-up in-built protection against the automated- attacks from cyber space in the IoT environment. A centralized regulator may be implemented to monitor the activities between the IoT devices and flag-off a suspected malicious activity for further probe. Following steps may be implemented in the system:

- Implement an IDS/IPS system along with a packet filter firewall and centralized Antivirus setup.
- Implementation of Network Monitoring Tools to regularly monitoring of network resources and its allocation
- System for quick neutralizing the detected Botnet in the setup.

Figure 12[23] provides the building blocks of a security policy that needs to be implemented for a holistic approach of security concerning IoT deployment.

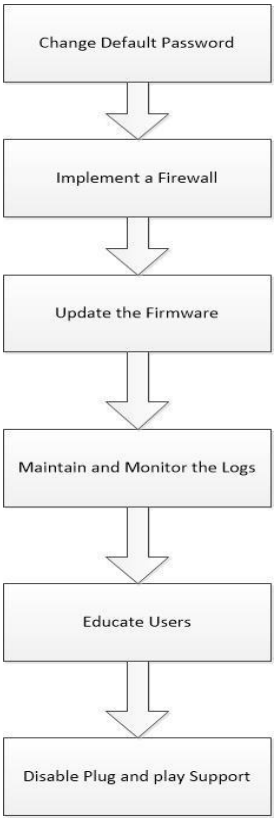


Figure 12. Suggestion for Security Policy

5. CONCLUSIONS

IoT devices have become synonym with modern world. With the development of standardization in interconnecting technologies of IoT with internet, a major growth is seen in the deployment of IoT devices. However limited efforts is seen on the part of manufacturers and service providers in the aspect of cyber security, leading to various types of security breaches having far-reaching effects. This paper attempted to study the basic perception of the security in the IoT setups. Further various attacks faced by the IoT infrastructure are analysed. Based on the observations a plan is proposed to implement a secure IoT deployment involving all the stake holders.

6. FUTURE SCOPE

An attempt has been made by this paper to theoretically study the security concerns of the IoT setup. The same may be evaluated practically by creating a small test bench of IoT deployment such as “Smart Room” by interconnecting various IoT devices used in home setups. The examples of the setup being smart light, AC systems, window blinds, door knobs etc. This may be further extended to the concept of “Smart Home” and further interconnect the autonomous smart-homes into “Smart Building” setups. The individual vulnerabilities of the devices may study and exploited in a limited scale and necessary security policies as described above may be implemented to mitigate the vulnerabilities. Further the security policies can be fine-tuned depending upon the field observation of the setup under study; thereby complementing the study further.

REFERENCES

[1] C.Kolias, G.Kambourakis,A.Stavrou,J.Voas,(2017) "DDoS in the IoT:Mirai and other Botnets*.", IEEE Computer Journal,* Vol. 50, No. 7, pp 80-84.

[2] F.Meneghello, M.Calore, D.Zucchetto, M.Polese, A.Zanella(2019) " IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices", IEEE *IoT Journal* Vol.6, No. 5, pp 8182-8201.

[3] M. Ray , M.Chandra(2017) " Evolution of Wavelet- Based Speech Codecs for VoIP Applications", *Proceedings of International Conference on Nano-electronics, Circuits & Communication Systems:* 29-37.

[4] N.Neshenko, E.Bou-hard, J.Crichigno, G.Kaddoum, N.Ghani(2019) "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Emperical Look on Internet-scale IoT Exploitations", *IEEE Communications Survey & Tutorials* Vol.21, No. 3,pp 2702-2733.

[5] Online Resource available at *https://www.gartner.com/newsroom/id/3598917* Accessed in June 2020.

[6] [6]. H.Saha, S.Auddy, A.Chaterjee, S.Pal, S.Sarkar, R.Singh,(2017) "IoT Solutions for Smart Cities", *Proceedings of 8th Annual Industrial Automation and Electro-mechanical Engineering Conference,* pp 16-25.

[7] W.Ejaz, A.Anpalagan (2018) "IoT for Smart Cities Technologies, Bigdata and Security".*Springer Briefs in Electrical & Computer Engineering.*

[8] A.Panchal, V.Khadse, P.Mahalle (2018) "Security Issue in IIoT: A Comprehensive Survey of Attacks on IIoT and its Countermeasures", *Proceedings of IEEE Global Conference on Wireless Computing and Networking,*pp 293-240.

[9] S.K.Gupta, S.B.Vanjale (2019) "Internet of Things in Smart City Enviornments", *International Journal of Recent Technology & Engineering,* Vol.8, No. 3, pp 7917-7921.

[10] D.Yin, L.Zhang, K.Yang (2018) " A DDoS Attack Detection & mitigation with Software-defined IoT Framework", *IEEE Access* Vol.6,pp 24694-24705.

[11] T.Pering, K.Farrington, T.Dahm(2018) "Taming the IoT:Operational Testing to Secure Connected Devices",*IEEE Computer Journal* Vol.51, No. 6, pp 90-94.

[12] J.W.Jones(2018) "Security Review on the IoT", *Proceedings of 3rd International Conference on Fog and Mobile Edge Computing,* pp 23-26.

[13] Online Resource available at https://www.conduiraonline.com/index.php/detail/ 368- what-is-a-smart-city Accessed in June 2020.

[14] Y.Mehmood, F.Ahmad, I.Yaqoob , A.Adnane, M.Imran, S.Guizani(2017) "Internet of Things based Smart Cities: Recent Advances and Challenges", *IEEE Communications Magazine,* Vol.55, No.9,pp16-24.

[15] R.Harmon, E.Castro-Leon, S.Bhide,(2015) "Smart cities and IoT", *Portland International Conference on management of Engineering and Technology,* pp 2-6.

[16] H.Rajab, T.Cinkelr(2018) "IoT based Smart Cities", *IEEE International Symposium on Networks, Computers and Communications,*pp.:19-21.

[17] I.Makhdoom, M.Abolhasan, J.Lipman, R.liu, W.Ni(2019)"Anatomy of threats to the IoT", *IEEE Communications Survey & Tutoril*a,Vol.21, No. 2, pp *1636-1675.*

[18] B.Viganau, R.Khoury, S.Halle(2019) " 10 years of IoT Malware: A feature based Taxonomy", *Proceedings of 19th IEEE International Conference on Software Quality, Reliability and security Companion,* pp22-26.

[19] K.Reeves, C.Maple(2018), " IoT Interoperability: Security Considerations and challenges in Implementation", *IEEE Living in the IoT: Cybersecurity of the IoT:* pp 28-29.

[20] A.Terkawi, N.Innab(2018) "Major Impacts of Key Reinstallation Attack on IoT", *Proceedings of 21st Saudi Computer Conference,*pp 25-26.

[21] A.Rajan, J.Jitish, S.Sankaran(2017) "Sybil attacks in IoT: Modelling & Defences", *Proceedings of International Conference on Advances in Computer, Communications & Informatics,* pp13-16.

[22] T.Gopal, M.Merolla, G.Jyotsana, P.Eswari,E.Mangesh(2018) " Mitigating Mirai Malware Spreads in IoT Enviornment", *Proceedings of International Conference on Advances in Computer, Communications and Informatics,* pp 19-22.

[23] A.Sajid, H.Abbas, K.Saleem (2016) "Cloud-Assisted IoT Based SCADA Systems Security: A Review of the State of the Art & Future Challenges", *.IEEE Access,*Vol 4, pp 1375-1384.

[24] B.Javed, M.Iqbal, H.Abbas(2017) "IoT design considerations for Developers and Manufacturers", *Proceedings of IEEE International Conference on Communications Workshop,* pp 21-25.

[25] Online Resource available at https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects- more-than-100-million-attacks-on-smart-devices-in-h1-2019#. Accessed in June 2020.

[26] K.Sonar, H.Upadhaya(2014) "A Survey: DDoS Attack on Internet of Things", *International Journal of Engineering Research and Development , pp* 58-63.

[27] C.P.Oflynn(2011) "Message Diluation and Alteration on IEEE 802.15.4", *Proceedings of New Technology Mobility and Security*, pp 1-5 .

AUTHORS

Sanjay Kumar Gupta received his Master's Degree in Physics with Specialization in Electronics from Garhwal University, Srinagar, Uttarakhand in 1990. He has obtained ALCCS degree in Computer Science from IETE, New Delhi in 1998. He has over 25 Years of Experience in Formulation and Implementation of various Information & Communication Technology applications across Domains and extensive experience in IT/ITeS/ESDM sectors. He is Pursuing PhD. from Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra. His area of interest includes IP Networking, Internet technologies, AI, IoT ,High Speed Data communication networking.

Dr. Sandeep B. Vanjale, received B.E. Computer Engineering from Shivaji University, Kolhapur , Maharashtra in 1998, M.E and PhD. in Computer Engineering from Bharati Vidyapeeth Deemed University, Pune, Maharashtra in 2004 and 2016 respectively. He is working as Professor in Computer Engineering Department of Bharati Vidyapeeth Deemed University, Pune , Maharashtra since 2008. He has got more than 19 Years of teaching Experience and guided more than 200 BE students and 25 Post graduate students in the field of Computer Engineering. He has published more than 38 research papers in the area of Information Technology in reputed International Journals. His areas of interest includes Internet Technologies , IoT and Advanced computing.