ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 8, Issue 3, March 2021

DDoS Attack in IoT: Vulnerabilities and Mitigation Techniques

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

[1] Faculty of Interdisciplinary Studies, Bharati Vidyapeeth (Deemed to be University), Pune, India
[2] Department of Computer Engineering, College of Engineering, Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra, India
Email: [1] skgru@yahoo.com, [2] sbvanjale@bvucoep.edu.in

***Abstract---* Internet of Things (IoT) is a platform that integrates the internet with the rudimentary devices. This technology catalysts the growth of Internet-connected devices in our daily activities. This provides numerous benefits to the end user; however, it also brings with itself new challenges related to security and privacy 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 paper analyses various security aspects of IoT setup and proposes security solutions for mitigation of the concerns.**

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

I. INTRODUCTION

Internet of Things (IoT) is combination of different interconnected technologies designed to provide innovative services [1][2]. In the recent years, on demand services have become sole requirement of end users and is made possible with the exponential development of access-technologies and embedded system. It has become possible to control the environment of the surroundings with the help of rudimentary devices connected to internet resulting in evolution of IoT [3]. This had resulted in exponential growth of IoT devices. 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. 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 [6].

The exponential growth of IoT devices and the objective of retaining its cost effectiveness has resulted in the neglect of security measures by manufacturers [7]. This vulnerability has led to the avalanche of security breaches in the IoT setup resulting in catastrophic situations. IoT security has now become a matter of critical importance in the recent security researches. Hence it is envisaged that security parameters should be an essential component of IoT setup [9].

The paper is structured in various sections. Section-I gives a brief introduction of the topic. Section-II discusses about the Internet of Things in details and its needs in the modern world. Section-III discusses the concerns of IoT and provides an analysis of major attacks faced by IoT setup. Section-IV deliberates about the existing security solutions and techniques and gives suggestions for improved network security. The last section concludes the paper with summary of discussions followed by future scope of study.

II. INTERNET OF THINGS

Internet of Things is an interconnection of systems having sensors, network connectivity and limited processing power [8]. It can be said to comprise of the interdisciplinary union of different branches of applied sciences viz. engineering, production, automation, health care, applied computation etc. [9]. For catalysing the deployment of IoT on the existing infrastructure, standardization is implemented in the IoT setup, which enables IoT devices to interface the rudimentary devices with internet [11]. 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. The essential features of IoT include interconnectivity, things-related services such as privacy protection and semantic consistency, heterogeneity, support of dynamic changes in the state and the number of devices and enormous scale.

III. IoT SECURITY CONCERNS

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. [4]. IoT brings convenience to people, but puts a major risk on the personal privacy. Compromising the IoT devices may bring about catastrophic consequences. If IoT cannot have a good solution for security issues, it will largely restrict its development. The sheer number of such devices and the environments they control, motivates a cyber-attacker. Figure-1 highlights some of the possible motivations of a cyber attacker.

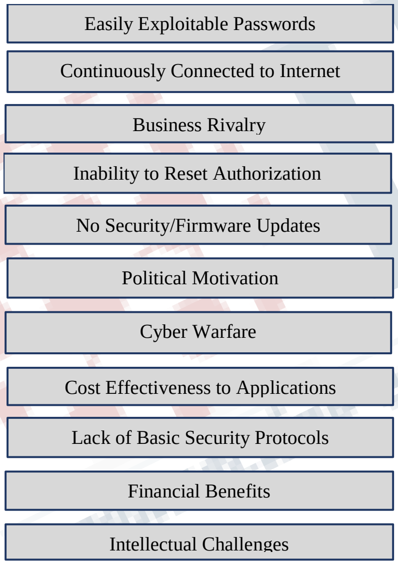
Easily Exploitable Passwords
Continuously Connected to Internet
Business Rivalry
Inability to Reset Authorization
No Security/Firmware Updates
Political Motivation
Cyber Warfare
Cost Effectiveness to Applications
Lack of Basic Security Protocols
Financial Benefits
Intellectual Challenges

Figure-1: Motivations for cyber attacks

The goals of cyber attackers [10] are to launch DDoS attack using the IoT devices as autonomous botnets, unleashing extortion from users by breaching their privacy, Data forgery and Synchronized attacks. In a smart environment, attackers may target 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 [5].

A. Analysis of IoT Security

Threat analysis in IoT can be classified in terms of general security characteristics of confidentiality, integrity, availability, authentication and access control. The components of the IoT environment may be classified as hardware, network and server [12].

(i) Hardware

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

(ii) Network

Compared to internet systems, IoT devices have limited bandwidth and are less complex requiring minimum power. Generally, WiFi is used for interconnectivity of IoT networks, causing them to be prone to jitters. Also due to their limited processing capacity, internet protocols need to be tweaked to be operable in the IoT setups. This is also true for encryption and other security measures.

(iii) Server

The data collected by IoT devices and submitted to server having highly privilege and privacy content, hence, needs to be accessed by authorized users only. The main concern is to deal with rogue devices and spoofing attacks. The Table-1 provides threat analysis of IoT environment.

Table-1: Threat Analysis of IoT Environment

Security Feature	**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

B. DDoS Attacks in IoT

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

IoT protocol stack as below:

(i) 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-2[13].

Table-2: 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.

(ii) 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-3[13].

Table-3: 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.

(iii) DDoS on Application Layer

Table-4: 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.

C. 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 [14]:

- 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. Other 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-5[1] on the internet with the help of compromised IoT devices

Table-5: Attacks of Mirai [1]

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

D. 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 [15], SYN flooding is the leading attack type with more than 79% attacks being SYN flooding followed by UDP flooding at 9.4%. This is graphically presented in figure-3.

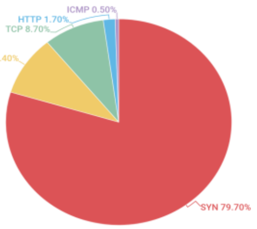

Figure 3. Types of DoS Attacks

IV. PROPOSED SECURITY FRAMEWORK

The proposed system designed by the authors can be termed as "Multilevel Cryptographic Hash function-based Security framework for Internet of Things". This System provides enhanced security to access the IoT devices against DDoS attacks. It is generic in nature and can be used in any IoT device access structure. In this System, two types of users are created with respect to the type of framework. This System includes two types of users viz. Admin user and IoT user. Admin user is able to access Framework I and Framework II. IoT user is able to access Framework III. Frameworks are developed in a such way that those can be accessed through cryptographic Uniform Resource Locators only. Cryptographic URLs are developed by using hash function. This System supports any hash function. However, for simplicity SHA 256 has function is considered. To access administrative account or IoT account, above mentioned cryptographic URLs are essential. Secret keys are used to access the respective frameworks. Secret keys are defined according to the types of user. Based on those secret keys only, user can access the respective frameworks. Respective users of this System are provided with the secrete keys to access the respective framework. A Servo motor is used as an IoT device for the setup.

Figure-4 provides the basic block diagram of the proposed system and Figure-2 provides the proposed secure communication system using the Framework structure.

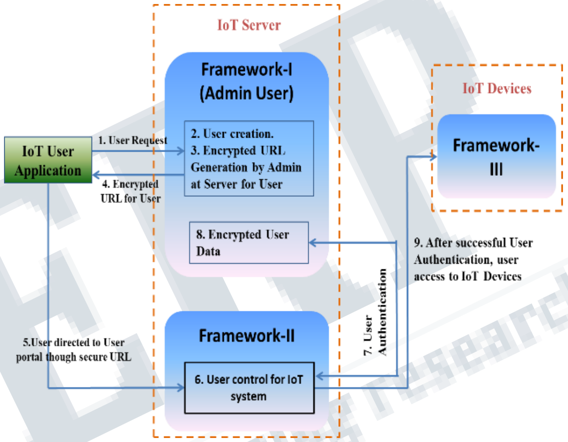
IoT Server
Framework-I (Admin User)
2. User creation.
3. Encrypted URL Generation by Admin at Server for User
8. Encrypted User Data
Framework-II
6. User control for IoT system
IoT Devices
Framework-III
IoT User Application
1. User Request
4. Encrypted URL for User
5.User directed to User portal though secure URL
7. User Authentication
9. After successful User Authentication, user access to IoT Devices

Figure-4: Proposed Framework

A. Salient Features of the Proposed System

The salient features of the proposed system are presented below. During the design of the system stress is made on Low complexity solution, faster DDoS detection and higher availability of desired service as required in a typical IoT setup. Following may be identified as distinguishable solution offered by the proposed solution to the problem statement:

- The proposed system security feature is operating using Layer 7 of the OSI model by employing unique URL thereby providing state of the art mechanism for the security, which can be implemented in any setup seamlessly.

- The Proposed system is a robust mechanism for mitigation of DDoS attack on IoT setup as it employs low complexity solution for the mitigation taking into account the limited processing capabilities of the IoT setup. It uses one framework at a time thereby limiting the processing and memory requirements of the system.

- Low complexity SHA 256 algorithm is used for encryption thereby, offering a light weight security approach.
- As can be seen during performance evaluation, described subsequent sections, it is seen that the Proposed system provides a higher magnitude of improvement in CPU Utilization, Lower detection time and significant lower round tip delay or latency indicating effective DDoS mitigation and availability of critical resources for the functioning of IoT systems.

Following Parameters are analyzed for the evaluation of the system:

- CPU utilization characteristics
- Execution time
- Thermal readings

CPU utilization is the measure of the system availability for performing the action. Figure-5 shows the performance of the CPU on idle condition and under DDoS attack.

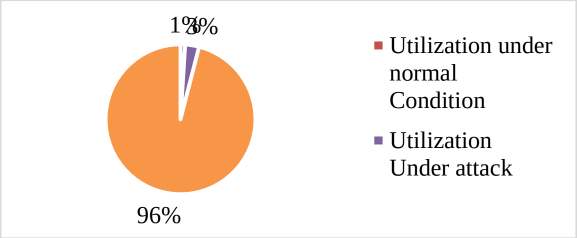

Figure-5: CPU utilization during DDoS attack

The above analysis indicates that the desired action is completed by the setup with minimal CPU utilization and also shows a state of art performance on the event of a DDoS attack.

Figure-6 details the execution time analysis of the setup. It shows total time of execution from providing the instruction by the user to performance of the activity concerned. The entire duration of the execution is < 1.1 seconds, which includes the physical start and stop of the motor connected. This shows the efficiency of the system to perform the assigned task in real-time.

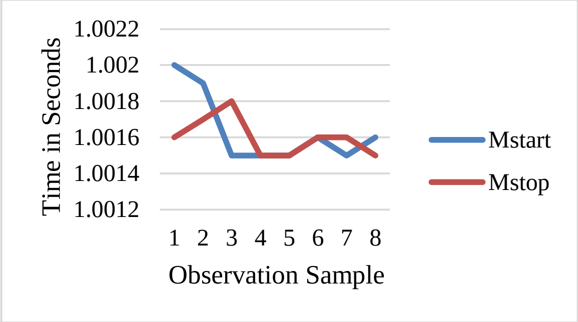

Figure-6: Execution Time analysis

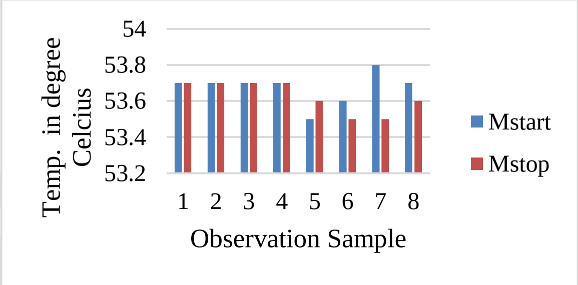

Figure-7: Thermal analysis of the setup.

Figure-7 indicates that the desired activity is completed without any major increase in the system temperatures indicating that the activity is performed in relatively good efficiency and in real time manner.

The proposed system is highly efficient in performing the assigned task in real-time and has capability to integrate more such activities to have a complex functionality. Further the system is demonstrating promising results in detecting and mitigating the DDoS attacks in the system.

V. CONCLUSION

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 are 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. A detailed study is conducted on the DDoS attacks faced by the IoT environment and the mitigation techniques available. Based on the analysis, a security framework is proposed to secure IoT deployment involving all the stake holders.

VI. 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. 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 be studied and exploited in a limited scale and necessary security policies as described above may be implemented to mitigate the vulnerabilities.

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] 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.

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

[5] 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.

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

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

[8] 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.

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

[10] Online Resource available at https://www.conduiraonline.com/index.php/detail/368- what-is-a-smart-city

[11] 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.

[12] 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.

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

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

[15] 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

[16] 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.