FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 2, Issue 4 | Pages 106-110 | ISSN XXXX-XXXX

Impact of 5G network on Internet of Things (IOT)

Sadhana Singh
Assistant Professor, ABESIT, AKTU, Lucknow, Ghaziabad, India , sadhana.singh.cs@gmail.com

***Correspondence:** *sadhana.singh.cs@gmail.com*

ABSTRACT- Now a days IOT (Internet of Things) is very common. IOT is that which is used to do some work with the help of sensing devices. In this we simply do any work with senser devices. We do any communication with sensors we need IOT devices. 5G network is the mobile network. It is the combination of different services which comes from different mobile network like 1G, 2G, 3G and 4G. In this paper I tell you about how 5G mobile network effect on IOT.

Keywords: 5G network, Internet of Things, Man in the Middle attack, Brute Force attack, Denial of Service Attack, Botnet.

ARTICLE INFORMATION

Author(s): Sadhana Singh;
Received: 05/10/2023; **Accepted**: 10/12/2023; **Published**: 30/12/2023;
e-ISSN: XXXX-XXXX;
Paper Id: IJCSR-020402;
Citation: 10.37391/IJCSR.020402

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

In today's scenario we do many things with the help of Internet. Let we take an example of video call we have to use the concept of Internet of Things. In this we simply use the mobile devices, laptop, tablet, etc., for video call with the help of Internet of Things. In past time there is no any system to which we simply call to someone or like videocall, at that we simply use like letters for posting from one place to another for talking but not any device used for video calling.

Internet of things are used regularly at present time. We simply pay any bills like electric bill, mobile bill, sending email, transferring money with the help of Internet of things. IOT is a network in which we use both hardware and software for communication. We have to use mobiles, laptop, tablet and computer for net we use LAN devices to connect network and provide facility to networking.

In today's scenario we use the 5G network for networking. In past decade we communicate simply letters but if 1G come in world the simply we call only. Then 2G come, in this we simply call and messages from one place to another using mobile devices, in 3G we use wireless technology to improve the quality of calling and messages and introduces MMS (Multimedia Messaging Service). In 4G introduces video call for calling. So, 5G network comes to improve all the qualities of the 4G network.

5G network is the wireless mobile device network to improve the better quality of voice calling, video calling, SMS (Short Messaging Service) and speed of network. Through the 5G network we do different things with the help of wireless technologies. 5G network is used to convey many things like we can control the temperature of AC (Air Conditioner) easily. We can also watch anything with the help of mobile just after installation of the video camera.

2. LITERATURE REVIEW

5G Technology stands for 5th generation mobile technology. 5G represent the next major phase of mobile telecommunication ethics beyond the upcoming 4G standards. 5G technology is contribution the service in Product Manufacturing, Documentation, supporting electronic communications, etc [1]. As the purchaser become more and more aware of the mobile phone technology, he or she will look for a decent package all together including all the advanced features a cellular phone can have [1]. Hence the search for new technology always the main motivation of the top cell phone colossuses to out innovate their competitors [1]. The aim of a 5G based telecommunication network would perfectly answer the challenges that a 4G prototypical would present once it has entered ubiquitous use [1]. No one company or person owns 5G, but there are numerous companies in the mobile ecosystem that are causative to bringing 5G to life [1]. Qualcomm has played a major role in originating the many introductory technologies that drive the industry forward and make up 5G, the next wireless standard [1]. South Korea is the country which arrayed the first 5G networks and the state is expected to stay in the lead as far as penetration of the technology goes, by 2025, nearly 60 percent of mobile contributions in South Korea are anticipated to be for 5G networks [1]. Huawei Technology Co. owns the utmost copyrights on the next-generation of 5G technology, confirming the Chinese company will get paid despite Trump administration exertions to erase it from the supply chain, according to a new study [1].

Even a few decades back, nobody could have imagined having a video chat with their families in a different continent [2]. All of these is due to technology getting cheaper, and devices emerging with new and improved capabilities [2]. People can get things done with a click on their smartphone, be it sending emails, paying bills, transferring money or booking a cab [2]. What we had since 1991 was "Internet of Computers (IoC)" and it gradually grew in size as more and more people started using it [2]. With the advent of pocket phones and connected devices,

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 2, Issue 4 | Pages 106-110 | ISSN XXXX-XXXX

the Internet of Devices started and eventually grew larger as mobile phones, computers, laptops and tablets became cheaper and more accessible to the common man. Gartner, Inc. forecasted that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020 [3]. In 2016, more than 5.5 million new things got connected every day, thus, emerging the huge scope for Internet of Things. Since various things are continuously connecting to form an IoT, there are various disciplines that get associated with IoT [3]. Therefore, IoT can also be thought of as a combination of various domains. *Figure 1* gives a representative list of some domains (most of these overlap with each other in terms of concepts and techniques) constituting the IoT. Internet of things is just a connected system of physical things (like appliances, crop fields, plants, animals, etc.) and humans [2]. Humans are connected to these devices using some smart objects attached to both which are capable of sending, receiving and analyzing data [2]. These smart objects represent the entity (a human or a physical thing), it is attached to, in the network [2].

3. METHODS OF ATTACKING IOT DEVICES

IOT is the technique in which we simply done various things like video calling, video conferencing, etc. But there are various attacks are occurred during transmission of data from one place to another. Attack surfaces may vary from hardware, software and firmware also through IOT in the network or we can say cloud area. There are various attacks occur through the IoT devices which is occurred through the three surface areas.

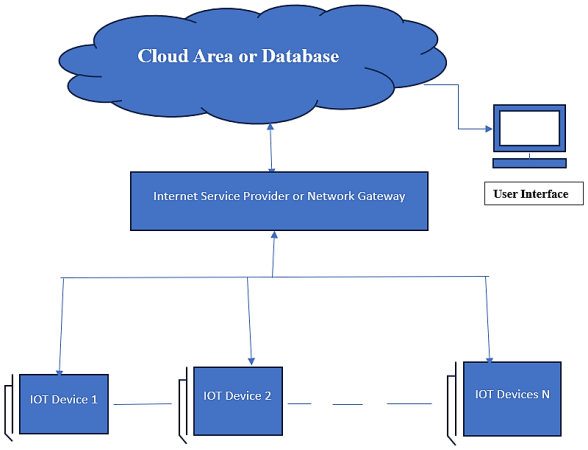

Figure. 1. Breakdowns of different services in IOT devices

Figure. 1. Shows the conversation among the IOT devices to the cloud service with the help of Internet Service Provider.

3.1 Man-In-The-Middle Attack

This attack is associated for the communication between two channels. In this attack if sender sends any information to the receiver, but receiver is not received at time then this attack is occurring. This attack is done via two ways: one is in which at sending time before receiving the information to the receiver information is changed by the attacker. Second one is in which the attacker is hack the information and modification is done and then sending the duplicate file or hacked file to the receiver. *Figure 2* [4] shows the Man-In-The-Middle attack.

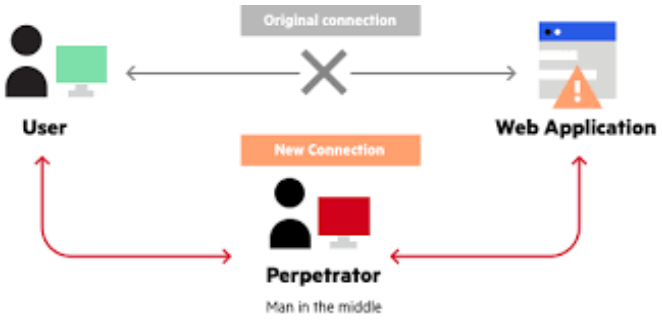

Figure 2. Man-in-the-Middle Attack

In regards to IoT, the attacker usually performs between MITM attacks and an IoT device [5]. IoT devices, in particular, tend to be more vulnerable to MITM attacks as they lack the standard implementations to fight the attacks [5]. There are two common modes of MITM attacks: cloud polling and direct connection. In cloud polling, the sender and receiver communicate continuously and then the attacker monitor this and capturing the information between the communication through the cloud or we say like footprint. Attacker can hack the network using the Address Resolution Protocol (ARP) poisoning or by inject coding in the Domain Name System (DNS) settings or intercept HTTPS traffic by using self-signed certificates or tools such as (Secure Sockets Layer) SSL strip [5]. The attacker in this attack shows like the bridge between the sender and the receiver for the communication. The attacker can easily able to read, Insert and modify any thing in the message transmission between sender and receiver.

3.2 Botnets

Botnet attack is work like Robot. Robot is doing work with the help of command, so the botnet attack is also doing such activities like password hacking, sensitive information hack, etc. using the commands. When botnet attack occurs, the speed of the server is too slow. Because the attacker hacks the main server and automatically control all over the connected systems to the server and then the user's information is also hacked by the attacker. Working of botnet attack is shown in *figure. 3* [8].

There are various kinds of attack happened due to IoT devices and is employing various tools to manage botnets and develop the Distributed Denial of Service (DDoS) attacks [6]. A denial of service (DoS) attack is defined by an arrangement of the effort to stop the illegal use of a service; a DDoS attack, attacks from multiple sources to point this goal [6]. DDoS attacks aim to find out the main server and attack them with the help of the botnet and rootkit installation on victim's computer [6]. DDoS attacks commonly go through a limited stages like recruitment, in which the attacker can fine the weak point of the victim's computer to be used in the DDoS to attack against the target; exploitation and infection, in which the vulnerable point is searched and then malicious coding is injected by the attacker; communication, in which the attacker assesses the infected

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 2, Issue 4 | Pages 106-110 | ISSN XXXX-XXXX

machines, sees which are online and decides when to schedule attacks or upgrade the machines; and attack, in which the attacker commands the infected machines to send malicious packets to the target [6].

One of the most famous malwares, the Mirai worm, has been used to perpetrate some of the largest DDoS attacks ever known and is designed to infect and control IoT devices such as DVRs, CCTV cameras, and home routers [7].

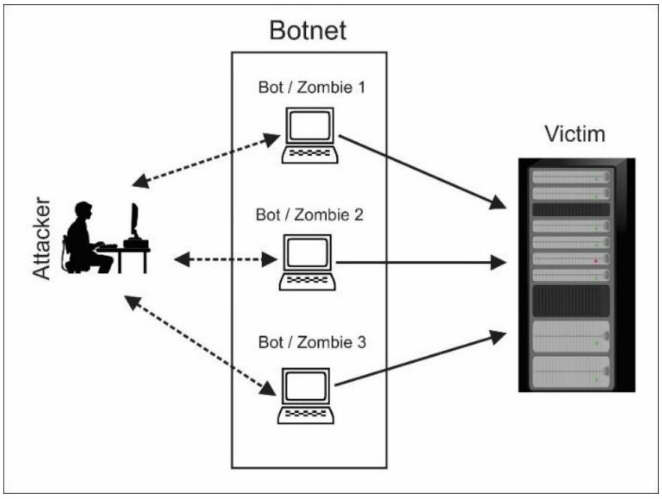

Figure 3. Working of Botnet Attack

3.3 Brute-Force Attack

The brute force attack, in which the attacker is used the concept of hit and trial method to threat our sensitive information's like login credentials, debit card pin, credit card pin, etc. So, we simply update the system, regular booting of the system, use updated antivirus and always try to make a strong password for protection.

In cyber security, a brute force attack is the web based attack. A brute-force attack, contains of an attacker hitting many passwords with the expectation of eventually guessing correctly [9]. The attacker continuously checks all possible ways to guessing passwords and tricks until the correct one is found [9]. An attacker can also guess the password he uses the key generation techniques. This is known as an exhaustive key search [9]. In cryptography, a brute-force attack is used to encrypt and decrypt the password by using the public and private keys. If the victim is chosen the password in minimum length, then attacker can easily guess this password by using hit and trial method. If we maintain the password in a strong way like we can use the capitalization of the character, small case of the alphabet, numbering and special characters, then the password is strong and the attacker is not easily hacked. If victim is managing your password by the combination of upper case, small case, numbering and special character then password is strong and also the password length is high, then attacker is not easily guessing this password. So, we need to know the length of maximum strong password is minimum 8 bits.

3.4 Denial of Service Attack

IoT devices may often carry out DoS attacks, but they themselves are susceptible to them as well [10]. IoT devices are particularly susceptible to permanent denial of service (PDoS) attacks that render a device or system completely inoperable [10]. This attack shows the user the website or the server which you like to know is like not available or busy. We all to know that if we search any thing on the internet then sometime, we see that the web page is not available, or we fill any form but the server site is taken too ling time then this case Denial of Service attack occurs. DoS attack is showing the website is unavailable because the attacker is injecting some malicious coding on that webpage. If we click on this webpage which is occurred due to malicious coding the just move another web page which had been derived with the help of this malicious coding. This attack attacks the single website to the single internet connection because if we fill any form from website, in this case we perform all the task on the single form link, in this case the attacker can easily hack the main server network to hack the information to the victim.

4. IMPORTANCE OF IOT IN CYBER SECURITY

IOT is the platform where we can use the different types of hacking techniques to hack the information of the victim. Through the IOT attacker can easily install the rootkit in the system and then access the information of the victim. In today's era there are various types of mobile phones available in market and many new app used for real life configurations. With the help of IOT devices hackers can access the victim's personal information by using the spyware technique. Spyware is in which the attacker is continuously watching the victim's information and used this information for personal use.

Keylogger technique is used to capture the key press information of the victims. In this process the attacker continuously checks your key press information and store this for personal use.

5. DIFFERENT TYPES OF NETWORK

There is various type of network used for communication in between source and destination, sender and receiver, etc.

5.1 1G Network

This was the first generation of cell phone technology [11]. First generation of cellular network was introduced in 1970s. but it was implemented in 1980s. It was introduced in 1987 by Telecom (known today as Telstra), Australia received its first cellular mobile phone network utilizing a 1G analog system [11]. This is an analog technique and in this case the battery of the cellular phone is very poor because of the charging capacity is very weak. In first generation we can use mobile phones only for calling. At that time there is no any concept like SMS (Short Message Service). The maximum speed of cell phone in First Generation network is 2.4 Kbps [11].

5.2 2G Network

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 2, Issue 4 | Pages 106-110 | ISSN XXXX-XXXX

In 1980s second generation of cell phone replaces the first-generation cell phones. In first-generation transmission of signals in the form of analog but in second generation network the transmission of data in digital form. In second generation, network we communicate by using the CDMA (Code Division Multiple Access) and GSM (Global System for Mobile Communication). In this generation we send any message from one place to another by using SMS. If we send any videos then MMS (Multimedia Messaging Service) was introduced in second generation cell phones. Second generation 2G cellular telecom networks were commercially launched on the GSM standard in Finland by Radiolinja (now part of Elisa Oyj) in 1991 [11]. With the help of 2G network we can call the voce call, conference call, find roaming, etc. The max speed of 2G with General Packet Radio Service (GPRS) is 50 Kbps or 1 Mbps with Enhanced Data Rates for GSM Evolution (EDGE) [11].

5.3 3G Network

After upgradation on second generation, 3G was introduced in 2000. But firstly, in commercial use in Japan in 2001. In this we more focuses on wireless technology. In this we can easily perform any downloading, sharing of pictures, videos, and many more thing by using the cellular phones. In third generation we more emphasis on the speed of the network at the time of sending and receiving any videos and pictures, voice transformation in clear ways.

5.4 4G Network

In fourth generation network we introduce more features on the third-generation network. Fourth generation network is also wireless technology. In this we increase the data transmission with security, voice transmission at high speed, call recording, video calling, multimedia services. This cutting-edge technology opens doors to a wide range of potential and existing applications, including improved mobile web access, IP telephony, immersive gaming experiences, high-definition mobile TV, seamless video conferencing, captivating 3D television, and efficient cloud computing solutions [11].

5.5 5G Network

5G, or the Fifth Generation, refers to the latest advancement in wireless communication technology [11]. Fifth generation network offers very fast speed for downloading and uploading of any huge amount of data in little time. It increases the capacity to do many tasks simultaneously. It enables transformative applications and services such as autonomous vehicles, Internet of Things (IoT), augmented reality (AR), and more [11].

6. 5G NETWORK ON IOT

5G network is the latest technology for transferring any simple information or videos, photos from one place to another by using the IOT. With the help of 5G network we can easily transform any information in very fast and accurate speed. Video calling is done very frequently. With the help of 5G network we can access all the services regarding IOT. We can easily perform the sensing information like we can adjust the temperature of Air Conditioner (AC) with the help of mobile devices. We can adjust the web camera security by installing the app and we can watch anytime and anywhere with the help of the 5G network and IOT devices. We can also imagine the virtual images is like real images with the help of the 5G network and the Internet of Things. For security purposes 5G technology is very useful because there are various cases of threats occur regularly.

If we put the cameras then then install this app is in your mobile devices then we can watch anytime and anywhere.

7. CONCLUSION AND FUTURE SCOPE

5G network is used to relate the real-world things to the human life. 5G network is increase the speed of downloading any data. With the help of 5G technology we can sit anywhere but we can watch everything but putting the camera. With the help of 5G technology we don't need to remote for controlling the any devices like AC temperature, Controlling the key functionalities of Televisions, etc. IOT is that it is the medium through this the functionalities are doing like controlling the television management, controlling room temperature, etc. With the help of Internet of Things, we sit anywhere but we can easily pay any electricity bill, credit card bill, etc. but 5G network is used to increase the speed of the network. Smart watch is the best example for the 5G technology and IOT.

In future people can make different gadgets for sensing the information from one place to the other with the help of the 5G technology and Internet of Things.

Acknowledgment

I really thankful to God, my family members to making this possible.

REFERENCES

[1] Vinayak Pujari, Rajendra Patil and Kajima Tambe, "Research Paper on Future of 5G Wireless System", Contemporary Research in India (ISSN 2231-2137): Special Issue: April 2021.

[2] Ashish Ghosh, Debasrita Chakraborty and Anwesha Law, "Artificial Intelligence in Internet of Things",IET Reasearch Journals, pp- 1-11, 2015. ISSN: 1751-8644.

[3] D. Câmara and N. Nikaein, Wireless Public Safety Networks 2: A Systematic Approach. Elsevier Science, 2016.

[4] https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[5] Cekerevac Z, Dvorak Z, Prigoda L, Čekerevac P. Internet of things and the man-in-the-middle attacks–security and economic risks. Mest J. 2017;5:15–25. https://doi.org/10.12709/mest.05.05.02.03.

[6] De Donno M, Dragoni N, Giaretta A, Spognardi A. Analysis of DDoS-capable IoT malwares. In: 2017 federated conference on computer science and information systems (FedCSIS), Prague; 2017. p. 807–16. https://doi.org/10.15439/2017F288.

[7] Mirai Botnet DDoS Attack. Corero, Corero. http://www.corero.com/resource-hub/mirai-botnet-ddos-attack/. Accessed 9 Dec 2019.

[8] https://www.researchgate.net/figure/A-Typical-Botnet-Attack-Structure_fig1_298788691

International Journal of
Computer Science Research (IJCSR)
Survey Article | Volume 2, Issue 4 | Pages 106-110 | ISSN XXXX-XXXX

[9] Kanakam Swathi, "Brute Force Attck on Real World Passwords", Internation Journal of Research Publications and Reviews, Vol 3, no 11, pp 552-558, November 2022.

[10] Herberger C. DDoS fre & forget: PDoS—a permanent denial of service. Radware Blog, Radware Ltd. http://www.blog.radware.com/security/2015/10/ddos-fre-forget-pdos-a-permanent-denial-of-service/. Accessed 12 Sept 2016.

[11] https://net-informations.com/q/diff/generations.html