International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-9, July 2020

Networking in IoT: Technologies used, Security Threats and Possible Countermeasures

Purnima Gupta, Aswani Kumar Singh, Archana Sharma

Abstract*: IoT is the networking of daily use objects. Internet of Things amalgamates various kinds of physical object to communicate with each other directly. These objects are commonly known as constrained devices. Constrained devices work with low memory, low storage, and low computation power. Implementing security algorithms in these devices is challenging. The researchers take these challenges as opportunity. The diverse and heterogeneous structure of the IoT phenomenon introduces a variety of new security risks and challenges. Many threats, like botnets, home intrusion, remote control of the IoT devices, and man in the middle attacks, are emerging and need a stronger security implementation to protect IoT devices from being compromised. The authors surveys different kinds of IoT networking technologies, security challenges and solutions of these challenges to form more secure IoT environment for trustful adoption of services through industrial or personal use. In this paper, the authors presented a study of numerous networking technologies along with possible threats and their countermeasures.

***Keywords*: IoT, RFID, Wi-Fi, Wi MAX, LoRaWAN, Ransomware, Botnet, APTs, Intrusion.**

I. INTRODUCTION

The Internet of Things is complex network architecture consists of variety of devices, sensors and equipment. It follows different communication protocols forming the heterogeneous devices connectivity. An IoT network refers to a collection of interconnected devices that communicate with other devices, for example, smart appliances and wearable things etc. The fundamental features of IoT networking architecture to sustain computing functionalities are scalability, availability, and maintainability. IoT is getting more attention of researchers and industries from last two decades. The main objective of IoT is the free flow of information by connecting various types of digital or physical objects having different communication protocols [1]. Devices are connected in the IoT platform through an internet connection to deliver a specific type of service using real-time communication. IoT includes communication technologies like Radio Frequency Identification (RFID), Cloud Computing, Wireless Sensor Network (WSN), Near Field Communication (NFC), Machine to Machine (M2M) Communication, Low Power Wireless Personal Area Network (LoWPAN), Worldwide Interoperability for Microwave Access (WiMAX), and others. IoT concept was initially given by Kevin Ashton in 1982 to establish an interface between human beings and the virtual environment to make their life easier [2].

The growth rate of connected devices in IoT is highly tractive today. According to an article published in Forbes, the global market of IoT growth is predicted from $157 billion in 2016 to $457 billion by 2020, attaining a Compound Annual Growth Rate (CAGR) of 28.5% [3]. The number of connected devices in IoT will grow up to 50 billion in 2020 and will surge up to 125 billion by 2030 [4].

Security vulnerabilities and cyber-attacks are more advanced and improved than before. IoT devices are widely used in electronic health monitoring systems, smart cards, home appliances, military and other types of personal or industrial objects. These devices could be vulnerable to external threats like malware, viruses, hackers, physical damages and theft. A hacker can attempt to launch phishing, SQL injection, cross-site scripting, and DDoS attacks to hack, performance downgrade or damaging devices used in IoT. Some of the popular attacks on IoT have been discussed below.

STUXNET is a malicious computer worm which affected the industrial Programmable Logic Controllers (PLCs) in Iran's nuclear-fuel enrichment project. Although STUXNET was not a type of IoT attack it was a sign that smart devices can be compromised [5]. The Mirai Botnet attack was launched to infect older routers, DVD players or IP cameras especially in 2016[6]. Mirai used these compromised IoT devices to launch the HTTP flood attack (DDoS attack) to the Dyn server. This IoT Botnet is made by Mirai malware and causes Twitter, New York Times, Netflix, GitHub, and CNN like networks to get affected by DDoS attack. The Reaper (IoTroop) was another botnet which stunned everyone in 2017, more dangerous than Mirai botnet [7]. Reaper botnet came in spotlight in September 2017 and infected over one million wireless networks. Reaper is an evolution of Mirai and uses more sophisticated hacking tools and software than Mirai. Another very harmful malware called BrickerBot came into existence and is capable of killing any unsecured IoT device. The most awful thing about BrickerBot is that consumers of IoT devices could never know that their devices are affected by this bot. BrickerBot finds an unsecured IoT device on the network and performs a series of Linux commands to corrupt the device storage or disturbs the connectivity to affect the device performance [8].

Revised Manuscript Received on July 30, 2020.
***** Correspondence Author
Purnima Gupta*, IT department, Institute of Management Studies Noida, Noida, India. Email: purnimaa018@gmail.com
Aswani Kumar Singh, Software Engineer, Soft-Tech development Solution, DDU, India. Email: aswanikumar124@gmail.com
Dr. Archana Sharma, IT department, Institute of Management Studies Noida, Noida, India, Email: asharma12569@gmail.com

The IoT environment are still having many security loopholes. It needs a strong and trustful security mechanism to eliminate these loopholes.

A clear and complete structure and design of IoT is yet to define and this could be a reason that the above threats are still capable to harm devices and applications in IoT. A possible architecture for IoT is shown in figure 1.

The rest of the paper is organized in the following sections. Section 2 describes the communication strategies in IoT. In section 3, existing security threats and vulnerabilities that can harm IoT devices are discussed. Section 4 describes major technologies and mechanisms to Secure IoT. In section 5, the authors have given the summary related to the topic that can help to identify all the risks and challenges before the adaptation of IoT. In section 6, conclusions about IoT security solutions and future scope for better security is provided.

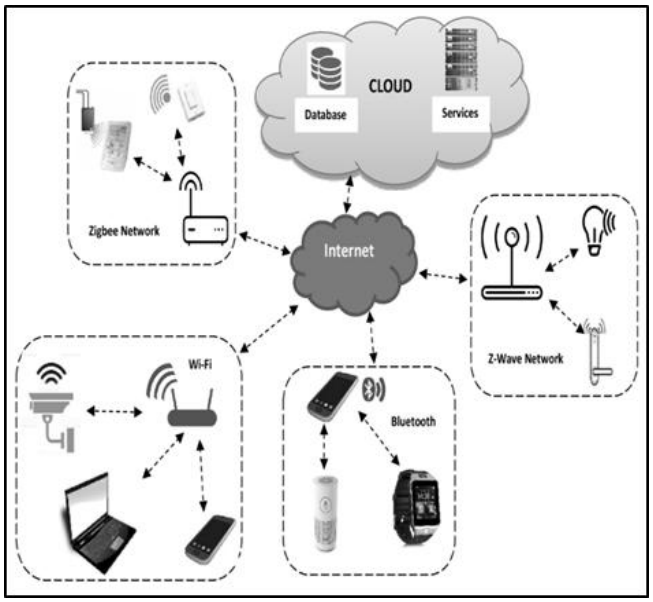

Fig.1. IoT Architecture

II. COMMUNICATION STRATEGIES IN IOT

Different networking technologies have been adopted in IoT. In this paper authors have described eight communication strategies with their operative background and architecture. Table 1 presents different IoT network architectures on different criteria like frequency, data rate and range. It also shows the vulnerabilities associated with each networking technology.

ZigBee is a low data rate, low power consumption, and low-cost wireless networking protocol used to define the operation of Wireless Sensor Networks (WSNs) and currently uses IEEE 802.15.4 MAC and PHY layers. IEEE and ZigBee combined their technological research regarding communication in devices inbuilt with Bluetooth technology and having low power and low data rate. These devices require long battery life and do not require the high-speed data rate. The range of these devices may vary from 10 meters to 75 meters. The data rates are 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, 20 kbps at 868 MHz [9]. ZigBee provides interoperable data networking which operates on the upper level of the protocol stack (network Layer to application Layer). This will eliminate the consumer's dependency on product manufacturer and ensures the working between different manufacturer devices [10].

The RFID (Radio Frequency Identification) allows a computing device to read the identity of RFID tags from a distance and is a replacement of Barcode technology. RFID devices can be categorized into two classes. First is Active class, in which devices use power either from an integrated power source battery or connected to a powered infrastructure. The second class is Passive RFID which contains antenna, a semiconductor chip attached to an antenna and some form of encapsulation [11].

Table I: Different Communication Strategies in IoT

Networking Technology	Frequency (GHz)	Stream Data rate (Kbps)	Approximate Range (Meter)	Vulnerabilities
ZigBee [12]	2.4	250	150	Device tempering, key secrecy required
RFID [13]	2.45	640	100	MITM Attack, Sniffing, Denial of Service attack, Cloning & Spoofing
NFC [14]	0.13	424	0.04	Low range, Low Security
WiMAX [15]	66	126976	50000	The jamming attack, Scrambling attack, Water torture attack
BLE [16]	2.4	2048	10	Bluejacking
Wi-Fi [17][18]	5	55296	100	Vulnerable to passive attacks, Jamming and Scrambling.
6LoWPAN [19]	2.4	250	100	Low security in multi hop
LoRaWAN [20]	0.923/ 0.915/ 0.868/ 0.433	50	20000	Once hackers have the encryption keys, they can perform DoS attacks

Near Field Communication (NFC) uses magnetic field induction to establish communication among short-range and high-frequency wireless devices. NFC devices use a peer-to-peer network to perform data exchange. NFC is an upgrade to the RFID technology and has been developed by Philips and Sony jointly [21]. NFC operates in three different modes. In read/write mode interaction is made with an NFC-enabled device that reads the data from a device or writes the data to a device. In peer-to-peer mode, two-way communication is established between NFC enabled devices. In card emulation mode, the system acts as a contactless smart card [22].

Machine to Machine (M2M) system establishes direct communication between two IP-based IoT machines or sensors over wired or cellular networks to send the data to gateways or cloud servers in IoT network. Human interaction is not required for communication between devices [23].

The Worldwide Interoperability for Microwave Access (WiMAX) allows the high-speed data transfer (30-40 MBPS) and belongs to IEEE 802.16 wireless family.

WiMAX is much faster than Wi-Fi and its range for connectivity and data transfer is up to 40 kilometers. Thousands of users or devices can be connected simultaneously through this network with security level implementation which lacks in Wi-Fi network [24].

Bluetooth Low Energy (BLE) uses IEEE 802.15.4 for communication between ultra-low-power IoT devices. BLE may use one of the topology formations like the tree, mesh, cluster or star for the connectivity. BLE implements frequency hopping over 37 channels for bidirectional and three channels of unidirectional [25].

IEEE 802.11 is a set of technical specifications related to communication between Wi-Fi devices. These specifications are related to the physical layer and Media Access Control (MAC) layer that connects devices like printers, scanners, smartphones, and laptops without wires. These network connections are an easy target for passive attacks. Active attacks can also be performed by exploiting hardware security loopholes and protocol vulnerabilities [26].

Low-Rate and low power Wireless Personal Area Networks (6LoWPAN) sends the data in the form of packets and uses IPv6 over the wireless network. Internet Engineering Task Force (IETF) defines the 6LoWPAN which later defines the compression and encapsulation mechanisms that enable the IPV6 over low power wireless LAN (WLAN). 6LoWPAN is being used in application areas of industrial monitoring, smart grid, general automation, home automation. 6LoWPAN utilizes the IEEE 802.15.4 to provide low layers for low power wireless network and uses 128-AES link-layer security defined by IEEE 802.15.4. IPv6 is applied to PHY and MAC layer in 6LoWPAN communications of the existing 802.15 standards [27]. LoRaWAN stands for Low Power Wide Area Network and as that name suggests, it refers to the features that support low-cost, low power, mobile communications for the IoT. It features low-power operation (around 10 years of battery lifetime), low data rate (27 kb/s with spreading factor 7 and 500 kHz channel or 50 kb/s with FSK) and long communication range (2–5 km in urban areas and 15 km in suburban areas) [28-30].

III. SECURITY THREATS AND VULNERABILITIES IN IOT

Spam is a messaging system which sends unrequested bulk messages to a target device. Spam filters are the option to identify and stop these unwanted messages. Spammers can use 2D bar codes to flood the physical site of the IoT and mislead users to reach unsolicited and unrelated content over the Internet [31]. The digital signature system can be used to overcome this problem. Mass flooding, website referrals, and Redirection hiding technique are the spamming techniques used by spammers.

Advanced persistent threats (APTs) is a type of attack in which an unauthorized user gets foothold through malware, physical malware infection or external exploitation to execute future continuous attacks for a long time period to achieve his malicious objective without being detected. There are many activities performed in this attack like network hacking, detection avoidance, determining the target area, collecting important information to gain access. This attack is basically targeted, goal-oriented, persistent and unnoticed in nature [32].

Ransomware is a type of malware that encrypts all data of your computer and sales the decryption keys to decrypt. The damage made by ransomware is irreversible and the decryption key is required for getting data back. The ransomware is a more serious threat for IoT because its action cannot be reset with our own and will have to pay for that.

Data and Identity theft could be a more serious security-related problem in the IoT. Suppose that all information got by your smartwatches, fitness tracker, GPS location data, and social media is combined together and may be sufficient to reveal your identity. Thus, identity and data theft are one of the biggest threats to the IoT [33].

Smart home corresponds to a heterogeneous network structure having a variety of devices, applications, and technologies connected together. The globally available smart home ecosystem data may prone to a security vulnerability. This electronic data needs to be protected from external intrusions which may cause several security issues like denial of service attacks [34]. Home Intrusion could be launched through several attacks like DDoS attack, Device Hijacking, and phishing (PDoS). Intrusion Detection Systems (IDS) are highly required for the safety of electronic data of a smart home. Current security measures of connected vehicles in IoT are in the poor state today. Connected remote vehicles may face several security-related issues like vehicle sensor attack, wireless carjacking, GPS Jamming and spoofing, back door attacks, front door attack, hacking of remote vehicle control application. Figure 2 has shown some of the security threats in the IoT environment. Intercepting a communication channel with malicious intention between two systems without acknowledgement of sender and receiver is called the man in the middle attack. The man in the middle attack can be launched through several techniques like Address Resolution Protocol (ARP), DNS spoofing, session hijacking, and sniffing. Once a communication channel is compromised, an attacker can hear all communication as well as can transmit false messages too. In the scenario of IoT, this attack can be more effective and saboteur.

An interceptor can track your daily activities through compromised IoT devices like health monitoring system, smart cars, mobile devices, cameras, GPS navigation system and many others. Smart cars can be misguided; false health monitoring system data can be transferred to show emergency situation. A strong encryption mechanism like RSA, AES, and Blowfish can be used in IoT to get protected from this threat [35].

Radio-Frequency Identification (RFID) Skimming is the process of stealing the data or information through a chip reading device from RFID chips. Most of the new debit cards, credit cards and identity cards contain RFID chips inside them. These RFID chips use radio waves to read and capture the information from several feet away and this facility can be used to hack the RFID chips for malicious intentions. Hacked information can be used to create duplicate cards or chips and use them for illegal financial benefits.

The unencrypted data travelling to cloud interface from IoT devices can be intercepted by attackers. Cloud computing introduces potential security-related risks to IoT devices connected with the cloud.

Although cloud has many strong security implementations when IoT devices with insecure credentials, unencrypted data transmission, and weak authentication mechanism connect with the cloud computing, this type of insecure connection possesses many security vulnerabilities for IoT-Cloud collaboration.

IoT devices with a mobile interface having weak or no security implementations are one of the biggest threats for the IoT.

Information can be hacked from the wearable, remote vehicle control system, remotely controlled home appliances, and other computing devices and sensors connected with an insecure mobile interface. An attacker can trace anyone's health-related information, identity, banking details easily through intercepting insecure mobile interface.

Insecure software and firmware is an easy target for botnets or malware. IoT devises firmware falls under two categories: embedded and OS-based firmware. Non-encrypted communication to the firmware of IoT devices is vulnerable to external threats like botnets. Access to these devices' firmware must be password protected and regular updates must be performed for better security. The easiest targeted devices are with default passwords. Default passwords must be changed as soon as possible to save the device from botnets and malware.

Table II: Popular Botnets with their attack techniques

IoT Botnets	Year	Attack Technique
Dark_nexus	2020	Hijacks IoT resources to carry out devastating DDoS attacks.
Mozi	2019	Used to launch distributed denial-of-service (DDoS) attacks, for data exfiltration, and for payload execution.
Brickerbot	2017	Uses exploit code to gain access and rewrite the device's flash storage with random data.
Hajime	2016	Targets devices via Telnet and gains access by brute-forcing default credentials.
Linux/IRCTelnet	2016	Sends UDP and TCP floods in both Ipv4 and Ipv6 protocols.
Mirai	2016	DDoS attacks, GRE floods and Water Torture attacks.
Bashlite	2015	Infects Linux system to launch DDoS attacks.
Wifatch	2014	Removes other malware and disables telnet access.
Aidra	2012	Telnet-based attacks on IoT devices.

IoT botnets are compromised independent internet-connected IoT devices like wearable, medical instruments, industrial systems infected with malware. These compromised devices and sensors are internet-enabled and able to transfer data automatically. Devices infection increases from one infected device to another without the knowledge of the device owner. Attackers can use these compromised devices as a botnet to launch DDoS attacks. Aidra, Bashlite, Linux/IRCTelnet, Hajime, Linux, Wifatch, Brickerbot and Mirai are some popular IoT botnets. IoT botnet is more destructive than traditional botnet and is the biggest threat for IoT network today [36]. Mirai is one of the biggest destructive botnets [37]. The first Mirai botnet attack (DDoS attack) was traced on 20 September 2016, against the website of journalist Brian Krebs at the 620Gbps.Over 24000 systems infected in this massive attack [38]. The Mozi botnet has been caught on September 2019 which relies on the distributed hash table (DHT) protocol to build a P2P network and uses ECDSA384 and the XOR algorithm. Mozi botnet uses algorithm having instruction for DDos attack, collecting bot information, execute payload on specific web address, and execute custom commands. The algorithm used to build this bot has combination of three different kind algorithms i.e. Gafgyt, Mirai, and IoT Reaper belong to malware family. it uses P2P network and there is no single point so that this bot can be eliminated completely. Another botnet Dark-nexus is based on Mirai and Qbot and uses identical code pattern of both. Dark-nexus has same attacking technique as it launches DDoS attacks and hijacks the vulnerable IoT devices.it was built by a known botnet author for selling it online to launch DDoS attack for economical profit.

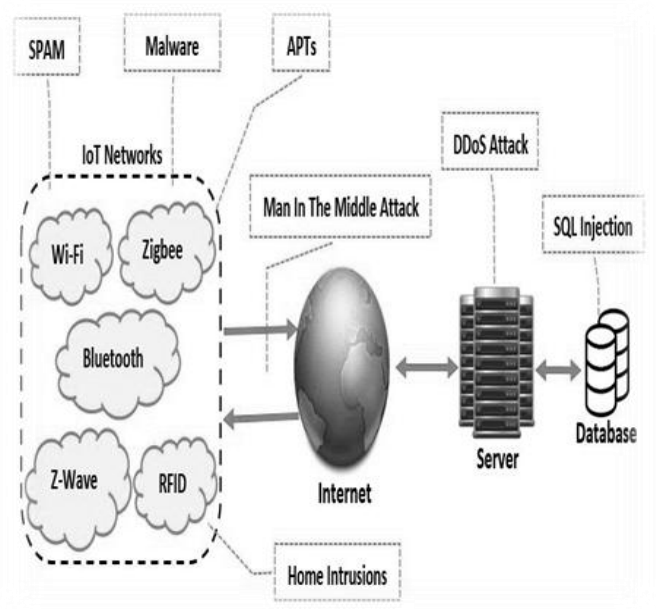

Fig. 2. Security threats in IoT

IV. SECURITY IMPLEMENTATIONS FOR IOT

IoT security threats are the major cybersecurity challenges in current IT ecosystem. In previous sections, we have discussed major IoT communication technologies and threats. Table 3 summarizes different IoT threats with their threat identity and security techniques used. A stronger security mechanism is needed to stop IoT devices from being compromised. Table 4 summarizes different network types with the security mechanism used. It's quite complex to implement stronger security to IoT devices due to their low computational capability and low memory. Cryptography with secure encryption and decryption keys can be used to determine device identity and could make a hurdle between user data and threats. SSL certificates can play a vital role to facilitate the device identification and authentication process. Authentication process must be enforced before any software or firmware update to save IoT devices from being compromised as a botnet (Thingbot). There should be a periodic examination of the IoT network by an anti-malware utility to detect any malicious activity.

Network devices like routers, printers, security cameras and other IoT devices having default passwords must be changed to a new one so that Mirai like botnets could not harm them. Spam filters can be used to stop the flood of spam. Spammers can flood the physical side of IoT devices to increase traffic for a specific page. As the problem of spamming explained in section 3, a possible solution to the spam problem is to digitally sign the 2d barcode and embedding the digital signature in QR code.

Advance Persistent Threats includes persistent behavior of attackers as they have patient until getting their target complete. Solutions to mitigate APTs may include, secure the entry point of the network, be careful to the outgoing traffic, install new security patches, and aware of any unusual activity being occurred in the network traffic.

Table III: IoT Threats and Their Security Technique

Threat Type	Threat Identity	Year	Security Technique
Advance Percistance Threats (APTs)	Monitors network activity and steal data with no damage.	2006	Beware of Trojans, suspicious emails, and malicious port scanning; install patches to prevent previously known vulnerabilities.
RFID Skimming	Stealing information from RFID cards.	2006	RFID blocking using RFID shield. Disable the RFID chip in your Credit Card.
Man in the Middle Attack	Intercepting and interrupting an interconnection between two separate network devices.	2003	Analyze the response time in the web traffic, authentication, use SSL/TLS Certificates for websites, PKI technology, WEP/WPA Encryption,
Botnet	DDoS attack	2001	Authentication, Encrypted device identity
Spam	Sends bulk messages	1994	Change passwords frequently, Web Application Firewall (WAF), DDoS mitigation system
Ransomware	Encrypts all data on the victim's computer.	1989	Data Backup, use Crypto locker software, disable RDP, and be careful when an email has a file with '.exe' extension.

Utilities like firewall, Intrusion Prevention System (IPS), Antivirus, botnet or command detection system and sandboxing should be used to ensure better security through these threats.

Table IV: IoT network security mechanisms for different network types [39]

Network Type	Security Mechanism
Zigbee	Link Layer encryption using 128bit AES, EAP, TLS.
BLE	Secure pairing
WiMAX	Sends UDP and TCP floods in both Ipv4 and Ipv6 protocols.
Wi-Fi	WEP, AES, TKIP, WPA, WPA2, and 802.1x.
6LoWPAN	Access control list, 802.15.4 link layer encryption.
NFC	Cryptographic methods and Hardware-based security (TDES, AES, RSA, ECC)
RFID	Cryptography such as Advanced Encryption Standard (AES)
LoRaWAN	AES-128 encryption, end-to-end security provided using application and network keys

The strongest possible way to save IoT from the man in the middle attack is a strong encryption system between IoT devices and communicating server of these devices. IoT devices communicate also with each other without the involvement of the server. So, encryption schemes should also be applied between IoT Devices because MITM attack is also possible between two communicating IoT devices. Another possible way to mitigate the MITM attack is by using an encrypted Virtual Private Network (VPN). This method ensures that everything comes in and goes out is encrypted and secured.

V. CONCLUSION AND FUTURE WORK

In this paper the authors reviewed and compared various existing networking technologies. Each networking technology has their own features. Authors have discussed about some prominent networking technology like Zigbee, RFID, WiMAX, Bluetooth, NFC 6LoWPAN, Wi-Fi, and LoRaWAN. The research has counter measure their scope in terms of frequency, data rate and range. The research concluded that Wi-Max has the highest frequency, data rate and network range, although Wi-Fi has also high-quality data rate and LoRaWAN has the second highest network range.

Further research has focused on authentication and access control protocols of IoT. Many researchers stated that identity of IoT devices must be secured and input-output traffic must be examined in real-time basis for any malicious activity. Devices must be protected from being compromised from malware. IoT devices need stronger security mechanisms for new emerging threats. Zigbee, LoWPAN, RFID, Bluetooth and other types of IoT networks are suffering from various types of threats like malwares, MITM attack, RFID skimming, APTs, and SPAM. Figure 3 represents the frequency comparison of different networking technologies, figure 4 provides approximate rate comparison of different networking technologies, and Figure 5 shows stream data rate comparison of different networking technologies.

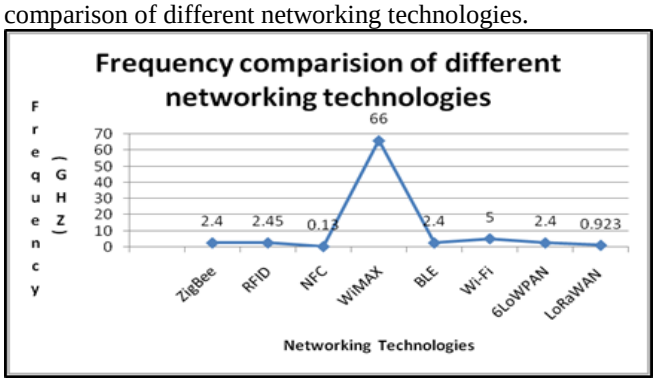

Fig.3. Frequency comparison of different networking technologies

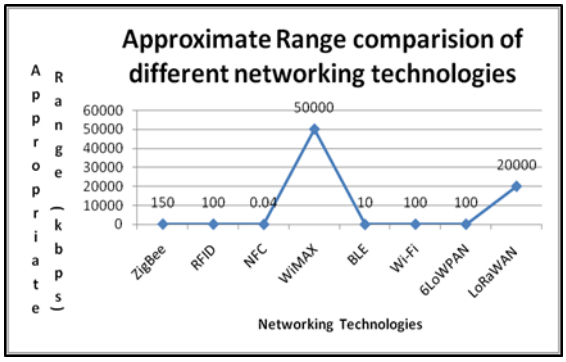

Fig.4. Approximate range comparison of different networking technologies

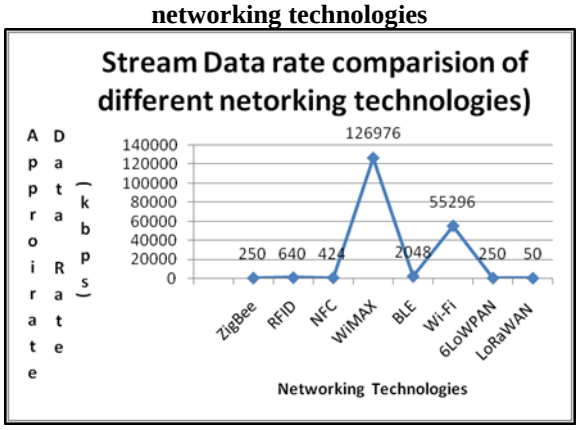

Fig.5. Stream data rate comparison of different networking technologies

The IoT framework is susceptible to attacks at each layer; hence there are many security challenges and requirements that need to be addressed. The paper illustrates the continuous attack of botnets on IoT network hence it is a biggest threat that must be included in future research on IoT security. IoT security-related challenges are getting the attention of researchers and inspire them to discover stronger security technique to mitigate these threats. Most of the IoT devices have low hardware configuration that is why the implementation of a stronger security mechanism is not possible on them. This weakness makes them vulnerable to security threats and needs further research to overcome this problem. The Internet of things reveals vulnerabilities exist in it and the requirement of research work to secure the communication between IoT device. There are several threats present which can cause damages to the IoT devices security and the world of computing has no full-proof plan or security technology to trace or eliminate these threats completely. In the end of the paper authors have presented some security mechanism to protect the networking technology.

REFERENCES

1. D. N. GUPTA, R. Kumar, and A. Kumar, "Efficient Encryption Techniques for Data Transmission Through the Internet of Things Devices," in IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks, 1st ed., V. Jain, O. Kaiwartya, N. Singh, and R. S. Rao, Eds. Pennsylvania, United States: IGI Global, 2020, pp. 203–228.
2. Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things." E-Business and E-Government (ICEE), 2011 International Conference on. IEEE, 2011.
3. Howell, J. (2017, October 24). Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says. Retrieved from IHS Markit: https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says.
4. Nordrum, A. (2016, August 18). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
5. Kushner, D. (2013, February 26). The Real Story of Stuxnet. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
6. Fruhlinger, J. (2018, March 9). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. Retrieved from CSO: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.
7. GOODIN, D. (2017, October 28). Assessing the threat, the Reaper botnet poses to the Internet—what we know now. Retrieved from Ars Technica: https://arstechnica.com/information-technology/2017/10/assessing-the-threat-the-reaper-botnet-poses-to-the-internet-what-we-know-now/.
8. Kolias, C., Kambourakis, G., Stavrou, A., &Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
9. Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.
10. Ergen, S. C. (2004). ZigBee/IEEE 802.15. 4 Summary. UC Berkeley, September, 10, 17.
11. Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. S. (2011). RFID technology principles, advantages, limitations & its applications. International Journal of Computer and Electrical Engineering, 3(1), 151.
12. Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011, April). Study on ZigBee technology. In 2011 3rd International Conference on Electronics Computer Technology (Vol. 6, pp. 297-301). IEEE.
13. Yeager, D. J., Sample, A. P., Smith, J. R., Powledge, P. S., & Mamishev, A. V. (2006, September). Sensor applications in RFID technology. In 2006 International Conference on Actual Problems of Electron Devices Engineering (pp. 449-452). IEEE.
14. Rahul, A., Krishnan, G., Krishnan, U. H., & Rao, S. (2015). Near Field Communication (NFC) Technology: A Survey. International Journal on Cybernetics & Informatics (IJCI), 4(2), 133-144.
15. Kabir, A. F., Khan, M., Hayat, R., Haque, A. A. M., & Mamun, M. S. I. (2012). WiMAX or Wi-Fi: The Best Suited Candidate Technology for Building Wireless Access Infrastructure. arXiv preprint arXiv:1208.3769.
16. Bensky, A. (2019). Short-range wireless communication. Newnes.
17. García-García, L., Jiménez, J. M., Abdullah, M. T. A., & Lloret, J. (2018). Wireless technologies for IoT in smart cities. Network Protocols and Algorithms, 10(1), 23-64.
18. Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). Emerging wireless technologies in the internet of things: a comparative study. arXiv preprint arXiv:1611.00861.
19. Al-Kashoash, H. A., & Kemp, A. H. (2016). Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, 13(4), 268-274.
20. Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 5(1), 1-7.
21. Hong, Y. G., Choi, Y. H., Youn, J. S., Kim, D. K., & Choi, J. H. (2015). Transmission of IPv6 packets over near field communication. draft-IETF-6lo-NFC-00.
22. Rahul, A., Gokul Krishnan, G., Unni Krishnan, H., & Rao, S. (2015). Near Field Communication (NFC) Technology: A Survey. International Journal on Cybernetics & Informatics (IJCI), 4(2), 133-144.
23. Iqbal, M. A., Olaleye, O. G., &Bayoumi, M. A. (2017). A review on the Internet of Things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology.
24. Papapanagiotou, I., Toumpakaris, D., Lee, J., &Devetsikiotis, M. (2009). A survey on next-generation mobile WiMAX networks: objectives, features and technical challenges. IEEE Communications Surveys & Tutorials, 11(4).

25. Narendra, P., Duquennoy, S., & Voigt, T. (2015, October). BLE and IEEE 802.15. 4 in the IoT: Evaluation and Interoperability Considerations. In International Internet of Things Summit (pp. 427-438). Springer, Cham.
26. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879.
27. Ech-Chaitami, T., Mrabet, R., &Berbia, H. (2011). Interoperability of LoWPANs Based on the IEEE802. 15.4 Standard through IPV6. International Journal of Computer Science Issues (IJCSI), 8(2), 315.
28. Al-Kashoash, H. A., & Kemp, A. H. (2016). Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, 13(4), 268-274.
29. Parmar, J. K., & Desai, A. (2016). IoT: Networking technologies and research challenges. International Journal of Computer Applications, 154(7), 1-6.
30. Bruce Zhou. (2017,February,9). Overview of networking technologies used to build IoT solutions. Retrieved from intelligent CIO: https://www.intelligenttechchannels.com/2017/02/09/overview-of-networking-technologies-used-to-build-iot-solutions/
31. Razzak, F. (2012). Spamming the Internet of Things: A Possibility and its probable Solution. Procedia computer science, 10, 658-665.
32. Hudson, B. (2014). Advanced Persistent Threats: Detection, Protection and Prevention. Sophos Ltd., US February.
33. D. N. Gupta and R. Kumar, "Lightweight Cryptography: an IoT Perspective," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 8, pp. 700–706, 2019.
34. D. N. Gupta and R. Kumar, "Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment," in INCET, 2020, pp. 1–6.
35. Cekerevac, Z., Dvorak, Z., Prigoda, L., &Cekerevac, P. (2017). INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS–SECURITY AND ECONOMIC RISKS. Journal of MEST, 5(2), 15-25.
36. Dange S., Chatterjee M. (2020) IoT Botnet: The Largest Threat to the IoT Network. In: Jain L., Tsihrintzis G., Balas V., Sharma D. (eds) Data Communication and Networks. Advances in Intelligent Systems and Computing, vol 1049. Springer, Singapore.
37. Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In Connectivity Frameworks for Smart Devices (pp. 23-41). Springer, Cham.
38. K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," 2017.
39. ConstantinosKolias, G. K. (2017). DDoS in the IoT: Mirai and Other Botnets. CYBERTRUST (published by the IEEE computer society), 40-44.

AUTHORS PROFILE

Ms. Purnima Gupta is working as Assistant Professor. She has qualified 4 times UGC NET and 2 times AWES PGT exam. She has been awarded 2 times by Eastern Central Railway Pt. Deen Dayal Upadhyay Division for developing their five projects (Pension Sanitization System, Central Receipt & Dispatch Management system, LAR, RMS and TROMGS). She has done MTech (CSE) and Master of Computer Applications. She is having a rich experience of teaching and research in the field of Computer Science & Engineering. She has published and presented a large number of research papers in International as well as national journals/conferences. Her area of interest is IOT, C/C++, Compiler Design, Artificial Intelligence, Data Structure, Network Security, DBMS (Oracle/PL-SQL), HTML, CSS, Java Script, Python (Pandas, NumPy, Matplotlib) etc.

Mr. Aswani Kumar Singh is working as CMS In-charge in Indian Railways posted at ECR/DDU. He has excellent software development skills and developed lots of utilities and web interfaces to overcome many issues at East Central Railways. He has also implemented web applications developed by Center for Railways Information System (CRIS) like Accounting Management and Information System (AIMS). He has been awarded four times by Indian Railways. He has done Master in Computer Application (MCA). His research papers have been published in reputed International as well as national journals/conferences. His core interest area is JAVA, Android, SQL, Scripting Languages, CSS e.t.c. With a PhD in Computer Science

Dr. Archana Sharma has over 24 years of experience spanning the IT industry and academia in different capacities and has published 33 research papers of which 12 are in international journals. She has also authored one text book for MCA and B.Tech. students. She has organized and attended various conferences, Faculty Development Programs, workshops and seminars during her stint in different organizations and has been credited with awards and commendations. Her major areas of competencies include Advanced Database, DBMS, Distributed systems, Operating systems and C++.