IoT Privacy and Security Challenges

Vardhan Adabala[1]

[1]Student, Department of Information technology, Joginpally BR Engineering College, Moinabad, Hyderabad, Telangana- 500075, India

Abstract - *Security and privacy are some of the most important challenges facing Internet of Things (IoT). Insufficient update of IoT devices, unawareness by the user, famous active device monitoring and inefficient and robust security policies and protocols are some of the major challenges facing IoT technologies. The paper highlights source of threats facing IoT and major privacy and security challenges facing IoT technologies.*

Key Words: Internet of Things, Security challenges, Privacy, Attacks, Vulnerabilities

1.INTRODUCTION

The Internet of Things (IoT) refer to concept where different types of devices and objects are connected over wired or wireless internet (Bugeja et al., 2016, August). Application of technology for various purposes such as business development, communication, education and transportation has made IoT very popular. The concept of hyperconnectivity was introduced by IoT implying that individuals and organizations can communicate with one another effortlessly from their local locations (Tawalbeh et al., 2020). Rapid growth of IoT has had several benefits to business and public organizations and in many ways business strategy and market research has been improved. Although there are many benefits associated with IoT from its rapid growth, there has been an increase in security and privacy challenges.

1.1 Source of security and privacy threats

Failure of regular updating software in IoT devices, not changing passwords and unconscious use of IoT devices make the devices highly prone to cyber security risks and access to IoT systems by malicious applications which may compromise sensitive data stored or processed by devices (Das, 2015, February). The above-named inappropriate practices among others raise the probability of cyber threats in IoT devices. IoT has been considered by several cyber security professionals as the most vulnerable point to cyber-attacks as a result of weak security policies and protocols.

Despite of security mechanisms that have been put in place to guard IoT objects from cyber-attacks, established security guidelines are not documented appropriately (Sandeep, 2018). In appropriate documentation hinder utilization of protective measures by end-users in averting cyber-attacks. Since the eve of 2008, there are several malwares intended to be injected in IoT devices that have been developed by hackers

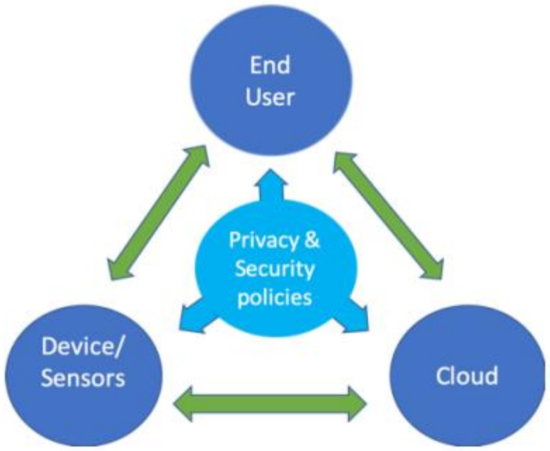

Fig -1: IoT generic model with privacy and security policies

Threat actors have developed several social engineering techniques aimed in provoking unsuspecting employees or person(s) into sharing sensitive information. Therefore, personal IoT devices and corporate workstations face high violations of privacy regularly due to different forms of attacks employed by threat actors (Bugeja et al., 2016, August). If cyber security experts and IoT device manufacturers accurately access cyber threats on IoT devices, there is a possibility of developing a protective mechanism that would efficiently prevent the attacks from facing these devices or neutralize the attacks.

1.2 IoT Privacy and Security Challenges

Despite of benefits that are associated with IoT devices, security and privacy forms main concerns for majority of cyber security specialists and researchers. Privacy and security of the devices forms two main predicaments that are considered by business and government organizations when acquiring IoT devices. Due to increasing number of cyber-attacks that have faced IoT devices, it is evident that there are several vulnerabilities that can be exploited by threat actors that are present in IoT devices. Although these vulnerabilities are a challenge to IoT technologies, ensuring security and privacy of the technologies form main concern. Continuous attacks on the devices by threat actors through different approaches are a compromise to privacy and security of devices that ought to be guaranteed by the technology.

2. Security

Diversity of IoT range from modern to traditional computers and computing objects making the technology more vulnerable to security challenges in several ways (Lin and Bergmann, 2016). First, majority of device sand objects in IoT are designed in a manner that they would be deployed in large scale, for instance sensors. Secondly, deployment of IoT usually contains sets of identical appliances possessing same features (Tawalbeh et al., 2020). Similarity in the features of appliances magnifies the probability of devices being vulnerable to security threats.

Table -1: Different types of IOT attacks

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tampering	Traffic Analysis Attacks	Virus and worms	Slide Chanel Attacks
RF Interference	RFID Spoofing		
Node Jamming	RFID Cloning	Spyware and Adware	Ciphertext Only Attack
Malicious Node Injection	RFID Unauthorized Access		
Physical Damage	Sinkhole Attack	Trojan Horse	Known Plaintext Attack
Social Engineering	Man in the Middle Attack		
Sleep Deprivation Attack	Denial of Service	Malicious Scripts	Chosen Plaintext Attack
	Routing Information Attacks		Man In the Middel Attack
Malicious Code Injection on the Node	Sybil Attack	Denial of Service	

IoT devices are interconnected to facilitate communication resulting to poor security in the devices. This interconnectivity is likely to affect resilience and security of internet globally. The behavior of interconnectivity and challenge of security are presented by vast application of IoT homogenous devices.

In the area of authentication, IoT face several vulnerabilities which act as main challenge in providing security in these devices (Tawalbeh et al., 2020). IoT devices apply limited authentication n protecting individual devices and organization systems from cyber-attacks such as denial of service among others. Natural multiplicity of IoT applications of gathering information from IoT environment make authentication if offering security of data vulnerable to cyber-attacks.

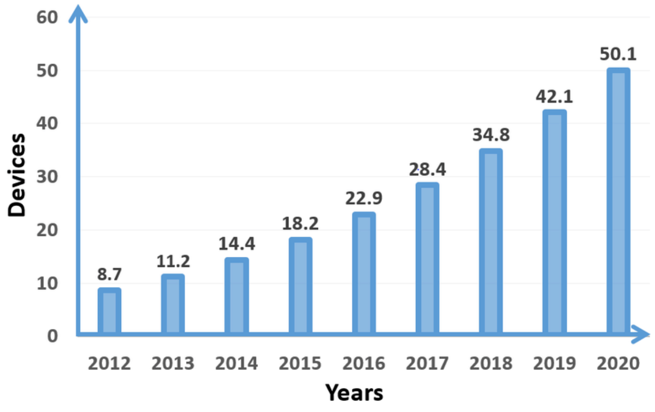

Chart -1: Number of connected IoT devices

Man in the middle attack which involve hijacking of communication by a third party with an aim of spoofing palpable nodes identities involved in exchange in the network is the most common attack experienced in IoT devices (Lin and Bergmann, 2016). In banking system, when man in the middle attack is initiated, bank servers identify the activity as a legitimate attack since the attacker do not require to be aware of victims' identity. The act compromises the security of the entire system.

3. Privacy

IoT technology can be considered to be useful based on its capability to guarantee privacy of data acquired, processed and stored in IoT devices together with respect to choices made by people (Sezer, 2018, September). Full adoption of IoT has been affected by privacy concerns which are influenced by constant attacks that are faced by IoT devices. It is important to understand that user privacy and rights of privacy respect basics in ensuring that self-assurance and confidence in IoT, devices connected, and several other services provided by the technology (Tawalbeh et al., 2020). Privacy becomes a major concern in IoT technologies due to omnipresent intelligence integrated artifacts where distribution of information and process of sampling in IoT may be carried in any place.

4. CONCLUSION

IoT devices are playing an important role in modern life. However, the devices comprise of several vulnerabilities and technicalities that hinder ensuring of privacy and security for the devices. Full adoption of IoT devices by organizations and individuals has been hindered due to security and privacy challenges possessed by the devices especially due to constant attacks that have faced the devices

REFERENCES

[1] Bugeja, J., Jacobsson, A. and Davidsson, P., 2016, August. On privacy and security challenges in smart connected homes. In 2016 European Intelligence and Security Informatics Conference (EISIC) (pp. 172-175). IEEE.

[2] Das, M.L., 2015, February. Privacy and security challenges in internet of things. In International Conference on Distributed Computing and Internet Technology (pp. 33-48). Springer, Cham.

[3] Lin, H. and Bergmann, N.W., 2016. IoT privacy and security challenges for smart home environments. Information, 7(3), p.44.

[4] Sandeep, C.H., 2018. Security Challenges and Issues of the IoT System. Indian Journal of Public Health Research & Development, 9(11).

[5] Sezer, S., 2018, September. T1C: IoT Security: -Threats, Security Challenges and IoT Security Research and Technology Trends. In 2018 31st IEEE International System-on-Chip Conference (SOCC) (pp. 1-2). IEEE.

[6] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M., 2020. IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), p.4102.