IJMRT: Volume (6), Issue 4, 2024
International Journal of Multidisciplinary Research Transactions
(*A Peer Reviewed Journal*)
www.ijmrt.in

ISSN (Print):2663-2381
ISSN(Online):2663-4007

Challenges and Threats to Security in The Internet of Things (IoT)

R. Sreenivasan

Assistant Professor, Department of Electrical and Electronics Engineering, CK College of Engineering & Technology, Tamil Nadu, India.

DoI: https://doi.org/10.5281/zenodo.11128875

Abstract

Vulnerability of wireless communication networks to security threats is well-documented, especially considering their widespread use in military, business, healthcare, retail, transportation, and various other sectors. These networks encompass wired, cellular, and adhoc systems, and specific attention has been directed towards WSAN and Actuator networks, garnering substantial interest in both societal and industrial realms. Recently there has been a notable research emphasis on internet of things widely regarded as internet future, poised to transform lifestyles, norms and business frameworks. Anticipated to experience exponential growth in diverse applications, the IoT facilitates the seamless connection and information exchange among various “n” number of devices, individuals, and services. However, the surge in internet of things device usage has made IoT networks susceptible to attacks like security attacks.

Keywords: Threats in Internet of Things, Challenges.

1. Introduction

The internet of things has attracted considerable attention in recent years, originally conceived by Kevin Ashton. These interconnected devices, encompassing a wide array such as Mobile phones, desktop systems and laptop rely on low-cost sensors and usage of wireless systems which are used to exchange valuable information within a centralized system. This information is processed centrally before being directed to its intended destinations. In today's fast-evolving

technological landscape, usage of daily schedule increasingly revolves around a virtual space facilitated by various technologies involved for the purpose of communication [1]. People conduct work, shopping, socializing, while residing in the physical world. However, the full replacement of activities of human to a complete automation poses a threat to the boundaries within this virtual space that hampers further internet development for improved services. IoT has bridged this gap by effectively integrating the virtual space with the world on a unified platform. The primary objectives of IoT include creating smart environments and deploying autonomous devices in areas such as intelligent living and good & prosperous health. [2]. Presently, the adoption rate of IoT devices is soaring, with an increasing number of devices interconnected via the internet. Estimates suggest that by 2020, there will be approximately 30 billion devices will be connected, facilitating around 200 million connections and generating revenue approximately 700 billion euros. In China approximately 9 billion devices are connected facilitating around 24 billion euros. The future internet of things is focused on business paradigms, fostering seamless communication between people and devices.

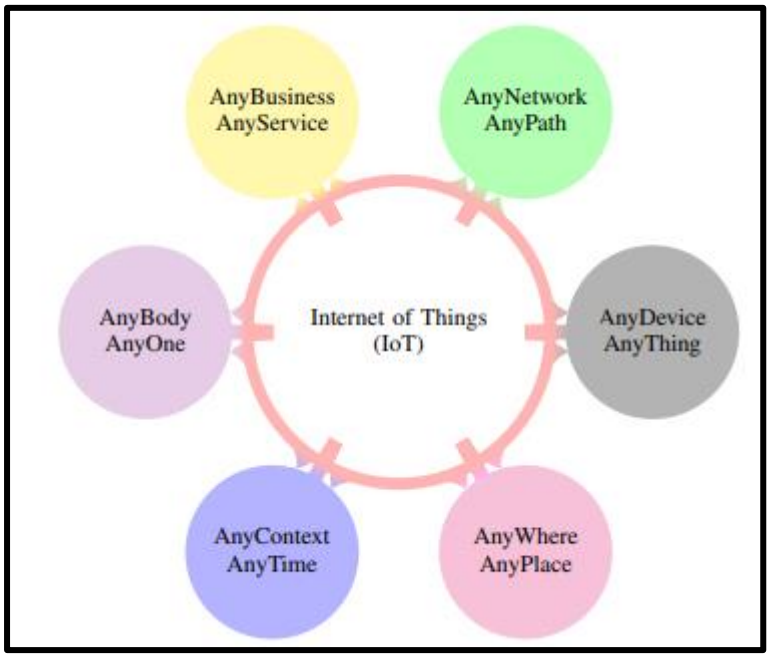

Figure.1. Various definitions of Internet of things

1.1. IoT in Industries

The emergence of internet of things has paved the way for the creation of substantial industrial systems and their applications. [6]. In an intelligent internet of things linked with transport system authorized personnel can actively monitor a vehicle's current location and movements while also predicting its future whereabouts and assessing road traffic conditions. Since internet of things primarily associated with uniquely identifying objects via RFID technology. However, in recent times, researchers have broadened the IoT concept to encompass various sensors, actuators, GPS etc... The widespread acceptance and utilization of the new technologies based on internet of things hinge significantly on data privacy and information security. The IoT enables the connection, tracking, and monitoring of numerous entities, leading to the automatic collection of valuable data. In the IoT landscape, safeguarding privacy presents a notably more pressing challenge compared to traditional networks primarily substantially reduced risk of attacks in IoT systems.

1.2. IoT in Personal Medical Devices

IoT devices are extensively utilized within healthcare systems to monitor and evaluate patients [7]. The equipment’s used for medical devices are employed to track a patient's medical status, can either be implanted inside the patient's body or attached externally. These compact electronic devices have gained significant popularity and are projected to reach a value nearly 18 billion dollars by 2019[8]. They rely on wireless interfaces to communicate with a base station, enabling the retrieval of device status, medical reports, parameter adjustments, and status updates. However, the use of wireless interfaces presents considerable privacy risks for patients. These interfaces are susceptible to cyber-attacks, posing threats to patient security, privacy, and overall safety. In healthcare scenarios, ensuring network security is paramount to safeguard patient privacy from hostile attacks. When attackers target mobile devices, they

typically have predefined objectives, which may include information theft, exploiting device resources, or disrupting applications responsible for monitoring a patient's condition.

1.3. IoT in Smart Home

Within a smart home world, the devices are interconnected to the internet. With the growing number of devices in this setting, the likelihood of malicious attacks also escalates. However, when smart home devices operate independently, the potential for malicious attacks decreases. Currently, smart home devices are accessible via the internet from anywhere and at any time, heightening the vulnerability to potential attacks.

In this setup, numerous devices interconnect and intelligently share information via a home network. Consequently, a home gateway regulates the information flow among the smart devices connected to the external network.

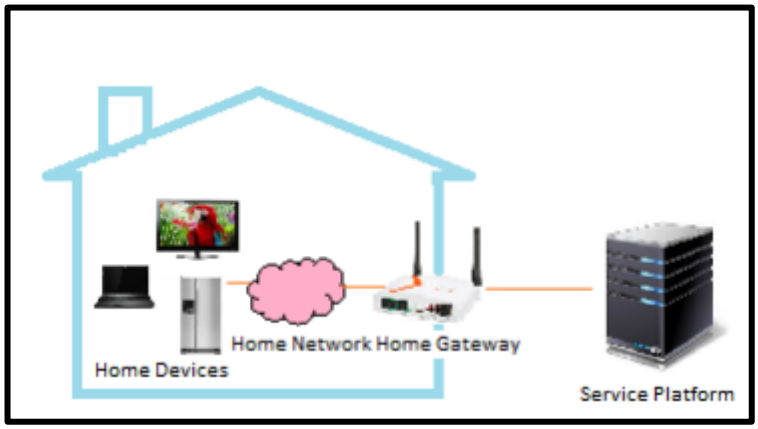

Figure. 2. Components of Smart home within Internet of things

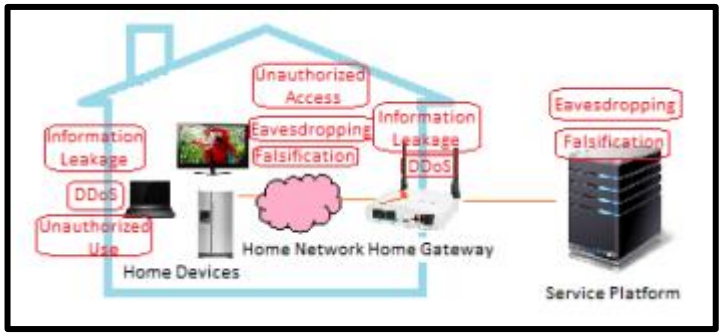

Figure.3. Various threats within IoT.

2. IoT Security, Privacy, Threats, and Challenges

A majority of these security threats involve information leaks and service disruptions. In the realm of IoT, these security concerns directly impact physical security risks. With diverse devices and platforms, each having unique credentials, individual systems require specific security measures based on their characteristics.

User privacy can also be uncovered from different routes. Some security threats in the IoT are as follows:

1. **End to End Protection:** This involves gathering data from interconnected devices and promptly transmitting it to other devices, necessitating a framework that ensures data protection, confidentiality, and management of information privacy throughout the entire data life cycle.
2. **Planning:** The connectivity and interaction between IoT devices fluctuate depending on circumstances. Hence, these devices need to consistently uphold a certain security standard. For instance, when local devices and sensors within a home-based network securely communicate with each other, their interactions with external devices should adhere to the same security protocols.

3. Security Threats in Smart Home

Smart home services are vulnerable to cyber-attacks due to the lack of consideration for security parameters during early stages of development by many service providers. This negligence can lead to various security threats, including.

Figure.4. Ex-Tree pass attack involving hacking a door lock

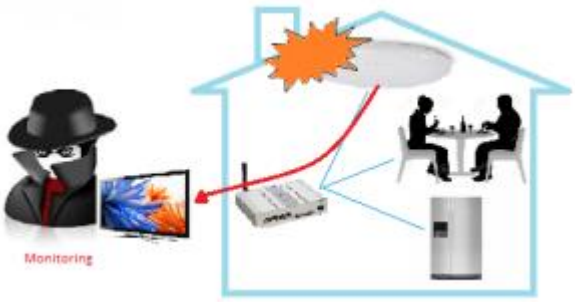

Figure.5. Ex-Information monitoring

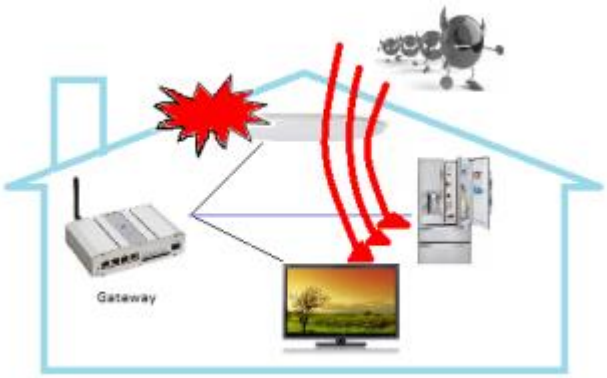

Figure.6. DDoS Attack

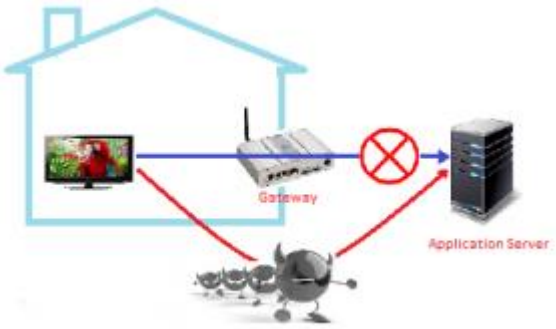

Figure.7. Ex- Falsification

4. IOT Challenges

Security remains the foremost challenge in IoT. The data generated by IoT applications encompasses industrial, enterprise, consumer, and personal information, all of which require protection from theft and manipulation. For instance, these applications might store sensitive health records of patients or transaction information from a retail store. Despite enhancing device communication, IoT encounters issues concerning scalability, availability, and response times. Ensuring secure data transmission over the internet is a significant security concern. Additionally, when data crosses international borders, government regulations.

5. Conclusion

The primary focus is to underscore the significant security issues prevalent in IoT, particularly highlighting the various attacks and their corresponding preventive measures. The absence of robust security mechanisms in IoT devices renders many susceptible, often without the user's awareness of their devices being compromised. It categorizes twelve distinct attack types into various levels—low, medium, high, and elaborates on their characteristics, along with proposed solutions to combat these attacks. It is imperative to implement robust security measures in both IoT devices and communication networks. Additionally, safeguarding against intruders or security threats involves steering clear of default passwords for devices and thoroughly acquainting oneself with a device's security requirements before initial usage.

REFERENCES

[1]. J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014.

[2]. M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[3]. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[4]. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.

[5]. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.

[6]. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233– 2243, 2014.
[7]. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
[8]. A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
[9]. S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in iot environment," in Computer Science and its Applications. Springer, 2015, pp. 691–696.
[10]. R. H. Weber, "Internet of things–new security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.
[11]. S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," in International Conference on Network Security and Applications. Springer, 2010, pp. 420–429.