IoT Security and Privacy

Nikitha Merilena Jonnada

PhD in Information Technology (Information Security Emphasis),
University of the Cumberlands, Williamsburg, Kentucky, USA

Abstract

In this paper, the author discusses the importance of IoT, its security measures, and device protection. IoT devices have become a trend as they allow users to easily use and understand the devices. IoT has become a widely used technique within many industries like banking, agriculture, health care, and others. It made the user's experience easy. IoT without AI has been a good investment for many users as its connectivity helps them use multiple devices from a single device and sometimes with a single click.

Keywords

Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Security, Hacking, Risks.

1. Introduction

The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects embedded with sensors, software, and network connectivity, allowing them to collect and share data [1]. IoT can connect many devices to communicate with each other. Smart devices have become a trend lately, and many people have bought and invested in them. The IoT makes the users experience hassle-free inter-device connectivity. IoT makes it easy to convert a home or an office into a brilliant place. Google devices are one of the best examples of an innovative experience. Many Google devices like speakers, doorbells, Google hubs, and other devices can all be connected to each other to help the users access all the users in one place, like the Google Home application [2].

2. Research Questions

- Will IoT help in mitigating risks?
- Will IoT still be the future with growing Artificial Intelligence (AI)?

3. Key Components of IoT

3.1. IoT Devices

3.1.1. Smartphones and Tablets

Though smartphones and tablets are not considered IoT devices, they are still smart devices that act similarly to IoT devices. They provide the users with a smooth use of the devices. These smart devices help users stay connected to many other smart devices [3].

David C. Wyld et al. (Eds): NLCAI, AIFU, CCSEA, BIoT, SEA, SIPRO, BDML, CLOUD – 2025
pp. 167-170, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151013

3.1.2. Wearables

These smart devices help users track their health and fitness goals and connect to other devices like smartphones [3].

3.1.3. Smart Home Devices

Many devices like thermostats, locks, cameras, lights, and digital video devices can be connected and accessed by the users with a voice command [3].

3.1.4. Smart Appliances

Many household appliances like washing machines, refrigerators, coffee makers, and others can be easily controlled through innovative applications by the users [3].

3.1.5. Vehicles

Many cars get connected to the smart devices. Many vehicles now have features like self-driving that help users with an effortless driving experience [3].

3.2. IoT Sensors

Sensors help detect changes in the temperature and environment around us. This data gets collected and assessed to generate results. Many sensors help us analyze, like temperature sensors, humidity sensors, motion Sensors, Pressure Sensors, Proximity Sensors, Light Sensors, Gas Sensors, Sound Sensors, and accelerometers [4].

3.3. Communication Networks and Protocols

Many protocols and networks like Wi-Fi, Bluetooth, cellular 5G, and others are used to establish a connection between various devices. They help users transfer data, access devices remotely, and attend and conduct meetings remotely. This type of communication allows the remote workers to stay connected with the teams and finish the tasks on time [4].

3.4. IoT Gateways and Cloud Servers

A gateway is a bridge between the devices and the cloud. For the device to work with IoT standards, it needs a cloud server and a gateway that helps with the connection. Clouds are prone to attack as a large amount of data gets stored within them. This could attract many hackers as hackers target only the data. A stronger firewall is needed for the secure usage of IoT devices [4(Hassan, Qamar, Hasan, Aman, & Ahmed, 2020)].

4. IOT APPLICATIONS

IoT can be applied within many industries. It can also be applied to home automation. We can use smart speakers, smart thermostats, smart lights, cameras, washing machines, refrigerators, and smart locks in our homes. IoT can be used within the healthcare industry by using smart inhalers, smart insulin pumps, smart pacemakers, and wearable devices that help track the heartbeat rate, glucose levels, and blood pressure. IoT can also be used to make a city a smart city. This can be done by adding smart streetlights and sensors to manage traffic, monitor the environment, and manage waste. IoT can also be used in agriculture to sense soil moisture, temperature, and crop health, to set fertilization schedules, to track livestock, and to use drones to monitor crops.IoT can be used within banking, industries, supply chains, inventory management, retail, transportation, logistics, utility departments, environmental monitoring, and education [4].

5. Advantages of IoT

- IoT allows task automation.
- IoT provides enhanced efficiency.
- IoT supports better decision making.
- IoT provides enhanced security.
- IoT helps in cost saving.
- IoT helps with better customer experience.
- IoT supports remote monitoring and management.
- IoT supports sustainability [1].

6. Disadvantages of IoT

- IoT are vulnerable and prone to security risks.
- Privacy is a major concern with IoT devices.
- Data overload can happen with IoT devices as it uses large amounts of data.
- IoT is highly dependent on the internet.
- IoT devices are vulnerable to malware.
- IoT could cause an impact on employment.
- IoT could be complex.
- IoT consumes high energy [1].

7. Risks to be Considered with IoT

- Security vulnerabilities like cyberattacks, botnets, and lack of encryption.
- IoT devices are prone to data privacy risks.
- IoT devices mostly use weak authentication mechanisms and security standards.
- IoT devices might not be compatible with different protocols [5].

8. Security and Privacy Challenges

With the use of smart devices and technologies come risks and challenges. Whenever the data gets exposed, many hackers try to steal that data. Hackers tend to steal essential data, which could help them if they decide to sell or misuse it for their benefit. As IoT uses connectivity between various devices, the data between these devices gets exchanged when a connection gets established. Many IoT devices are designed to make user usage easy. This might lead to the devices having weak authentication and authorization security standards. Communication can also be unencrypted as it happens over a wireless network. Most of the time, many IoT devices do not get frequent software updates, leading to devices with weak firmware that could attract hackers to steal data from IoT devices [6].

9. Mitigating Risks within IoT

To mitigate the risks within the IoT devices, companies must add an extra layer of security to ensure safe and risk-free user usage. Regular software and security updates would help companies secure their user's data from getting stolen or hacked. By implementing many safety measures, IoT users can be protected from risks while using IoT devices [7].

10. FUTURE TRENDS

Artificial Intelligence (AI), Machine Learning (ML), 5G security, and edge computing are some of the future trends within IoT. AI could be the future of many industries, but IoT would still be a continuing trend within many devices as AI could become a costly implementation. As IoT has been successful, many devices will still be using IoT in the future [3].

11. CONCLUSION

IoT has made many industries introduce devices that make users' lives easier. These devices made the device connectivity easy. But every innovation comes with security issues and privacy concerns. Even with advancing AI and ML techniques and usage, IoT device software might only be updated to the standards of AI, as this would be an easier shift than replacing the entire software. Users of IoT devices would prefer to use their existing devices, making it much more complicated when the software gets replaced. The IoT devices must enhance their security measures to keep users using their devices even with existing AI-supporting devices. IoT devices need enhanced security measures as their security standards are currently weak. With enhanced security standards, IoT would still exist for years [3].

REFERENCES

[1] What is the Internet of Things (IoT)? (2023).

[2] Mouha, R. A. (2021). Internet of Things (IoT).

[3] Khanh, Q. V., Hoai, N. V., Manh, L. D., Le, A. N., & Jeon, G. (2022). Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges.

[4] Hassan, R., Qamar, F., Hasan, M. K., Aman, A. H., & Ahmed, A. S. (2020). Internet of Things and Its Applications: A Comprehensive Survey.

[5] Griffioen, P., & Sinopoli, B. (2021). Assessing Risks and Modeling Threats in the Internet of Things.

[6] Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N.-A. (2020). Security Considerations for Internet of Things: A Survey.

[7] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions.

AUTHOR

The author earned her PhD in Information Technology (Information Security Emphasis) from the University of the Cumberlands in 2024. The author is continuing her research within the security emphasis and is also expanding her research into artificial intelligence and machine learning to develop security measures using the latest technology standards.