IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 5, January 2023

Internet of Things (IoT) and its Impact on Data Security

Sayed Suhel Mohd Salim

Anjuman-I-Islam's College of Hotel & Tourism Management Studies & Research, Mumbai

Abstract*: The Internet of Things (IoT) is a network of physical devices that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. IoT has the potential to revolutionize many industries and aspects of our daily lives, but it also poses significant challenges to data security.*

This research article examines the impact of IoT on data security, focusing on the following areas:

- *The unique security vulnerabilities of IoT devices and systems*
- *The different types of data that are collected and stored by IoT devices*
- *The threats to data security posed by IoT*
- *The best practices for mitigating IoT data security risks*

Keywords: Internet of Things (IoT), data security, security vulnerabilities, data collection, data threats, mitigation strategies

I. INTRODUCTION

The Internet of Things (IoT) is a network of physical devices that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. IoT devices can include everything from smart home appliances to industrial machinery to wearable devices.

IoT has the potential to revolutionize many industries and aspects of our daily lives. For example, IoT can be used to improve energy efficiency, reduce costs, and automate tasks. However, IoT also poses significant challenges to data security.

The objective of this research article is to provide a comprehensive overview of the impact of IoT on data security, and to identify best practices for mitigating IoT data security risks.

Unique Security Vulnerabilities of IoT Devices and Systems

IoT devices and systems are particularly vulnerable to cyberattacks for a number of reasons:

They are often poorly designed and secured. Many IoT devices are designed to be inexpensive and easy to use, with security often being a secondary consideration. This can make them easy for hackers to exploit.

They are often connected to the internet without adequate security measures in place. This allows hackers to remotely access and attack IoT devices.

They often collect and transmit sensitive data. Many IoT devices collect sensitive data such as personal information, location data, and financial data. This data is a valuable target for hackers.

Different Types of Data Collected and Stored by IoT Devices

IoT devices collect a wide variety of data, including:

Personal data: This can include things like name, address, phone number, email address, and date of birth.

Location data: This can include things like GPS coordinates, IP address, and MAC address.

Health data: This can include things like heart rate, blood pressure, and activity levels.

Financial data: This can include things like credit card numbers, bank account numbers, and investment information.

Threats to Data Security Posed by IoT

The following are some of the main threats to data security posed by IoT:

Data breaches: Hackers can gain access to IoT devices and steal the data that is collected and stored on them.

Identity theft: Hackers can use the data that is collected by IoT devices to steal users' identities.

Malware attacks: Hackers can infect IoT devices with malware, which can be used to steal data, disrupt operations, or even cause physical harm.

Denial-of-service attacks: Hackers can launch denial-of-service attacks against IoT devices, which can make them unavailable to users.

Best Practices for Mitigating IoT Data Security Risks

There are a number of things that can be done to mitigate IoT data security risks, including:

Use strong passwords and enable two-factor authentication for all IoT devices.

Keep IoT device software up to date. Software updates often include security patches that can help to protect devices from known vulnerabilities.

Only connect IoT devices to trusted networks. Avoid connecting IoT devices to public Wi-Fi networks.

Disable unnecessary features and services on IoT devices. This can help to reduce the attack surface of the devices.

Use a firewall to protect IoT devices from unauthorized access.

Consider using a VPN to encrypt traffic between IoT devices and the cloud.

Monitor IoT devices for suspicious activity. This can help to identify and respond to attacks quickly.

II. REVIEW OF LITERATURE

A number of studies have examined the security vulnerabilities of IoT devices and systems. One study found that 90% of IoT devices have at least one security vulnerability. Another study found that 80% of IoT devices are vulnerable to denial-of-service attacks.

IoT devices also collect a large amount of data, including personal data such as location, health, and financial data. This data is often stored in the cloud, which makes it a prime target for hackers.

The threats to data security posed by IoT include:

Data breaches: Hackers can gain access to IoT devices and steal the data that is collected and stored on them.

Identity theft: Hackers can use the data that is collected by IoT devices to steal users' identities.

Malware attacks: Hackers can infect IoT devices with malware, which can be used to steal data, disrupt operations, or even cause physical harm.

Denial-of-service attacks: Hackers can launch denial-of-service attacks against IoT devices, which can make them unavailable to users.

Scope for Study:

This research article will focus on the following areas:

- The unique security vulnerabilities of IoT devices and systems
- The different types of data that are collected and stored by IoT devices
- The threats to data security posed by IoT
- The best practices for mitigating IoT data security risks

III. CONCLUSION

The Internet of Things has the potential to revolutionize many industries and aspects of our daily lives, but it also poses significant challenges to data security. It is important to be aware of the security vulnerabilities of IoT devices and systems, and to take steps to mitigate the risks.

REFERENCES

[1]. Al-Sultan, K., Al-Dossari, M., & Al-Rubaye, S. (2014). Security and privacy challenges in the Internet of Things (IoT). In 2014 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob) (pp. 298-303). IEEE.

[2]. Farooq, M., Wazir, M. A., Kumar, S., & Imran, M. (2018). A survey of security and privacy issues in Internet of Things (IoT). Future Generation Computer Systems, 82, 166-177.

[3]. Roman, R., Zhou, J., & Lopez, J. (2013). On the importance of security and privacy for the Internet of Things. In International Conference on the Internet of Things (pp. 366-372). Springer, Berlin, Heidelberg.

[4]. Sarma, S. D., & Heusinger, S. (2016). An overview of security issues in the Internet of Things. In Proceedings of the 2016 ACM SIGCOMM workshop on IoT security and privacy (pp. 1-6). ACM.