OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Short Communication

Security Assessment of Data Sharing Scheme for Analyzing usage of Datasets over the Internet of Things

Hashim Karim*

Department of Automation and Information Engineering, Deakin University, Geelong, Australia

DESCRIPTION

Internet of Things (IoT) security secures cloud-connected devices such as home automation, SCADA machines, security cameras, and other technologies that are directly connected to the cloud. IoT technology differs from mobile device technology (such as smartphones and tablets) due to the automatic cloud connectivity of gadgets. IoT security is all about protecting traditionally poorly designed devices for privacy and cybersecurity. Recent data breaches show that IoT security is a priority for most manufacturers and developers. Many organizations are deploying some form of IoT device. In other words, they are all exposed to some IoT security risks. However, certain organizations are particularly vulnerable to attacks and should pay particular attention to IoT security best practices. Unfortunately, many IoT devices remain insecure for the simplest of reasons.

In California, Japan, and the UK, a significant number of devices are left with default settings, requiring the default password to be changed when the device is powered on. The IoT in the workplace is one of the most advanced ways of increasing security an enterprise can implement. IoT successfully helps companies around the world to improve working conditions, collect data, streamline operations, and increase productivity [1].

IoT devices do not fully protect workers in high-risk industries. Instead, it helps administrators deal with a multitude of preventable threats. IoT technology enables companies to monitor the environmental conditions and physical health of employees, limit employee risks and exposures, and prevent accidents. An IoT device is anything that connects to the cloud and collects data.

This includes locks, garage door openers, temperature monitors (such as Google Nest), refrigerators, security cameras, stoves, TVs, or any other device that connects to the cloud. Many modern warehouse machines are connected to the cloud [2]. Please note that these devices are not considered mobile devices with standard operating systems and proprietary cyber security standards. IoT devices use an operating system, typically Linux, which is a full software modification.

As the number of connected devices continues to grow, organizations find it increasingly difficult to protect them and keep threats at bay. IoT devices are full of vulnerabilities and vulnerable to security breaches [3]. These are attractive targets for cybercriminals. Whether an organization is just beginning to adopt IoT or looking to expand an established IoT network, they all face similar challenges when it comes to managing, monitoring, and securing connected IoT environments. To ensure the security of IoT devices, enterprises should keep several things in mind [4]. Security-by-design is an approach to software and hardware development in which security is built in from the beginning, rather than being added on after hackers attack. As technology companies continue to produce a wide variety of consumer and enterprise IoT objects, the need for security by design becomes critical. By protecting, identifying, and monitoring risks, IoT security protects Internet devices and the networks they connect from threats and breaches while remediating vulnerabilities in a wide variety of devices that can pose security risks to organizations [5].

Most things in IoT are connected wirelessly. In fact, today there are many technologies for connecting devices wirelessly, some belong to Personal Area Networks (PAN), and some belong to Wireless Local Area Networks (WLAN) and Wide Area Networks (WAN). There are two aspects to consider when it comes to wireless network security. First and foremost, it is important to protect the data in transit using encryption mechanisms. Otherwise, everyone has access to the data as the air is a shared medium. Unauthorized access to these devices could allow attackers to reconfigure the network or route traffic to undesirable destinations. Security and privacy are important aspects of IoT networks. With the prevalence of IoT devices in many fields, network security is becoming more and more important. Similarly, maintaining data integrity is essential, especially when IoT sensors are used in the medical field. This chapter has promoted and supported the need for IoT security and privacy by providing examples of past attacks against IoT networks. The number of IoT devices deployed in networks is growing at a staggering rate, with up to 1 million devices being connected per day. While IoT solutions open up exciting new ways

Correspondence to: Hashim Karim, Department of Automation and Information Engineering, Deakin University, Geelong, Australia, E-mail: haskarim@edu.au

Received: 05-Jan-2023, Manuscript No. JITSE-23-21891; **Editor assigned:** 09-Jan-2023, PreQC No. JITSE-23-21891 (PQ); **Reviewed:** 23-Jan-2023, QC No. JITSE-23-21891; **Revised:** 30-Jan-2023, Manuscript No. JITSE-23-21891 (R); **Published:** 06-Feb-2023, DOI: 10.35248/2165-7866.23.13.315

Citation: Karim H (2023) Security Assessment of Data Sharing Scheme for Analyzing usage of Datasets over the Internet of Things. J Inform Tech Softw Eng. 13:315.

to improve efficiency, flexibility, and productivity, they also introduce new risks to networks. IoT devices, often designed without security, have become a new threat vector that malicious actors can use to launch attacks [6]. IoT technologies also ensure long-term workplace safety by analyzing data and using it to develop occupational safety strategies for employees. For example, IoT tools can be integrated with HR and workforce solutions to create a factory worker's schedule to minimize exposure levels or ensure workers are accurately distributed across the 24-hour shift.

CONCLUSION

IoT manufacturers must take steps to improve the security of their devices, but many IoT security challenges require user interaction and training. Users are required to change default passwords when installing devices, but many are unaware of the dangers or simply prefer the convenience of using default passwords. Users must be trained to change default passwords, but manufacturers cannot enforce password changes.

REFERENCES

1. Yu J, Kang H, Bang H, Bae M. A study on autonomous cooperation between things in Web of things. Advanced information technology and sensor application. ASTL. 2013;26:1-6.
2. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst. 2013;29(7):1645-1660.
3. Perera C, Liu C, Jayawardena S, Chen M. A survey on Internet of things from industrial market perspective. IEEE J Mag. 2014;2:1660-1679.
4. Atzori L, Iera A, Morabito G. The internet of things: A survey. Comput Netw. 2010;54(15):2787-2805.
5. Dohr A, Modre-Opsrian R, Drobics M, Hayn D, Schreier G. The internet of things for ambient assisted living. In 7th international conference on new generations in information technology. 2010:804-809.
6. Hasan S, Curry E. Thingsonomy: Tackling variety in internet of things events. IEEE Inter Comput. 2015;19(2):10-18.