Security Measures in IoT Devices, Including Wireless Medical Devices:

Factors Influencing the Adoption of Effective Security Measures

Patricia G. Foley, American National University, USA*

Kathleen Hargiss, Touro University Worldwide, USA

Caroline Howard, Touro University Worldwide, USA

Anne Pesanvento, Touro University Worldwide, USA

ABSTRACT

The exponential growth in global adoption of the internet of things (IoT) has resulted in increasing challenges to secure devices against the rapid escalation of malicious users and external attacks. Security of IoT devices is particularly critical in the medical sector, where data breaches have become common in recent years at healthcare facilities, medical laboratories, and medical insurance companies. The phenomenological study focused on the experiences of users of IoT devices and the adoption of effective security measures in IoT devices, especially wireless medical devices. The results from this research study indicated that there was a need for policymakers to be more aware of the security issues that plague some IoT devices, including the need for training to detect potential breaches and cybersecurity aberrations, improved features for protection of devices, and better password security. The study concludes with recommendations for policymakers and device manufacturers.

KEYWORDS

Cyber-Attack, Cybersecurity, Internet of Things, IoT, Medical Internet of Things, Medical IoT, Network, Personally Identifiable Information (PII), Smart Devices, Wireless Medical Devices

INTRODUCTION

The global exponential growth in the adoption of the Internet of Things (IoT) has resulted in increasing security challenges to protect devices against the rapid escalation of malicious users and external attacks. IoT devices are widely used in a range of applications in the healthcare, facility management, transportation, and other industry sectors (Boeckl, Fagan, Fisher, Lefkowitz, Megas, Nadeau, O’Rourke, Piccarreta, & Scarfone, 2019). IoT devices can function as essentially small computer to control and home electronics and appliances (Ensenat, 2018). IoT devices are becoming increasingly popular, and it is estimated that approximately 31 billon devices are connected currently, and 75 billion are expected to be connected by 2025 (Sagay & Jahankhani, 2020). IoT cyberattacks

DOI: 10.4018/IJCPS.2021010102

*Corresponding Author

have major impacts on a wide variety of stakeholders due to the interconnectivity and ubiquitous use of IoT in a wide variety of applications (Schiller, Aidoo, Fuhrer, Stahl, Ziörjen, & Stiller, 2022).

Security of IoT devices is particularly critical in the medical sector, where data breaches have become common in recent years at healthcare facilities, medical laboratories, and medical insurance companies. IoT devices, which include cardiac defibrillators, pacemakers, and other wireless implanted medical devices, were designed and equipped with wireless technology to make it easier for medical personnel to monitor and treat individual patient's health problems without the need for more invasive and costly procedures (Allen, 2019). Unfortunately, the wireless technology made it easy for malicious individuals to compromise patient safety and privacy (Allen, 2019).

Governmental agencies are increasing their focus on patient privacy and security to protect against disclosure of a patient's personal information, unauthorized reprogramming of medical devices, and malicious security (Allen, 2019). The IoT Cybersecurity Improvement Act of 2020 directed the National Institute of Standards and Technology (NIST) to take the steps necessary to increase the cybersecurity of IoT (Dover, 2021). To comply, NIST published a special publication, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements, which can be used by both government agencies and non-governmental organizations (Dover, 2021; Megas, Fagan, Lemire, 2021).

Vulnerabilities found in IoT devices, especially implanted wireless medical devices, have caused the medical industry to attempt to implement modifications (Allen, 2019). In March 2021, President Biden issued an Executive Order on Improving the Nation's Cybersecurity, which included a list of components to be used by manufacturers and developers building software applications to ensure MIoT security (Dover, 2021). Due to the limited storage and battery life of wireless implanted devices, securing and protecting implanted devices can be especially difficult (Camera, Peris-Lopez & Tapiador, 2015). Solutions to the security issues with these devices must consider the safety and wellbeing of the patient and the security level achievable with the battery life of these devices (Camera et al., 2015).

The study reported in this article was designed to increase understanding of the security issues with IoT devices and possible solutions. The research explored the security risks and factors that influence the adoption of effective security measures in IoT devices, including wireless medical devices. The article begins with a discussion of a definition, relevant history of IoT and background of IoT medical devices. Next, it describes a phenomenological study focused on the experiences of users of IoT devices and the adoption of effective security measures in IoT devices, especially wireless medical devices. The article presents methodology, and results of the study. The article concludes with areas for future research.

BACKGROUND

IoT consists of interconnected and highly diversified networked objects and networks that adhere to several different communication patterns, such as human-to-human (H2T), thing-to-thing (T2T), or thing-to-things (T2Ts) (Garcia-Morchon, Kumar, & Sethi, 2019). The term "IoT" was first utilized in 1999 by the Auto-IT center, which had visualized a society in which each physical object has a radio-frequency identification (RFID) tag accompanied by an identifier that is globally unique (Fleisch, 2010). Over time, the definition of the IoT has grown and now includes a large assortment of objects, protocols, and technologies (Alieyan, Almomani,, Abdullah, Almutairi, & Alauthman, 2021: Garcia-Morchon et al., 2019). The research community started to give a lot of attention to the design, security, and application of standard Internet technology and protocols of the IoT (Garcia-Morchon et al., 2019). The objects or "things," associated with the IoT are computing devices that comprehend and respond to the environment they occupy (Garcia-Morchon et al., 2019). These objects or things are called smart devices or smart objects (Garcia-Morchon et al., 2019).

While the range of IoT is not precisely defined, it is substantial (Alieyan et al., 2021; Boeckl et al., 2019). Every industry has its types of IoT devices unique unto itself, such as medical equipment

Related Content