11-14-2021

Security of IoT Wearables

Salem Suhluli
Jazan University, salem.jazanu@gmail.com

Security of IoT Wearables

Abstract

Internet of things (IoT) has rapidly begun affecting several industries and services ranging from transport, home control, industrial automation, energy, and health. Most of these industries are transforming to add new network devices and pave the way for optimal solutions and enhanced services. When considered collectively, the features affect critical societal services such as home control and health management systems. This work will execute the research by the following procedure. To begin with, relevant stakeholders will be able to determine people's feelings and views on security and privacy about wearable IoT devices. The overall aim of this research extends two ways. First, assessing data security requirements for wearable devices as part of the fast-paced IoT technology is essential. Second, the study will determine user perceptions and concerns regarding the privacy and security features of wearable devices. This extended abstract will explore relevant literature reviews, then provide some insight into possible research gaps.

Keywords: IoT wearable, internet of things, privacy, information security.

Introduction

Ching and Singh (2016) define wearable technology (WT) as a device with computational capability which is attached to a human body as either a computer incorporated as an accessory or an object fitted to clothing. The IoT-enabled gadgets are integrated into various devices, for instance, cutlery, watches, wristbands, and jewellery. Wearable devices have particular features such as unrestrictive access and usability. A few other examples include location finding in cities and sensors in the home that track electricity usage and consumption, vehicle routes, and driver behaviors (Siboni, Shabtai, Tippenhauer, Lee, & Elovici, 2016). It would be appropriate to explore the security and privacy concerns that would influence end-user perspectives of wearable IoT enabled technologies.

Internet of things (IoT) has introduced new horizons to the computing world where all digitally enabled appliances are either equipped with or are connected to a smart device. IoT facilitates data sharing, synchronized access, data collection, and device communication over the internet (Caron, Bosua, Maynard, & Ahmad, 2016). It exemplifies one of the most pivotally disruptive techniques in this century: the emergence of global, web-based technical architecture - a new method being implemented quickly. The primary element that enables the IoT is by integrating multiple communicative and collaborative techniques that allow for complete data collection (Colom, Mora, Gil, &Signes-Pont, 2017). Researchers have projected that over 50 billion distinctively identifiable devices will have facilitated IoT usage without considering personal computers, mobile phones, and tablets (Andrea, Chrysostomou, &Hadjichristofi, 2015). IoT allows unbounded and pervasive connectivity of various devices through the internet at any time and in any place via sensors implanted in those devices. Mobility enables users to communicate with one another and incorporate the digital and physical worlds (Zheng, Apthorpe, Chetty, &Feamster, 2018). The proliferation of IoT devices has led to privacy and security challenges affecting the diffusion of the technology among consumers.

For developing IoT systems which are accepted and thereby adopted by an extensive range of users, thus, ensuring the security and privacy of users' personal data is important (Stergiou et al., 2018). From exploring the relevant literature review this paper will try and explain the impact of wearables security issues on users adoption. without addressing these concerns, ensuring the sustained growth of the sector will be very difficult. In addition, the findings of the present research are expected to have important practical implications in terms of how to devise security and privacy concerns and which dimensions of users' concerns to focus on.

Therefore, understanding security issues in IoT wearable devices will significantly help in understanding the adoption of IoT wearable devices from the perspective of security concerns is of great significance for the future of IoT-based devices.

Background of the Study

In consideration of the various layers of an IoT system model, security and privacy issues are noted in the literature. At the perception layer, these include eavesdropping, unauthorized access, and spoofing; Sybil attack, malicious injection of code, and denial of service (DoS) attack at the network layer; and sniffing attacks at the application layer (Farooq, Waseem, Khairi, &Mazhar, 2015). Other inherent challenges have included trust issues, authentication issues, detection of rogue nodes, detection of intruders, privacy breaches, and access control issues (Alrawais, Alhothaily, Hu, & Cheng, 2017). It is reported that several security solutions are established in IoT. It includes authentication, risk assessments, detecting intrusion, and routing security – most of them are specific only to identity establishment, authentication, and access control (Mahmoud, Yousuf, Aloul, &Zualkernan, 2015). This actuality lends attention to the many aspects of IoT security and privacy, especially in devices, which increase vulnerability to attacks. These flaws then become the source for varying user attitudes and perceptions towards the use of IoT wearable devices.

Certain established user perceptions are considered critical to addressing issues related to privacy and security in IoT. First, convenience and undisrupted connectedness are a top priority for most IoT and smart device users. Through these values, user sentiments and behaviors towards privacy are directed to external entities charged with the management, tracking, and regulation of IoT devices and data (Zheng, Apthorpe, Chetty, &Feamster, 2018). Second, outlooks regarding access to IoT device are dependent on user perceptions regarding the benefits and security of IoT devices. One way through which mobile and wearable device manufacturers make their privacy provisions known to the user is through privacy policies. Gluck et al. (2016) explored the outcome of reducing the length of a privacy policy as a way of promoting privacy awareness among users. They reported that while a shorter policy could adequately inform users about privacy practices, negative framing of these practices did not affect how users understood the procedure. Further, eliminating certain privacy practices from the policy reduced user knowledge of said practices, but this did not enhance the level of understanding of the remaining methods in the policy. To that end, user benefits addressed within comprehensive privacy statements play a role in anchoring user attitudes and raising their awareness on security and privacy needs in the IoT architecture.

People have never been so close to technical devices as they have been since the invention of the smartphone, and as wearables become more portable, smart devices will become even more common in human life. Wearables can work independently, yet they may be regarded obtrusive (Mani & Chouk, 2017). Users might experience a loss of independence due to using smart wearables (Rauschnabel et al., 2018). Thoughts of intrusiveness also lack of independence can guide to negative emotions also a reduction in inherent drive. A few citizens might happen to overly reliant on, or still enthusiastic to, smart wearables.

The frequent interchange of personal data within the wearable and the IoT hub, like important fitness signals, dose, and place, might lead to secrecy violations. Wearable IoT devices remain typically set to distribute mode, making them effortlessly discoverable by other network nodes. If adequate privacy policies are not implemented, unauthorized nodes may be able to steal personal data. In such modes, the IoT devices' inbuilt hardware safety technologies may not be sufficient to safeguard personal data from breaches.

Overall, discussions show that security concerns can be major inhibiting factors for the adoption of IoT technologies. However, there is a research gap in the literature regarding providing systematic literature review about users security concerns and how these concerns impact the adoption of wearable devices.

Conclusion

Security issues in IoT wearable devices remain significant issues because IoT wearable devices obtain personal data such as names and mobile numbers users. Users are usually concerned about the data collection of medical history or medical records due to the higher information sensitivity. Previous Studies show that security concerns negatively influence the willingness to provide personal information. Therefore, it is highly important to explore security issues and their impact on users adoption.

References

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE Symposium on Computers and Communication (ISCC) (pp. 180–187). IEEE. https://doi.org/10.1109/ISCC.2015.7405513

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer Law & Security Review, 32(1), 4–15. https://doi.org/10.1016/j.clsr.2015.12.001

Colom, J. F., Mora, H., Gil, D., & Signes-Pont, M. T. (2017). The collaborative building of behavioral models based on the internet of things. Computers & Electrical Engineering, 58, 385–396. https://doi.org/10.1016/j.compeleceng.2016.08.019

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A Critical Analysis of the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), 1–6. Retrieved from https://pdfs.semanticscholar.org/35f0/899d941e9e34ff1225448c21662d5ccca74c.pdf

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet of Things Journal, 5(4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). How short is too short? Implications of length and framing on the effectiveness of privacy notices. In the Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 321-340).

Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2017). IoT technologies for smart cities. IET Networks, 7(1), 1-13.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In 2015 IEEE World Congress on Services (pp. 21–28). IEEE. https://doi.org/10.1109/SERVICES.2015.12

Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2019). The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products. IEEE Security & Privacy, 17(2), 39-48.

Laurent, P. (2016, May). IoT Past and Present: The History of IoT, and Where It's Headed Today | Page 2.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges, and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336–341). IEEE. https://doi.org/10.1109/ICITST.2015.7412116

Mani, Z & Chouk, I. (2017), "Drivers of consumers' resistance to smartproducts", Journal of Marketing Management, vol. 33, no. 1–2, pp. 76–97

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. International Journal of Advanced Computer Science and Applications (IJACSA), 8(6), 383-388.

Rauschnabel, P. A, He, J & Ro, Y.K. (2018), "Antecedents to the adoptionof augmented reality smart glasses: A closer look at privacy risks" Journal of Business Research, vol. 92 , pp. 374–384.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered. Journal of Business Research, 57(9), 1000–1011. https://doi.org/10.1016/S0148-2963(02)00345-4

Siboni, S., Shabtai, A., Tippenhauer, N. O., Lee, J., & Elovici, Y. (2016). Advanced Security Testbed Framework for Wearable IoT Devices. ACM Transactions on Internet Technology, 16(4), 1–25. https://doi.org/10.1145/2981546

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. Security and Communication Networks, 2018, 1–9. https://doi.org/10.1155/2018/5978636

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1–20. https://doi.org/10.1145/3274469

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1–20. https://doi.org/10.1145/3274469