Privacy Concerns and Proposed Solutions with IoT in Wearable Technology

Hyacinth Abad
Old Dominion University

Privacy Concerns and Proposed Solutions with IoT in Wearable Technology

Hyacinth Abad

Old Dominion University

Murat Kuzlu

COVA CCI Cybersecurity Undergraduate Research Fall 2023

Introduction

As part of the technological evolution, the rise of the Internet of Things (IoT) and wearable technology has become an intrinsic part of people's daily lives. The year 2008 marked the birth of IoT, which has since proliferated exponentially especially in homes and businesses. As these interconnected digital and analog devices exchange data seamlessly, the realm of cybersecurity has taken center stage to safeguard against the numerous vulnerabilities that accompany this technological surge.

Simultaneously, wearable technology, encompassing devices like smartwatches, fitness trackers, and body-mounted sensors, has emerged as a transformative force. These devices, leveraging wireless connections and the Internet of Things (IoT), offer an array of benefits such as health data tracking and real-time communication. However, this innovation is not without its challenges, particularly in the domain of privacy. The convergence of these two technological realms prompts an examination of the interplay between IoT cybersecurity and the privacy concerns associated with wearable technology.

Section 1: IoT Cybersecurity

Subsection 1.1: Overview of IoT Growth and Cybersecurity Concerns

The beginning of IoT in 2008 intertwined the digital and physical worlds in unprecedented ways. Today, IoT fosters accessibility, integrity, availability, scalability, confidentiality, and interoperability. However, the rapid evolution and the multitude of attack surfaces inherent in IoT systems have given rise to formidable cybersecurity concerns (Kuzlu et al.).

As IoT permeates various aspects of daily life, cyber threats exploit vulnerabilities in hardware, software, networks, and applications (Taddeo et al.). The sheer diversity of cyberattacks, targeting different facets of IoT systems, necessitates a robust cybersecurity framework. Artificial Intelligence (AI) has emerged as a frontline defense, wielding complex algorithms to detect anomalies and strengthen networks against malicious activities (Kuzlu et al.). Nevertheless, the dual-edge nature of AI is apparent, as cyber-attackers utilize AI to breach defenses, complicating the cybersecurity landscape.

Subsection 1.2: AI in Cybersecurity for IoT

Within the realm of cybersecurity for IoT, Artificial Intelligence (AI) stands as a vanguard against the evolving tactics of cyber adversaries. The utilization of AI has become imperative in detecting and thwarting cyber threats (Taddeo et al.). As IoT systems generate vast amounts of data, AI algorithms excel in discerning patterns and anomalies that may signify potential attacks.

AI's role in cybersecurity extends beyond traditional methods, offering dynamic defense mechanisms that adapt to emerging threats. Decision trees, linear regression, machine learning, support vector machines, and neural networks identify and counteract threats in IoT environments (Kuzlu et al.). The proactive nature of AI in discerning unusual behavior provides a crucial layer of defense, aiming to mitigate the ever-present risk of cyber intrusions.

However, the paradox lies in the exploitation of AI, introducing adversarial AI into the cyber landscape (Kuzlu et al.). This strategic usage by cyber attackers amplifies the complexity of cybersecurity challenges, highlighting the constant need for innovation and adaptation in the face of evolving threats.

Section 2: Privacy Issues with wearable technology

Over the course of a few decades computer technology has proliferated in terms of numbers and applications in society. Computers and the Internet in general have led to recent innovations such as Artificial Intelligence, self-driving cars, and virtual reality. One of the more popular innovations is the creation of wearable technology (Thierer, 2014). Similar to Iphones, wearable technology such as smart watches, fitness trackers, and body-mounted sensors utilize wireless connection to assist in processing and communication capabilities (Ching & Singh, 2016). However, the extent of the capabilities of wearable technology varies from one device to another. The adoption of these modern devices is due to their numerous benefits such as gathering health data and information about the user's surroundings, tracking fitness performance, and sending and receiving calls and messages (Kapoor et al., 2020). Because of their popularity and easy accessibility with the public, there have also been concerns about privacy. People who utilize these devices for collecting personal information are at a risk for security breaches (Ching & Singh, 2016). Surprisingly, surrounding people can also have their data leaked through the use of pictures and audio data captured during social interactions (Michael et al., n.d.). Privacy issues brought on by the increased societal consumption of wearable technology can be resolved through the use of mechanisms that give users the option to collect information or not, public engagement and awareness made by users about privacy risks, and data encryption technologies and alerts that notify people of any wearable devices in their vicinity.

Subsection 2.1: Solutions to privacy concerns of wearable technology

One solution that addresses the privacy concerns of wearable technology is the implementation of mechanisms in the devices that give users the option to either collect or prevent the collection of data from the user and his surroundings (Kapoor et al., 2020). Wearable technology can connect or communicate to the Internet because of the concept called the Internet of Things (IOT) which gives physical objects such as wearable devices the capability to sense, process, and exchange data through the communication networks (Ching & Singh, 2016). Because of its direct connection to the Internet, the data collected by these devices are automatically stored in a database on the Internet which is worrisome for some people. In a survey about the concerns of wearable technology, 41.6% of participants chose privacy as the key issue with security trailing close behind (Perez & Zeadally, 2018). Features such as location services are common in smart watches or fitness trackers for GPS routes or training routes. According to (1), violations in privacy can occur during the transfer of these types of data from the device to smartphones via Bluetooth or Wi-Fi (Fafoutis et al., 2017). Most companies use connections that delay the transfer of data (such as Bluetooth Low Energy) rather than using one that ensures the most security (Ching & Singh, 2016). A user's regular local spots or a runner's trail path can be easily accessed and displayed online for the general public to see. A solution for these concerns involve giving users the option to prevent or allow data collection (Page, 2015). One approach called the Virtual Trip Line (VTL) approach allows data collection by these devices to occur in a specific area (Kapoor et al., 2020). Likewise, the virtual wall approach prohibits data collection in chosen areas by the user. These approaches utilize context to determine whether to access sensor data or not (Perez & Zeadally, 2018). More research is needed about these two approaches since total control is not owned by the user but by campaign organizers (Tang & Shi, 2021).

Subsection 2.2: Solution #2

Another solution that addresses the privacy concerns of these devices is to promote engagement and awareness of the privacy risks and complications that come with using wearable technology. It is common for many of these devices to have microphones and cameras to assist with their many functions (Kapoor et al., 2020). For instance, the Android Wear is a watch that utilizes a built-in microphone that allows users to Google search through voice dictations. Body worn cameras are also another form of wearable technology which are small enough to be worn inconspicuously (Perez & Zeadally, 2018). They are mostly used by organizations such as police departments to record evidence from different suspects. In these instances the visual and audio features in these devices serve to be very beneficial for the user (Ching & Singh, 2016). On the other hand, however, it is worrisome that both users and people might be recorded either visually, audibly, or both without their knowledge or permission. Voice activation on the Android Wear, for example, can be activated unbeknownst to the user. Likewise, cameras can be hacked and their content displayed on the Internet (Thierer, 2014). One suggestion for people is to increase their awareness about the devices' features by reading the user's manual and following the guidelines (Thierer, 2014). The user's manual includes useful instructions such as how to initiate device start up, connect it to Wi-Fi or Bluetooth, and most importantly how to set the security and privacy settings to the user's preferences (Michael et al., n.d.). Likewise, it is highly recommended that users change username and passwords, run regular software updates, and check where the device stores data (Tang & Shi, 2021).

Subsection 2.3: Solution #3

A third solution to the privacy issues of wearable devices is to utilize security alerts and data encryption technologies to warn and prevent data from being leaked. Unfortunately, people do not have to wear any of these devices for their privacy to be at risk. Bystanders is the term used to describe people who may or may not use this type of technology but are still at risk of getting their information leaked (Kapoor et al., 2020). Proposals have been made to include a notification system which would alert both users and bystanders if wearable devices are in their surroundings or if there is potential for data sharing such as voice recordings or photo sharing (Page, 2015). After being alerted, people can then take the appropriate actions to prevent information leaking such as turning off data collection in their devices, leaving the area, or letting the other person know about their privacy concerns (Przegalinska, 2018). One approach that is already widely popular is blurring out people's pictures on the Internet. Algorithms and machine learning allow people's faces and bodies to be blurred out based on their privacy settings on their profiles (Przegalinska, 2018). Another approach is through the use of data encryption technologies (Michael et al., n.d.). In this type of method, data is encoded into a different encryption and can only be accessed using the correct encryption key (Fafoutis et al., 2017). To the general public, the encrypted information can look like a jumbled mess thereby preventing the information from being shared. For example, at an organization level, government agencies use the Advanced Encryption Standard. Similar algorithms can also be used to hide personal information collected by wearable technology (Przegalinska, 2018).

Section 3: Conclusion

The intersection of wearable technology, IoT, and artificial intelligence (AI) presents a landscape rich with possibilities and challenges. Wearable devices have become indispensable tools, integrating into our lives to track health metrics, facilitate communication, and harness the power of AI-driven features. However, the multifaceted nature of these devices raises concerns related to cybersecurity and privacy.

As wearable technology evolves, incorporating advanced AI capabilities and deeper integration with IoT ecosystems, the need for robust security measures becomes essential. The ability of wearables to capture personal data, coupled with their growing connectivity to the broader Internet of Things, amplifies the potential risks. Users may inadvertently expose sensitive information, leading to privacy breaches and security vulnerabilities.

Addressing these challenges requires a multifaceted approach. Proposed solutions, such as the implementation of Virtual Line protocols and virtual walls, offer promising avenues to empower users with control over their data sharing preferences. Moreover, increasing awareness through comprehensive user manuals and leveraging security alerts alongside data encryption technologies can contribute to minimizing the unintentional sharing of information.

While these solutions represent significant strides in enhancing the security of wearable technology, the evolving landscape calls for continued research and innovation. Future efforts should focus on refining existing measures and exploring novel approaches to strike a balance between the benefits of wearable technology, AI, and IoT, and the imperative to safeguard individual privacy and data security. Embracing a proactive and collaborative mindset can lead the way for a safer and more resilient future in the era of interconnected devices.

References

Ching, Ke & Mahinderjit Singh, Manmeet (Mandy). (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Applications. 8. 19-30. 10.5121/ijnsa.2016.8302.

Fafoutis, Xenofon & Elsts, Atis & Piechocki, Robert & Craddock, I.J.. (2017). Experiences and Lessons Learned From Making IoT Sensing Platforms for Large-Scale Deployments. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2787418.

Kapoor, Vidhi & Singh, Rishabh & Reddy, Rishabh & Churi, Prathamesh. (2020). Privacy Issues in Wearable Technology: An Intrinsic Review. SSRN Electronic Journal. 10.2139/ssrn.3566918.

Kuzlu, M., Fair, C. & Guler, O. (2020). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discov Internet Things* **1**, 7 (2021). https://doi.org/10.1007/s43926-020-00001-4

Madden, M. (2015, May 20). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Przegalinska, Aleksandra. (2019). Wearable Technologies in Organizations: Privacy, Efficiency and Autonomy in Work. 10.1007/978-3-030-00907-6.

Perez, A. & and Zeadally,S. (2018). "Privacy Issues and Solutions for Consumer Wearables," in IT Professional, vol. 20, no. 4, pp. 46-56, Jul./Aug. 2018, doi: 10.1109/MITP.2017.265105905.

Tang F, Zhu D, Ma W, Yao Q, Li Q, Shi J. Differences Changes in Cerebellar Functional Connectivity Between Mild Cognitive Impairment and Alzheimer's Disease: A Seed-Based Approach. Front Neurol. 2021 Jun 17;12:645171. doi: 10.3389/fneur.2021.645171. PMID: 34220669; PMCID: PMC8248670.

Taddeo, M., Floridi, L., & McCutcheon, T. (n.d.). *Trusting artificial intelligence in cybersecurity is a ... - philarchive*. philarchive.org. https://philarchive.org/archive/TADTAI-2

Thierer, A. (n.d.). The internet of things and wearable technology - bja.ojp.gov. https://bja.ojp.gov/sites/g/files/xyckuh186/files/bwc/pdfs/Thierer-Wearable-Tech.pdf