Connecting the System to Enhance the Practitioner and Consumer Experience in Healthcare
E. Cummings et al. (Eds.)

doi:10.3233/978-1-61499-890-7-8

Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review

Sami ALKHATIB[a,1] , Jenny WAYCOTT[a], George BUCHANAN[a] and Rachelle BOSUA[a]
[a] *Computing and Information Systems, The University of Melbourne*

Abstract. The rapid increase in the number of older adults in developed countries has raised concerns about their well-being and increasing need for healthcare. New technologies, including Internet of Things, are being used to monitor older adults' health and activities, thus enabling them to live safely and independently at home as they age. However, Internet of Things monitoring solutions create privacy challenges that need to be addressed. This review examines how privacy has been conceptualised in studies proposing new Internet of Things solutions for monitoring older adults. The literature reviewed mostly links privacy with information security and unauthorised accessibility threats. There is a limited consideration of other aspects of privacy such as confidentiality and secondary use of users' information. We argue that developers of Internet of Things solutions that aim to monitor and collect health data about older adults need to adopt an expanded view of privacy. This will ensure that safeguards are built in to Internet of Things devices to protect and maintain users' privacy while also enabling the appropriate sharing of data to support older adults' safety and wellbeing.

Keywords. Internet of Things, aged care, privacy, monitoring

Introduction

In Western countries, more people tend to live alone in their homes as they age rather than living with family members [1] or in residential care facilities. This trend presents an opportunity for new technologies to facilitate the provision of healthcare services to older adults [2]. Aged care monitoring solutions utilise new technologies including Internet of Things (IoT) to remotely monitor older adults' activities, health status and safety in and around their homes [3]. IoT enables physical objects to act smartly by equipping objects with computing resources and sensors; this empowers physical objects to autonomously sense and collect data from individuals and their surrounding environment as well as to transfer these data via the Internet.

Despite the potential benefits of IoT-based aged care monitoring solutions, these devices raise serious concerns about older adults' privacy. Monitoring solutions are designed to operate in older adults' homes, which are private places [4]. Collecting and sharing data is a core function of these monitoring solutions, but this function gives rise to potential threats to older adults' privacy; the devices may collect and share information

[1] Corresponding Author.

that older adults consider to be personal or the data could be accessed/used by unauthorised third parties. Any violation to the older adults' privacy might enhance the risks of dignitary, monetary, or physical harms to occur for them [5]. Therefore understanding how to address and protect privacy in IoT monitoring devices is an important consideration.

1. Study Aims

Privacy is a human right, but is inevitably threatened when technologies are used to monitor people's health and wellbeing. Aged care monitoring is an area where privacy is particularly complex. While researchers have investigated users' concerns about privacy [6], little is known about how developers conceive of privacy. Developers' conceptualisations of privacy play an important role in determining how privacy is addressed. This study aims to gain an initial understanding of the privacy issues that IoT developers are concerned about, by analysing how privacy is addressed in published studies that describe the development of IoT aged care monitoring solutions.

2. Methodology

2.1. Literature Search

The literature search focused on academic literature published between 2010 and 2017. Google Scholar and the university library search engines were the main sources for the literature searched. A search string containing the following keywords with Boolean operators "OR", "AND" was used: Privacy AND ("Older adults" OR "Aging adults" OR Elderly OR "Older population" OR "Older people" OR "Older society") AND ("Internet of Things" OR "Ambient Assisted Living" OR Pervasive OR Ubiquitous OR "Body Sensor") AND (Health OR Healthcare) AND (Monitoring OR Surveillance). The initial search identified 200 papers that were downloaded for primary screening. Based on abstracts and keywords used in these studies, 132 papers were primarily selected. The references used in the selected studies were checked, resulting in 25 more relevant studies. A total of 157 papers were downloaded for secondary screening.

Following closer inspection, 74 papers were excluded according to the following criteria: 1) studies that were poorly written, 2) studies not published in peer-reviewed journals or conference proceedings, 3) studies not written in English, 4) studies that mentioned privacy but did not highlight it as a challenge that needed to be addressed, and 5) papers that discussed the issues but did not describe new aged care monitoring solutions. The final number of papers that were eligible for in-depth content analysis was 29 studies, all of which proposed devices, architectures, frameworks and protocols in the field of IoT-based aged care monitoring.

2.2. Content Analysis

The 29 eligible papers were subjected to a summative content analysis. This approach aims to identify and quantify certain words or content in text with the purpose of understanding the context of the used words [7]. The content analysis started by

searching for occurrences of the term privacy and identifying alternative terms used to describe privacy. Conceptual themes were created based on the identified alternative terms and the occurrences of these alternative terms from the reviewed studies.

3. Findings

The findings are presented as conceptual themes which emerged from the analysis, in a descending order according to the number of occurrences in the reviewed studies.

3.1. Data Security

Nineteen papers highlighted data security as a threat to users' privacy. The sensitive nature of health information such as personal, medical, or human vital parameters imposes securing these data during their collection, transmission and even their storage [8]. Any anomalous events during these processes like intercepting transferred data by malicious users [9], will be considered as eavesdropping [10] or as an unauthorised access to user's data [11]. Many studies (e.g. [11, 12, 13]) proposed solutions that focus on protecting communicated and stored data against security threats such as impersonation, replay, man-in-the-middle, and modification attacks [11] by improving robust security models [13] that employ cryptographic and encryption algorithms.

3.2. Data Accessibility

Fourteen papers mentioned the need to limit access to data only to authorised people and services; not being able to do this was considered a privacy threat. Although data accessibility could be considered part of data security, some of the reviewed studies differentiated between both issues. Data security focuses on protecting data from malicious attacks. Meanwhile, data accessibility is related more to the mechanisms and policies applied in order to regulate stakeholders' access to users' data.

Access to users' data should only be granted to legitimate stakeholders such as caregivers or medical professionals by implementing authentication [14] or access control mechanisms [15, 16]. For instance, Costa et al [17] applied user and password tokens to secure data channels and assure that information about a specific individual was directed only to the appropriate caregiver. Yu et al [18] suggested that user's stored data should be invisible unless a permission to access it has been given by the data owner. Users should also have the ability to restrict data access to only those parts of data that are needed to accomplish a predetermined purpose [19].

3.3. Breach of Confidentiality

Six papers considered breach of confidentiality as a threat to users' privacy that needs to be addressed. Breach of confidentiality is an unauthorised revelation of a user's information that violates the "trust" [5] given by users to service providers for protecting their own information. When users agree to use a particular service, this initiates a relationship based on trust. The trust stipulates that service providers should secure users' data and should allow only legitimate stakeholders to access it. The failure of this will result in a violation to the trust given by users to service providers and may result in

leakage of their own data. For instance, Elkhodr et al [8] and Ogunduyile et al [14] mentioned that privacy involves the confidentiality of patient's data and the assurance that no information leakage from the users' data records is feasible. Su and Chiang [15] highlighted information confidentiality as a security concern, and defined it as the need to protect stored personal data from unauthorised access and manipulation.

3.4. Identification

Identification has been highlighted in six papers. Identification enables us not only to confirm the identity of a person, but also to discover other true information about that specific person [5]. Being able to connect data to an individual could be against individual's will, as this data may reveal true information about them that individuals consider private and do not want to share [5].

Malicious security attacks, weak access control mechanisms or confidentiality issues may lead to unauthorised access to different pieces of users' data collected and stored by aged care monitoring solutions. One example is inference attacks that could be used by malicious users to analyse users' data in order to learn or identify sensitive user behaviors that are considered by users private [20].

Aged care monitoring solutions employ different types of sensors to collect various personal data. As an example, biometric and location sensors are employed to collect sensitive vital parameters and to track the location or the places visited by users [21]. Having the ability to access users' data collected by monitoring solutions raises serious concerns about their privacy; this data has the potential to reveal much more about a person than just their medical conditions [21]. For instance, in the previous scenarios, having the ability to access user's data reveals the different locations that users visit which could be against the user's will.

3.5. Surveillance and Intrusion

Six papers mentioned surveillance and intrusion as an issue that affects user's privacy. Surveillance is to watch, listen or record individual's data that might occur without a person's knowledge or consent [5]. Intrusion is to disturb a person's preference of solitude [5] and is seen to be more related to the user's physical privacy.

Five papers out of six described monitoring solutions that use surveillance cameras, microphones and vision sensors as intrusive to user's privacy and hence were combined in this study in one category. Verbal surveillance in IoT aged care monitoring could lead to recording of conversations that users believe to be private [22]. Moreover, older adults described surveillance as "intrusive" as it interferes with their daily activities [23]. Older adults should be informed whenever information they perceive to be private is recorded and transmitted [22]. Therefore, older adults may not accept monitoring solutions that employ surveillance cameras, [24] or microphones.

3.6. Data Secondary Usage

Using personal data for a different purpose, without consent is considered to be a secondary usage of data [5] and has been mentioned as a privacy threat in three papers. One example of data secondary usage is employing the data collected by monitoring devices that contains sensitive health data in advertisement services [19]. The advertisement agencies might use this data to build insights about the user's health status

and target them with related marketing campaigns [25]. Therefore, only authorised advertisement services should be able to access data and send users health- related advertisements based on it [26].

The lack of control or transparency over access to users' data might result in concerns about who the data might be given to and whether it will be misused [19]. This creates a sense of feeling vulnerable and uncertain [5]. The lack of adherence to users' concerns related to any illegal or unintended uses of personal data could result in undesired consequences such as the rejection of their services or costly lawsuits [19].

4. Discussion

While each reviewed study proposed a solution to protect users' privacy, no clear method on how the developers of these solutions reached their understanding of privacy has been identified. Only one study relied on a privacy theory, "Privacy by design," [27] and defined its principles as rules that govern the development and design of its proposed solution [21]. This raises questions about how developers reach their understanding of privacy and thus propose solutions for it.

Furthermore, most of the reviewed studies focused on addressing privacy by proposing solutions for data security threats. Although data security is a fundamental principle in protecting users' privacy [28, 29], focusing only on security solutions to protect privacy is considered insufficient [8]. A user's privacy could be affected by many threats and solutions should not focus on only a few threats. For instance, none of the reviewed studies highlighted the storage life-time of the user's data collected by monitoring solutions. The longer the data remains stored the greater likelihood of exposure to attacks. User's data should be retained only as long as necessary to fulfill the purposes for which it was collected, and then securely destroyed [27].

Given the General Data Protection Regulation (GDPR) has just come into effect in the EU, this could be considered as a step forward towards creating legal systems to enforce building a more trusted, secure and resilient monitoring devices where older adults privacy is protected. The GDPR covers broad privacy aspects such as affording individuals' explicit control over their personal information and imposing robust security and access control measurements on user's sensitive information.

5. Conclusion

This review found there is no profound understanding of the notion of privacy in the development community. The developers operationalize a narrow view of privacy by focusing on some privacy aspects and ignoring other important aspects. Thus, developers need to adopt an expanded view of privacy by focusing on different privacy issues associated with the use of aged care monitoring devices. Moreover, it is important to conduct empirical studies to further explore older adults' privacy concerns and the limitations in the proposed monitoring solutions in addressing these concerns. Involving older adults to provide insights into privacy issues in aged care monitoring solutions will help proactively detect and address privacy issues by proposing solutions that reflect the developers' and the older adults' perspectives.

References

[1] J. Gaymu & S. Springer, Living conditions and life satisfaction of older Europeans living alone: a gender and cross-country analysis. Ageing & Society, 30(7), (2010), 1153-1175.

[2] F. Jimenez & R. Torres, Building an IoT-aware healthcare monitoring system. In Chilean Computer Science Society (SCCC), 2015 34th International Conference of the IEEE, (2015), 1-4.

[3] A. Sixsmith, Technology and the challenge of aging. In Technologies for Active Aging, Springer US, (2013), 7-25.

[4] B. D Mittelstadt, N. B. Fairweather, N. McBride & M. Shaw, Privacy, risk and personal health monitoring, In ETHICOMP 2013 conference proceedings, (2013), 340-351.

[5] D.J. Solove, Understanding privacy, (2008).

[6] R. Steele, A. Lo, C. Secombe & Y. K. Wong Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. International journal of medical informatics, 78(12), (2009), 788-801.

[7] H. F. Hsieh & S. E. Shannon, Three approaches to qualitative content analysis, Qualitative health research, 15(9), (2005), 1277-1288.

[8] M. Elkhodr, S. Shahrestani & H. Cheung, Ubiquitous health monitoring systems: Addressing security concerns, Journal of Computer Science, 7(10), (2011).

[9] A. J. Jara. M. A. Zamora-Izquierdo & A. F. Skarmeta, Interconnection framework for mHealth and remote monitoring based on the internet of things, IEEE Journal on Selected Areas in Communications, 31(9), (2013), 47-65.

[10] P. Gope & T. Hwang, BSN-Care: A secure IoT-based modern healthcare system using body sensor network, IEEE Sensors Journal, 16(5), (2016), 1368-1376.

[11] C. K. Yeh, H. M. Chen & J. W. Lo, An authentication protocol for ubiquitous health monitoring systems, Journal of Medical and Biological Engineering, 33(4), (2013), 415-419.

[12] R. Lu, X. Lin & X. Shen, SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency, IEEE Transactions on Parallel and Distributed Systems, 24(3), (2013), 614-624.

[13] C. J. Su & C. Y. Chiang, IAServ: An intelligent home care web services platform in a cloud for aging-in-place. International journal of environmental research and public health, 10(11), (2013), 6106-6130.

[14] O. O. Ogunduyile, O. O. Olugbara, & M. Lall, Development of wearable systems for ubiquitous healthcare service provisioning, APCBEE Procedia, 7, (2013), 163-168.

[15] C. J. Su & C. Y Chiang, Pervasive community care platform: Ambient Intelligence leveraging sensor networks and mobile agents, International Journal of Systems Science, 45(4), (2014), 778-797.

[16] J. H. Abawajy & M. M. Hassan, Federated internet of things and cloud computing pervasive patient health monitoring system, IEEE Communications Magazine, 55(1), (2017), 48-53.

[17] A. Costa, P. Novais & R. Simoes, A caregiver support platform within the scope of an ambient assisted living ecosystem, Sensors, 14(3), (2014), 5654-5676.

[18] Z. Yu, Y. Liang, B. Guo, X. Zhou & H. Ni, Facilitating medication adherence in elderly care using ubiquitous sensors and mobile social networks. Computer Communications, 65, (2015), 1-9.

[19] M. Henze, R. Hummen & K. Wehrle, The cloud needs cross-layer data handling annotations. In Security and Privacy Workshops (SPW), 2013 IEEE, (2013), 18-22.

[20] S. Samarah, M. G. Al Zamil, A. F. Aleroud, M. Rawashdeh, M. F. Alhamid & A. Alamri, An Efficient Activity Recognition Framework: Toward Privacy-Sensitive Health Data Sensing, IEEE Access, 5, (2017), 3848-3859.

[21] J. Pedraza, M. A. Patricio, A. De Asís & J. M. Molina, Privacy-by-design rules in face recognition system, Neurocomputing, 109, (2013), 49-55.

[22] I. D. Addo, S. I. Ahamed, S. S. Yau & A. Buduru, Reference architectures for privacy preservation in cloud-based IoT applications. IJSC, 2(4), (2014).

[23] F. Portet, M. Vacher, C. Golanski, C. Roux & B. Meillon, Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects. Personal and Ubiquitous Computing, 17(1), (2013), 127-144.

[24] K. R. Pragnya & J. K. Chaitanya, Wireless Sensor Network based Healthcare Monitoring System for Homely Elders. International Journal of Advances in Engineering & Technology, 6(5), (2013), 2078.

[25] R.A. Spinello, Privacy rights in the information economy. Business Ethics Quarterly, 8(04), (1998), 723-742.

[26] Z. Pang, L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova & Q. Chen, Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things, Enterprise Information Systems, 9(1), (2015), 86-116.

[27] A. Cavoukian, Privacy by design. Take the challenge. Information and privacy commissioner of Ontario, Canada, (2009).

[28] Y. Wang & A. Kobsa, Technical solutions for Privacy-Enhanced personalization, Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies: IGI Global, (2008).
[29] H. J. Smith, T. Dinev & H. Xu, Information privacy research: an interdisciplinary review, MIS quarterly, 35(4), (2011), 989-1016.