How to cite this paper:

Kavenesh Thinakaran, Jaspaljeet Singh Dhillon, Saraswathy Shamini Gunasekaran, & Lim Fung Chen. (2017). A conceptual privacy framework for privacy-aware iot health applications in Zulikha, J. & N. H. Zakaria (Eds.), Proceedings of the 6th International Conference of Computing & Informatics (pp 175-183). Sintok: School of Computing.

A CONCEPTUAL PRIVACY FRAMEWORK FOR PRIVACY-AWARE IOT HEALTH APPLICATIONS

Kavenesh Thinakaran[1], Jaspaljeet Singh Dhillon[2], Saraswathy Shamini Gunasekaran[3], Lim Fung Chen[4]

[1]*College of Computer Science and Information Technology*
[2]*Universiti Tenaga Nasional, Malaysia*
[3456]*kavenesh13@gmail.com, jaspaljeet@uniten.edu.my, sshamini@uniten.edu.my, fclim@uniten.edu.my*

ABSTRACT. Internet of things (IoT) is intensely gaining reputation due to its necessity and efficiency in the computer realm. The support of wireless connectivity as well as the emergence of gadgets alleviates its usage essentially in governing systems in various fields. Though these systems are ubiquitous, pervasive and seamless, an issue concerning consumers' privacy remains debatable. This is most evident in the health sector, as there is an immaculate rise in terms of awareness amongst patients where data privacy is concerned. In this paper, we propose a framework modelling the privacy requirements for IoT-based health applications. We have reviewed several privacy frameworks to derive at the essential principles required to develop privacy-aware IoT health applications. The proposed framework presents important privacy requirements to be addressed in the development of novel IoT health applications.

Keywords: Internet of things, privacy framework, requirements, healthcare applications

INTRODUCTION

Privacy can be conceptualised as "the right to be left alone" (Warren & Brandeis, 1890). It refers to the process of disclosing and mobilizing one's personal data under certain conditions and safeguarding measures (Ruback, 2015). The distinction or overlap between 'privacy' and 'security' are subtle. While 'privacy' indicates freedom from unauthorized intrusion, 'security' alludes to procedures or measures taken to ensure the safeguarding of privacy. Privacy encompasses five prominent aspects as described below (Buttyan & Hubaux, 2008):

Unlinkability. Protecting information regarding the relationship between any items, for example, actions, messages and subjects.

Untraceability. Impossible to trace back an individual based on performed set of actions.

Unobservability. Protecting the fact that a text was sent and the identity of both the sender and recipient.

Anonymity. Protecting information with regards as to who performed a certain action or who is mentioned in a given dataset per say.

Pseudonymity. Utilization of pseudonyms instead of real identifiers.

Privacy is a prominent issue for consumers in a globally connected network society (Smith et al., 2011). The concern towards privacy risks is escalating as we are moving forward into a ubiquitous world, where more innovative self-care applications are being developed using a prominent technology widely known as the Internet of Things (IoT).

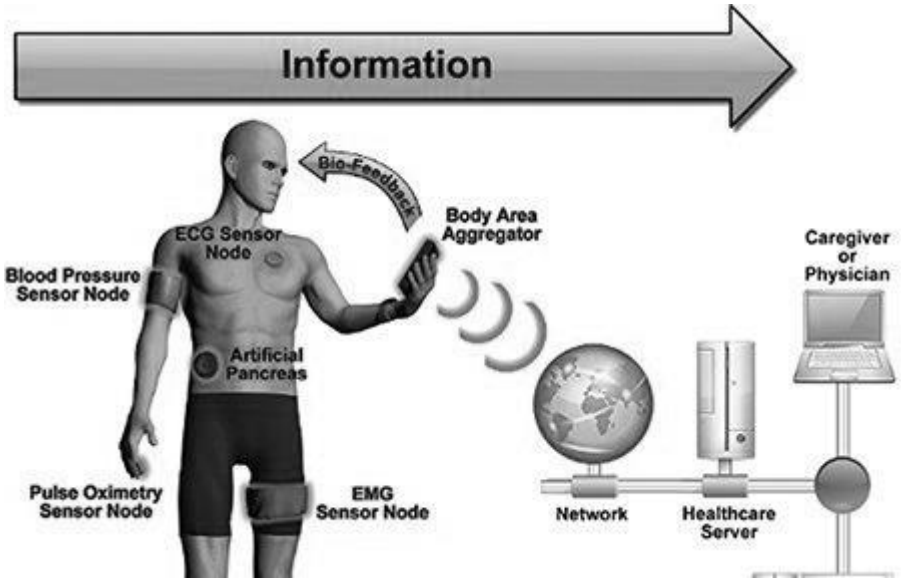

Figure 1. Remote healthcare enabled via IoT (Ianace, 2015).

IoT is a highly distributed and ubiquitous network of seamlessly connected heterogeneous devices that is integrated with the existing Internet and mobile networks. This paves the development of new intelligent health services which is made available anytime, anywhere, by anyone and anything. Healthcare is one of the most attractive applications for IoT (Pang, 2013) because it is designed to improve the efficiency, effectiveness, quality and cost of healthcare by enabling physicians to remotely monitor their patients as well as letting individuals manage their own health at ease (Islam et al., 2015).

Unlike typical health applications that offer health-related services via smartphones and tablets, IoT-based health applications involve a collection of health tools and medical devices which require Internet connectivity (Islam et al., 2015). They encompass a broad range of applications that provide healthcare services such as remote health monitoring, fitness programs, elderly care, electronic patient records, telemedicine, surgical simulations and so much more. The devices associated with this application often are wearable technology devices. Some other examples include headsets that measure brainwaves, clothes with sensing devices, BP monitors, glucose monitors, ECG monitors, pulse oximeters, sensors embedded in medical equipment, dispensing systems, surgical robots and device implants. Figure 1 illustrates an example of how IoT enables remote healthcare, in which health data of patients are transmitted to healthcare providers via wireless telecommunication devices for monitoring and treatment purposes. In a nutshell, these applications have great potential for advance personalized connected healthcare, some of which has never been imagined before, but are nevertheless possible via integration of diverse technologies. However, these applications are prone to unknown risks and issues.

Despite the benefits of leveraging on IoT-based health applications, there are many challenges associated with its implementation. As an example, health data collected rapidly from various sources may significantly impact consumer's privacy. This may lead to potential widespread surveillance of individuals without their consent or knowledge (Oriwoh et al.,

2013). In June 2015, a huge privacy-violation attack occurred when malware comprising blood gas analyzers gained access into hospital networks and in the process stole confidential data (Storm, 2015). Apart from this, the open and interconnected environment of IoT supports the exchange of sensitive data like mental health, genetics, reproductive care and substance which are prone to privacy risks abuse. Furthermore, all online and offline activities are recorded and stored forever which may be prone to identity threats, location threats and data eavesdropping (Al-mawee, 2015). This raises concerns as to who will have access to this information and under what terms, conditions, and whether the public will be subjected to serious privacy infringement (Medagalia & Serbanati, 2010). Eventually, this portrays a strong case on why is our study important.

Given these challenges, IoT-based health applications are expected to be open and transparent to the patients and thus be explicit with the patients on the reasons for collecting their personal information and hence also ensuring the protection of their data along the road (Medagalia & Serbanati, 2010). There are guidelines available for developers to design applications to safeguard the privacy aspects of consumers. Likewise, there are also the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) to enforce the privacy and protection of health information of consumers (Blumenthal, 2010). However, most of the guidelines available provide general privacy principles which may be insufficient to design novel IoT applications that deal with sensitive health information. We argue that IoT-based health applications are more susceptible to privacy risks and hence privacy guidelines for health applications in general are inadequate. Moreover, it is apparent that privacy is often oversighted, causing consumers to lose interest from using an application continuously. The emphasis of most research efforts are in the design of security frameworks or the combination of both the privacy and security frameworks. Hence, the prominent objective of this paper is to develop a privacy framework to assist in the design of the IoT-based health applications. We have critically reviewed several privacy frameworks to identify the relevant principles to be included in the framework here. The framework will be useful for developers to understand better the privacy requirements of consumers when designing novel IoT-based health applications that deal with sensitive health information.

The remainder of the paper is structured as follows. The succeeding section reviews existing privacy guidelines, where an overview of the framework and respective principles are presented. In the subsequent section to that, the principles are compared and the shortcomings are discussed with regards to the development of privacy-aware IoT-based health applications. In addition, the proposed framework is also presented. The final section concludes the paper.

EXISTING PRIVACY FRAMEWORKS

Identification of privacy requirements for IoT-based health applications is vital for developers to understand the expectations of consumers in ensuring confident and sustainable use of novel IoT applications. In this section, we review existing solutions that are aimed at preserving privacy in several areas. These solutions are presented in a chronological manner. Table 1 summarizes privacy principles that are included in existing frameworks.

Aivaloglou, Gritzalis & Skianis (2006) reported a set of requirements to design privacy-aware sensor networks. The proposed framework was derived based on the understanding built upon privacy requirements and challenges in preserving privacy. This guideline presents five principles that are emphasized on sensor networks, which is the backbone to develop ubiquitous IoT-based solutions that are known to impose greater privacy risks.

In May 2008, the Center for Democracy & Technology released a comprehensive privacy and security framework to support the protection of health data (Center for Democracy & Technology, 2008). This framework is a revised version of the common framework which was released by the Markle Foundation in the project Connecting for Health (Markle Foundation, 2008) The framework contains nine principles that is based on mix legislative action, regulation and industry commitment.

A comprehensive framework governing the electronic exchange of individually identifiable health information was introduced by the U.S. Office of National Coordinator (ONC) for Health Information Technology (Office of National Coordinator, 2008). In the development process of this ONC framework, various international, national, public, private sector and security principles were reviewed. A careful review and analysis of these principles were conducted by accommodating as much variation as possible keeping well in mind at the same time as to how they may be applied to electronic data. The ONC framework covers eight principles that serve as a guideline for public and private sector entities that hold or exchange electronic individual health-related data and help to guide the Nation's adoption of health information technologies.

In the year 2014, Alqassem and Svetinovic released a taxonomy on security and privacy requirements for the IoT. The taxonomy presented quality attributes that were applied in an IoT smart grid scenario. The document provides support for more investigation of expected privacy and security vulnerabilities and threats in relation to IoT. The presented four principles mainly cover the security aspects of IoT.

In recent times, AL-mawee (2015) reported a survey on security and privacy issues in IoT healthcare applications in the context of disable users. A wide range of IoT based applications for the disabled were presented. These presentations identified the respective security and privacy issues for the applications. Furthermore, main solutions to these applications were discussed at length and prominent privacy and security requirements for the disabled were defined as well. This study presented a framework consisting of seven principles.

Recently, Porambage et al. (2016) reported design guidelines for preserving privacy in IoT in general. The guidelines presented are applicable to govern privacy issues and concerns of different industries specifically for healthcare, smart homes, public safety and supply management. It provides insight into privacy requirements that needs to be integrated in the development of privacy frameworks, in our context, IoT-based health applications. The guidelines developed are based upon examining the complementary pieces of technology or application-specific privacy frameworks and the IoT network attributes such as the technological aspects and legal regulations. It provides nine characteristics to be included when deploying an IoT privacy framework.

Table 1. A Summary of Privacy Principles included in Existing Frameworks.

Framework Code	**F1**	**F2**	**F3**	**F4**	**F5**	**F6**
Author	Aivaloglou, Gritzalis & Skianis (2006)	Center for Democracy & Technology (2008)	U.S. Office of National Coordinator for Health Information Technology (2008)	Alqassem & Svetinovic (2014)	Al-mawee (2015)	Porambage et al. (2016)

Objective of the framework	To identify the requirements for privacy preserving sensor networks	To generate a comprehensive privacy and security framework for • e-health efforts	To establish a privacy framework for electronic health information exchange	To present a taxonomy on security and privacy requirements for IoT	To identify privacy requirements for IoT health based applications for the disabled	To develop a holistic privacy framework for IoT
For IoT?	Yes	No	No	Yes	Yes	Yes
Privacy principles included	• Data confidentiality, • Protecting the communication's context • User anonymity • Ensuring data authenticity and integrity • User data disclosure	• Openness and transparency • Purpose specification and minimization • Collection limitation • Use limitation • Individual participation and control • Data integrity and quality • Security safeguards and controls • Accountability and oversight • Remedies	• Individual access • Correction • Openness and transparency • Individuals choice • Collection, use and disclosure limitation • Data quality and integrity • Safeguards • Accountability	• Access control • Data integrity • Contextual Integrity • Intrusion detection	• Data ownership • Disabled's permission for access to her data • Disabled anonymity and pseudonomity • Location privacy • Maximizing locality of information • Privacy provided devices • Empathizing on privacy for application design	• Openness, transparency and purpose specification • Identify privacy • Temporal and location privacy • Query privacy • Access control • Interoperability • Data minimization • Accountability • Security

FINDINGS & DISCUSSION

This study proposes a framework modelling the privacy requirements for IoT-based health applications. Frameworks presented in the preceding section are critically reviewed in terms of their suitability to aid development of privacy-aware IoT-based health applications. The principles were evaluated using a list of pre-defined criteria. Thereafter, essential privacy principles to govern for IoT-based health applications were derived. The following list describes the criteria used to gauge suitability of the existing frameworks for privacy-aware IoT health applications: (1) generalizability: to what extent is the framework applicable to IoT-based health applications in general?, (2) ambiguity: is there any principle(s) that is ambiguous or similar but segmented into two different principles?, (3) relevance: are the principles relevant for IoT-based healthcare applications?, and (4) completeness: are the principles adequate to cater for IoT-based healthcare applications?

Our analysis of existing privacy frameworks reveals essential principles that are to be considered in an ideal privacy-aware application. It is apparent that most of the frameworks are aimed at preserving privacy in specific areas. Out of the six frameworks analysed, four are related to IoT (i.e. F1, F4, F5 and F6), whereas F2 and F3 focus on preserving privacy in health data in general. Based on our review, there hasn't been much work done in the area of

preserving privacy in IoT and to the best of our knowledge, ours is the first study whose primary focus is on IoT-based health applications.

F1 systemically outlines the requirements for designing a privacy aware network. Although, it is an IoT framework, the focus is into sensor networks' security requirements and as such, it may not be suitable for IoT healthcare applications in general. In addition, the issue of complexity arises in having to distinguish between privacy and security principles as both relate to completely different aspects. For instance, *protecting the communication's context* is considered as a security factor since it involves encryption keys. Furthermore, it covers only a few principles, making it singularly inadequate to cater for a broad range of IoT sensors especially in healthcare industry.

F2 highlights the core privacy principles for healthcare applications. However, some of the principles are ambiguous in nature, which makes it difficult to comprehend their meaning. For example, *collection limitation* and *use limitation* principles may convey the same meaning. In addition to that, F2 segments the principle *security safeguards and controls* and *remedies* into two different principles. In actuality, the two segments actually rely on one other and could have been merged since the former was addressed to protect the health data and the latter was to inform consumers regarding security attacks or privacy breaches.

F3 is a comprehensive privacy framework developed to govern the electronic exchange of health information. However, two of its principles, i.e. *individual access* and *individual choice* could have been merged. Furthermore, *correction* isn't relevant to privacy of consumers. F4 provides a list of principles to address a combination of security and privacy issues. However, it provides a total of only four principles. Hence, the privacy principles covered here are seen to be insufficient to generate a workable framework.

Unlike the rest of the frameworks, F5 clearly distinguishes the fine line between privacy and security requirements by segmenting security and privacy requirements into two different principles from the outset. However, some of the principles included are predominantly confined toward disabled consumers. For instance, principles such as *privacy provided devices and empathizing on privacy for application* are not relevant for IoT health apps in general. Furthermore, F5 also lacks important principles such as those pertaining to protection of ownership of consumers' health information.

F6 proposed a general framework on characteristics to include when developing an IoT privacy framework that is directly relevant and useful to develop different types IoT applications. However, the principles included cover both security and privacy aspects of an application. In addition, some of the principles are ambiguously overlapping each other (e.g. *identity privacy, query privacy, temporal and location privacy).* As an instance, similar to F1, these three principles are merged into one principle called *user anonymity*.

Results presented in Table 2 indicate that the frameworks reviewed in this paper are useful for their respective purposes, but isn't sufficient if they are to be used to govern IoT health applications. Based on the review, each of the reviewed frameworks has its own strengths and limitations with regards to its suitability to govern privacy aspects of IoT health applications. However, F2, F3 and F6 require minimum modification if applied in our context. We also took notice that none of the above mentioned frameworks are on governing the life-span of the collected data. The duration of storing of the health data might post a privacy concern. The data subjects should be informed with the duration of storage of their data by the data users and it is also the right of the data subjects to be made aware of the time of disposal of their health data.

Table 2. Framework Evaluation Results.

	F1	F2	F3	F4	F5	F6
Generalizability	x	√	√	√	x	√
Ambiguity	x	x	x	√	√	√
Relevance	√	√	√	x	√	x
Completeness	√	√	√	x	√	√

Table 3 presents the conceptual framework, with a definition of all the principles incorporated. The framework was formulated upon discarding irrelevant requirements, extracting repeating core principles, and merging relevant principles. This framework will be empirically tested with consumers to confirm the principles included. The resulting framework will provide essential privacy principles that should be adhered in designing privacy-aware IoT health applications.

Table 3. A Conceptual Framework for IoT-based Health Applications.

Principle	Description	Source
Access control	Consumer health related information should only be accessible to authenticated and authorized personnel. Limited access to consumer's health related information should be ensured. Consumers should possess a little control over the data.	F2, F3, F4, F5 & F6
Anonymity	The identity of the consumers using IoT-based health applications, device and system needs to be protected. Unlinkability must be ensured between the consumers and their health related data respectively. Identification and tracking of consumers should be impossible. Indistinguishability among consumers should be achieved	F1, F5 & F6
Consent	Before the collection of health related data, the consumer needs to be acknowledged on the details being collected. Clinicians or third parties may access the information only via the consent of the consumer. Data subject's consent is also needed for the duration of storing and disposal of the collected health data.	F5
Data disclosure	Health consumer needs to be notified and aware of with whom his/her health data is being shared with. Once the user has clearly understood via a short notice with whom the data will disclosed, then the collection process may take place. Consumer needs to be empowered whether to share his/her health related information to third parties or other entities.	F1 & F3
Data minimization	The collection and storage of consumer's health data should be minimized to which that information is necessary to perform a service.	F2 & F6
Openness and transparency	Consumers not only need to know the use of their health data but the manner of collection as well. The personnel who has access to it and where it resides should also be made loud and clear.	F2, F3 & F6
Purpose specifications	The purpose why the health data is being collected needs to specified at the time of collection. The usage of data should be limited to that particular purpose stated in the beginning and if there is further use of it, the user should be notified from time to time.	F2, F3 & F6
Safeguard and remedies	Consumer's health data should be protected against risks for example unauthorized access, destruction, and etc. In the event it happens. the consumer should be notified regarding the breach and violation.	F2, F3 & F6
Data life-span	The duration of storing the health data collected. After the prescription,	

	for how long the health data can be kept by the data user. If the health care data is no longer needed, it should be disposed of with the data subject's consent. If the data is required for further prescription, then the data subject's consent is needed for the extension of data storing duration.	

CONCLUSION

There have been inadequate studies with regards to privacy requirements of IoT-based health applications. We have studied existing privacy frameworks in deriving suitable principles that are salient to develop privacy-aware IoT-based health applications. The derived principles make up a framework that would be useful for policy makers and applications developers to better understand the privacy requirements of consumers towards IoT-based health applications. Now that we have identified the necessary core principles, we are geared towards an empirical evaluation of the proposed framework with health consumers to finalize them based on their significance.

ACKNOWLEDGEMENTS

This study is funded by the Malaysian Ministry of Higher Education (MoHE) under the Fundamental Research Grant Scheme (FRGS).

REFERENCES

Aivaloglou, E., Gritzalis, S., & Skianis, C. (2006). Requirements and Challenges in *the Design of Privacy-aware Sensor Networks.* Retrieved from http://ieeexplore.ieee.org/document/4150864/

Al-mawee, W. (2012). Privacy and Security Issues in *IoT Healthcare Applications for the Disabled Users a Survey.* Retrieved from http://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses

Buttyan, L., & Hubaux, J.P., "Privacy protection," in Security and cooperation in wireless networks: Thwarting malicious and selfish behavior in the age of ubiquitous computing. *New York: Cambridge University Press, 2008,* pp. 237-254.

Blumenthal, D. Launching HITECH, *N. Engl. J. Med*., vol. 362, no. 5, pp. 382–385, 2010.

Center for Democracy & Technology. Comprehensive privacy and security: Critical for health information technology. *White paper, May 2008*. Retrieved from https://www.cdt.org/files/healthprivacy/20080514HPframe.pdf

Darlene Storm. (2015). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks.* Retrieved from http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

Health Information Privacy. Retrieved from http://www.hhs.gov/hipaa/D.

Ianace, P. (2015). *Internet of Things, Remote Healthcare, One Example*. Retrieved from https://www.linkedin.com/pulse/delivering-iot-promise-one-example-pete-ianace

Islam, S. M. R., Kwak, D., Kabir, H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. Access, *IEEE, 3, 678–708.* http://doi.org/10.1109/ACCESS.2015.2437951

Markle Foundation. Common Framework for networked personal health information: Overview and principles. Connecting for Health, June 2008. Retrieved from https://www.markle.org/sites/default/files/CF-Consumers-Full.pdf

Medaglia, C. M., Serbanati, A. "An overview of privacy and security issues in the internet of things", *In Proc. of 20th Tyrrhenian Workshop on Digital Communications, Italy, 2010, pp. 389-395*

National Committee on Vital and Health Statistics. Individual control of sensitive health information accessible via NHIN. *NCVHS letter to HHS Secretary, Feb. 2008*. Retrieved from http://www.ncvhs.hhs.gov/080220lt.pdf.

Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. *The nationwide privacy and security framework for electronic exchange of individually identifiable health information*, Dec. 2008. Retrieved from https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

Oriwoh E, Sant P, Epiphaniou G. Guidelines for internet of things deployment approaches–the thing commandments. *Procedia Comput Sci 2013*;(21):122–31.

Pang, Z., "Technologies and architectures of the Internet of Things (IOT) for health and well being," M.S. Thesis, Dept. Electron Comput. Syst., *KTH-Roy. Inst. Technol*., Stockholm, Sweden, Jan. 2013

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing, 3(2), 36-45*. doi:10.1109/mcc.2016.28

Ruback, T. (2015*). Understanding the Differences Between Privacy and Security Online*. Retrieved from https://www.ghostery.com/intelligence/business-blog/privacy/understanding-the-differences-between-privacy-and-/

Smith, H. J., Dinev, T. & Xu, H. (2011). Theory and Review Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly Information Privacy Research, 35(4), 989–1015*.Retrieved from http://pal.ist.psu.edu/MISQ.pdf