

IoT Healthcare: Benefits, Issues and Challenges

Roberta De Michele

Department of Industrial Engineering
University of Bologna
Bologna, Italy
roberta.demichele2@unibo.it

Marco Furini

Dip. di Comunicazione ed Economia
Università di Modena e Reggio Emilia
Reggio Emilia, Italy
marco.furini@unimore.it

ABSTRACT

A sportsman's watch no longer marks the time, but it also provides information on the geographical location, on the number of steps, on the heart rate, on the blood oxygenation, on the blood pressure, etc. The bracelet of an elderly person can measure different physiological signals and can transmit them in real time to her doctor, allowing him to monitor the state of health even if the two are not in the same place. Thanks to the implementation and use of sensors, watches and bracelets have become *smart objects*. It is the world of the Internet of things that enters the health sector and fills the shelves of electronic stores with objects that can monitor our bodies. A market sector that is worth billions of dollars, but that has several implications along with its benefits. *What happens to our data? Who has access to our data? Is it possible to cyber-attack these devices? Is our behavior influenced by reading this data?* These are some of the questions that arise from the use of IoT devices in the health sector and in this paper we will address them by analyzing this scenario in detail, by highlighting threats and vulnerabilities and by proposing approaches that might mitigate issues related to the use of IoT in the health scenario.

CCS CONCEPTS

• **Applied computing** → **Life and medical sciences; Consumer health; Distance learning; E-learning;**

KEYWORDS

IoT healthcare, privacy, security

ACM Reference Format:

Roberta De Michele and Marco Furini. 2019. IoT Healthcare: Benefits, Issues and Challenges. In *EAI International Conference on Smart Objects and Technologies for Social Good (GoodTechs '19)*, September 25–27, 2019, Valencia, Spain. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3342428.3342693>

1 INTRODUCTION

People use social media to talk about their illnesses, symptoms, and feelings and make their health decisions according to what

they read on-line [9, 14, 22, 29]. This phenomenon is highlighted by the number of online health data that increased a lot in the last few years [30] (i.e., approximately 72% of US and 47% of European Internet users have searched online for information about a range of health issues like specific diseases and treatments [3, 17]). In addition to people, the scenario is observing an increasing number of algorithms that access to these data to understand not only what people think (e.g., [10, 15, 20]), but also to identify whether they are healthy or not (e.g., [8, 11, 33]). Far from deciding whether this is a promising or a dangerous scenario, we simply observe that the Internet of Thing is about to revolutionize the health scenario.

Internet of Things (IoT) is an idea recently embraced by academia, industry, governments, city administrators to connect people and physical objects with the final goal of improving the life quality of citizens [6]. To achieve this improvement, it is necessary to transform these objects into their "smart" version. Indeed, objects should be able to capture, share and communicate data to service providers, where the analysis of the collected data might performed and then used to produce intelligent services [19, 25]. Examples of physical objects that might become smart are vehicles, home appliances, smartphones, home and wearable sensors, whereas examples of intelligent services are: road lane control, efficient electricity consumption, crash prevention or exercise tips to keep fit. In general, these services can be grouped under the name of *smart city*, *smart home*, *smart environment*, *smart health*, *smart industry*, etc. Among these, one of the most promising IoT application is the so called "Smart Health" scenario.

The global IoT in healthcare market size is projected to reach USD 534.3 billion by 2025 and the penetration of connected devices in various healthcare institutes and the use of personal IoT systems are seen as the key factors augmenting the market growth [12] together with advancements and innovation in wearable technology (sensors, wireless communication and computational capability) and increasing incidence of chronic diseases. Statistics of 2018 talk about more than 97,000 mobile health apps available on main app stores and at least 52% of smartphone users collecting health-associated information on their cell phones. The importance of IoT technologies in the medical sector is highlighted by the term IoMT, a recent definition that became available to indicate the Internet of Medical Things, a collection of medical and fitness devices and applications that connect to healthcare IT systems through online computer networks. It is important to note that, if until a few years ago, medical devices available to private citizens were very expensive and cumbersome, nowadays we are witnessing a convergence between fitness and medical devices [35] and the progressive development of smaller and low cost versions that are being sold

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

GoodTechs '19, September 25–27, 2019, Valencia, Spain

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6261-0/19/09...\$15.00

<https://doi.org/10.1145/3342428.3342693>

at affordable prices. For instance, the Apple watch incorporates a photoplethysmogram sensor to measure heart rate. Moreover, the acquired physiological data are usually used by smartphone apps to provide medical advice.

The fields of applications of IoT in the medical sector seem to be endless, but the most promising ones are:

- **Remote Patient Monitoring:** healthcare professional might remotely monitor patients thanks to the use of smart body sensors able to perform specific tests on the patient's body. Needless to say, this monitoring is particularly suited to the chronically ill and the elderly;
- **Electronic Healthcare Records:** patient's data might be collected into a centralized center where healthcare professional such as doctors, nurses, labs, etc., might find all the patient's data in real time regardless of their geographical location. The availability of patient's data will allow data analytics to provide insights and/or predictions about the health status of a patient;
- **Preventive Healthcare:** the availability of patient's data might trigger a personalized, collaborative and preventive form of care: when a potential problem is sensed, IoT devices might alert the patient's doctor for a proactive action) [26, 34].

There are many examples of IoT healthcare applications. For instance, Philips developed devices that are able to alert patients when it's time to take their pills, and can provide pre-filled cups with medication ¹; Eversense provides a glucose monitoring system that uses a sensor, implanted below the patient's skin, to measure the blood glucose level and send it to patient's doctor using a mobile phone app ². In general, the benefits that IoT might introduce in the health sector can be summarized in:

- **Cost reduction** (e.g., thanks to the remote monitoring, it is likely that visits to doctors and hospital stays will be reduced);
- **Better accuracy:** (e.g., a continuous monitoring will likely improve the accuracy of the diagnosis);
- **Medicine tracking:** (e.g., IoT will make it possible to check if patients adhere to their treatment plans, rehabilitation and post-operative care);
- **Improved efficiency:** (e.g., through the avoidance of unnecessary tests, but also by increasing the speed of intervention in emergency situations);
- **Geographical independence:** (e.g., patient's data will be available to health professional regardless of the patient's location and health care delivery will be ensured even in resource-limited settings and remote locations);
- **Real-time monitoring:** (e.g., IoT devices can collect, and transfer to doctors, health data such as blood pressure, oxygen and blood sugar levels, weight, and ECGs and so on and so forth, allowing constant management in case of cardiovascular diseases or timely intervention in case of acute trauma or stroke).

The benefits described above are just the bright side of the IoT healthcare scenario, but there are threats and vulnerabilities that

might slow down the adoption of IoT devices. In the following, we describe what we consider the most important issues that need to be addressed.

2 ISSUES IN THE IOT HEALTHCARE SCENARIO

In 2011, a research highlighted that an insulin pump might be remotely hijacked and its entire insulin supply administrated to the patient causing her a possible lethal insulin shock [23]. On August 2014, a news reported a massive health data theft by a group of hackers that managed to breach the network that connects 206 hospitals in the United States, and to obtain 4.5 millions patients' records including sensitive information such as names, addresses, birth-dates, telephone numbers and social security numbers [16]. It is very plausible that these threats remain nowadays, since it was just in the end of 2017 when Privacy researchers at Yale Law School have discovered third parties clandestine app trackers secretly collecting and analyzing data from a wide range of Google Play and Apple Store apps. On 2017, a research showed that implantable cardiac devices (i.e., pacemakers and defibrillators) have vulnerabilities that could allow hackers to deplete the battery or to give incorrect pacing or shocks. These examples shows some security vulnerabilities of IoT devices in the health scenario, but security is not the only problem.

In 2013, IoT botnets were found to be collecting users' personal information and monitoring their activities without user consent and not even awareness of this data acquisition [31]. The sale of fitness data to third parties - mostly for advertising reasons, but also to insurance companies with an interest in knowing about customers' pre-existing conditions or chronic diseases - had occurred and was denounced again in 2014. Indeed, a study conducted by the US Federal Trade Commission on several fitness apps, found dissemination of users' data to third parties without their consent. Some years later, in 2018, the launch and introduction of Apple Health app opened new questions and concerns about the security and privacy of users' health data, especially when its storage and processing take place on the cloud. These events clearly show the problems that affects the market of medical devices and wearables: they are vulnerable to tampering from hackers and cybercriminal, that could be able to access them and manipulate their functioning, with dangerous implication for patients' health (see implantable defibrillators or pacemakers). As established by Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule ³ the providers must ensure that the infrastructure is secure and that their clients' data and applications are protected [35].

In general, IoT sensors have the potential to provide benefits to patients and to potentially transform healthcare, but they might also expose patients and healthcare providers to risks. Among the several threats and vulnerability, in the following we describe details of the most important ones:

- **Security.** It refers to "physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure" [2] at back-end (IT systems), front-end (sensors) and network level [28]. In a scenario where health depends on devices connected to

¹<https://www.lifeline.philips.com/>

²<https://ous.eversensedabetes.com/products/>

³<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>

the network, ensuring safety is of fundamental importance. Indeed, a cyberattack alters the number of steps in a bracelet it is certainly harmless, but an attack on a pacemaker, a defibrillator or an insulin pump can become lethal. Furthermore, when connected to an unprotected or poorly protected network, all devices represent endpoints for potential cyberattacks, or access points to the wider network where patient health information are stored. Indeed, health information are now more valuable on the black market than credit card information [37] (e.g., health insurance records are valued 10 times more than credit card verification value (CVV) numbers and may be used to purchase prescription drugs, submit billings in other people names and obtain health insurance) Needless to say it is necessary to ensure the security of communications, otherwise people could be wary of these devices, slowing down or eliminating personal and healthcare benefits.

- **Confidentiality.** It refers to the obligation of all professionals involved with access and processing of patient records or information, to hold such data in confidence, that is, that health information are protected from being shared with third parties without express consent. It is the traditional professional confidentiality that applies to conversations and visits between physicians and patients, that is it nowadays evolving into its digital form: patients can send medical reports or measurements to doctors via mobile apps or directly from wearables, but are we completely confident these data is not being shared with other individuals or companies? From a more technical point of view, confidentiality is also defined as the process that ensures that sensitive data will be readable only by the intended destination [32]. When all your personal health data are in one place there might be benefits but also threat. It is very useful for doctors to establish a diagnosis, it can facilitate the task of analysis algorithms that, having a lot of data available, can try to predict the health status of a patient. But what happens if these data are available to health insurance companies or to employers? A person with a chronic illness could be discriminated against, denying her the health insurance or a job. Again, it is necessary to implement mechanisms able to guarantee the confidentiality of data.
- **Privacy.** It refers to the right of patients to be in control of “the acquisition, uses, or disclosures of his or her identifiable health data” [27], because even if health data is usually stripped of users’ identification information, it can easily be combined with other data to give a full portrait of each individual. Of course, the privacy right can be exercised by individuals who have ownership of the data. To clearly establish the ownership of data could not be as straightforward as it seems and it may also vary depending on the context, i.e. people collecting data on a sleep monitoring app or calories tracker versus data collected by hospitals or doctors and stored in patients’ Personal Health Records. The issue of privacy is also connected to the protection from exposure (accidental or malicious) of personal data that may reveal the user/patient identity: even if health data is anonymized

and stripped of users’ identification information, it can easily be re-combined with other data to give a full portrait of each individual. Kumar et al [28] further distinguish four layers of privacy to be addressed: (1) Privacy in device, or the unauthorized manipulation of hardware/software in device; (2) Privacy during communication, e.g. during data transmission; (3) Privacy in storage, that should affect only the minimum necessary amount of information and anonymized for identity protection; (4) Privacy at processing, that should be done in compliance with data owner’s

- **Unintended behavior.** It refers to people who change their behavior according to the physiological data they observe on their device. Some people might become less active when they notice that many other people are less active; other become addicted to their physical activities; other become anxious about their health; other try to analyze their data to produce self-diagnosis, etc. The point is, data is not information. Turning raw data into meaningful and useful information is a task reserved for specialists. Heartbeat data can be turned into insights by a doctor, that could take decision and act appropriately, but could be turned instead into misleading information by an ordinary person. It is therefore necessary to inform people that these sensors provide data, not information. Similarly, it is always good to remind people that smartphone applications that gather and process this data by turning it into information, in most cases have no scientific value, do not rely on scientific literature and ultimately do not replace medical advice.

These four issues can put the entire IoT health sector at risk. For this reason, it is necessary to address these aspects and to look for solutions that allow people to enjoy the benefits rather than fear the risks of IoT sensors and devices.

3 CURRENT APPROACHES

Since news and “scandals” related to data theft and data breaches continue to appear on newspapers regularly, some of these issues have been noticed already in the last times, along with some attempts to address them in various ways.

It has been proposed, for example, to submit Health apps to the same certification process of medical devices, that are actually being controlled and assessed by entities such as the Food and Drug Administration (FDA) for the United States, or the European Medicines Agency (EMA) for Europe. It has been observed that this idea implies the need for definition of a clear boundary between medical and fitness/wellness apps [36]. For the Medical and Healthcare Regulatory Agency (MHRA) in England, apps are considered comparable to medical devices depending of the activity they perform (record archiving vs data interpretation; monitoring vs diagnosis) and the level of risk for patient that they represent [1]

Others have suggested that an app review system should be developed to help final users to take informed decision before deciding which app to download and install on their devices. For example, it has been proposed by Boulos et al. [5] that such assessment system should take into account aspects like content quality, usability, device connectivity standards, app security and user privacy. Also, a plethora of app evaluating frameworks exist: Henson et al. [24]

analyzed 45 of them mapping all parameters that they evaluate into a structure of five main levels, that can be used by developers as a guidance. Aspects to be evaluated include (1) background information, (2) privacy and security, (3) evidence based, (4) ease of use and (5) data integration. For what concerns privacy, and in Europe specifically, it is worth mentioning that GDPR has been adopted in the attempt to protect users' privacy and increase control over data uses.

4 CHALLENGES

The IoT might open endless opportunity to healthcare professional and private citizens, but for a large employment it is necessary to address important and different challenges. Despite some approaches that have been proposed, such challenges still hold today. In the following, we highlight the most important ones and related questions that should guide further investigation with the aim to find better solutions.

4.1 Security

A smart object acquires data (e.g., blood pressure, heart rate, etc.) and transmits it to a processing center where data analytics software transforms it into information. Needless to say, in order to transmit this data, the physical object must be connected to a communication network. As a result, like any other device connected to the network, smart objects might become possible targets of attacks that can lead to data loss and/or data manipulation. If we want IoT medical devices to become popular and widespread, a basic requirement to have tangible benefits from network effects, it is necessary to have real-time and secure communications (i.e., no malicious and/or accidental attacks) [4, 7, 13]. One might think that the use of standard security techniques (e.g., cryptography) may be sufficient, but the IoT scenario has peculiar characteristics. Indeed, IoT devices are produced by different manufacturers and have very different features from one another. For example, devices might be active (i.e., devices with batteries such as smartwatches) or passive (devices without batteries such as RFID), communication protocols might have a high consumption of energy (e.g., Wi-Fi) or a low consumption (e.g., bluetooth low energy). Moreover, ensuring security in this scenario means ensuring security from one end (at the sensor side) to the other end (at the processing center) and security means *authentication* (every device involved in the communication must be identifiable), *confidentiality* (only authorized persons must be able to access the data), and *integrity* (the data cannot be modified during their journey to the destination).

4.2 Privacy

In the Internet scenario, the majority of users are increasingly aware of the fact that personal data is often a currency for obtaining free services [18, 21]. For instance, they know that the service provided by a search engine is paid with the knowledge of the keywords they are using; they are aware that the use of a social network is paid with personal data. Even in the mobile environment, there is a growing awareness that the applications that are installed free of charge are paid with personal data (i.e., calling data) and metadata (e.g., location). The IoT health scenario is rather unclear. For example, where do the data collected by wearables go? Certainly, IoT sensors

collect data and transmit it to the application on the smartphone to allow its basic functioning, but does the transmission end there? Or does the data “come out of the phone” to other stakeholders? If a user is willing to share a photo or her geographical location, perhaps she is not as happy if the sharing concerns her own health conditions. More clarity is needed. The terms of use of IoT health devices must be transparent and must explicitly say who has access to the data, who is the owner of the data, who is in control of it. Without this clarity it is likely that in the long run users will begin to look at these devices with great suspicion. If today many users do not share their geographical location, one day they could stop using health applications.

4.3 Integration

IoT is a heterogeneous scenario: many devices, many manufacturers, many communication protocols. The result is a set of devices with very different characteristics. This variety limits the development and adoption of IoT devices. For example, as a final user, how can I be sure that the device I bought to monitor my heart rate is compatible with my smartphone? And, as a producer, what technology should I embed in the device I'm producing so that it does not immediately become obsolete? Having so many different producers trying to impose their standard or their ecosystem does not favor the development of the entire IoT health sector. On the contrary, it slows it down. It is necessary to have a common standard, used by any IoT device. Fortunately, it seems that the scenario is moving in this direction as demonstrated by the Open Connectivity Foundation⁴ initiative that provides an open source IoT framework to produce a connected ecosystem.

4.4 Business Model

Considering how profitable the medical records business is envisaged [38] and the key value personal and medical data represent for a range of sectors from research to health agencies to pharma companies and even marketing and insurance agencies, it is indeed a rightful thinking to suspect a flourishing market for health and fitness data. The growing interest of key players like Apple and Google in the race to healthcare applications is cause of concern for users, that generally distrust companies that are usually and ultimately motivated by profit; even though the great potential in terms of insights that can be obtained from AI and machine learning analysis on health data for the prevention of severe diseases, the eventuality of data being sold to third parties with commercial purposes stresses the necessity of laws that protect patients' right to anonymity and consent handling. Although there are producers who have invested heavily in IoT health (e.g., companies in the fitness sector) there is not a clear business model in the sector. For this reason, many companies are aiming to create their own ecosystem, but the presence of many eco-systems (e.g., Samsung vs. Apple vs. Huawei vs. Google, just to name a few) is slowing down the expansion of the IoT health sector. Indeed, other manufacturers are afraid to enter the market as the uncertainty about the return on investment limits their investments. It is undeniable that the development of a solid business model cannot take place until the problems highlighted above are present. Once security, privacy and

⁴<https://openconnectivity.org/>

integration are guaranteed, then it will be possible to think of a solid business model. Until then, we will have to settle for companies that seek to dominate the market or to visionary entrepreneurs who are trying to break the domain of a few.

5 CONCLUSIONS

IoT applied to personal and public health is certainly a fascinating scenario. On the web, there are many examples of the wonders that can be achieved by connecting simple sensors to the human body. This new computational paradigm is about to change health prevention and patient's treatment but is about to revolutionize the entire health industry composed of pharmaceutical companies, research centers, insurance agencies, hospital centers, public health, and personal health. Everything is changing, but not each new product, service or device necessarily contributes thing moves towards a better scenario. On the horizon there are a lot of dark clouds: security, privacy, interoperability, business models are some aspects that can jeopardize the benefits that IoT health can bring to our society. In this paper, we have tried to shed light on unconsidered aspects of this new and promising scenario that could bring benefits to the whole society, if it is not compromised by the greed of some companies willing to do anything for profits, and we underlined the need for policies and standards for industries and developers, along with more transparency towards final users.

REFERENCES

- [1] Regulatory Agency. 2018. Medical devices: software applications (apps). *Medicines and Healthcare products. Regulatory Agency*. Available at: <https://www.gov.uk/government/publications/medical-devices-software-applications-apps> (2018).
- [2] Shifali Arora, Jennifer Yttri, and Wendy Nilsen. 2014. Privacy and Security in Mobile Health (mHealth) Research. *Alcohol Res* 36, 1 (2014).
- [3] Nicolai Bodemer, Stephanie M. Müller, Yasmina Okan, Rocio Garcia-Retamero, and Angela Neumeyer-Gromen. 2012. Do the media provide transparent health information? A cross-cultural comparison of public information about the HPV vaccine. *Vaccine* 30, 25 (2012), 3747 – 3756. <https://doi.org/10.1016/j.vaccine.2012.03.005> Special Issue: The Role of Internet Use in Vaccination Decisions.
- [4] Luciano Bononi, Lorenzo Donatiello, and Marco Furini. 2009. Real-Time Traffic in Ad-Hoc Sensor Networks. In *Proceedings of IEEE International Conference on Communications (ICC)*. 1–5.
- [5] Maged Kamel Boulos, Ann Brewer, Chante Karimkhani, David Buller, and Robert Dellavalle. 2014. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. *Online Journal of Public Health Informatics* 5, 3 (2014). <https://doi.org/10.5210/ojphi.v5i3.4814>
- [6] Armir Bujari, Marco Furini, Federica Mandreoli, Riccardo Martoglia, Manuela Montangero, and Daniele Ronzani. 2018. Standards, Security and Business Models: Key Challenges for the IoT Scenario. *Mobile Networks and Applications* 23, 1 (01 Feb 2018), 147–154. <https://doi.org/10.1007/s11036-017-0835-8>
- [7] Marco Conti, Lorenzo Donatiello, and Marco Furini. 2002. Design and Analysis of RT-Ring: a protocol for supporting real-time communications. *IEEE Transaction on Industrial Electronics* 49, 6 (December 2002), 1214–1226.
- [8] Xiaohui Cui, Nanhai Yang, Zhibo Wang, Cheng Hu, Weiping Zhu, Hanjie Li, Yujie Ji, and Cheng Liu. 2015. Chinese social media analysis for disease surveillance. *Personal and Ubiquitous Computing* 19, 7 (01 Oct 2015), 1125–1132.
- [9] Munmun De Choudhury. 2014. Opportunities of Social Media in Health and Well-being. *XRDS* 21, 2 (Dec. 2014), 23–27. <https://doi.org/10.1145/2676570>
- [10] Giovanni Delnevo, Silvia Mirri, Lorenzo Monti, Catia Prandi, Manesha Putra, Marco Rocchetti, Paola Salomoni, and Robert J. Sokol. 2018. Patients Reactions to Non-Invasive and Invasive Prenatal Tests: A Machine-Based Analysis from Reddit Posts. In *IEEE/ACM 2018 International Conference on Advances in Social Networks Analysis and Mining*. 980–987. <https://doi.org/10.1109/ASONAM.2018.8508614>
- [11] G. Delnevo, M. Rocchetti, and S. Mirri. 2018. Modeling Patients' Online Medical Conversations: A Granger Causality Approach. In *International Conference on Connected Health: Applications, Systems and Engineering Technologies*. 40–44.
- [12] Deloitte. 2019. Global Health Care Outlook. In *Research Report*. Available at: <https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/global-health-care-sector-outlook.html>.
- [13] Lorenzo Donatiello and Marco Furini. 2003. Ad Hoc Networks: A Protocol for Supporting QoS Applications. In *Proceedings of the 17th International Parallel and Distributed Processing Symposium (IPDPS 2003)*. IEEE, New York.
- [14] Mark Dredze, Zachary Wood-Doughty, Sandra Crouse Quinn, and David A. Broniatowski. 2017. Vaccine opponents' use of Twitter during the 2016 US presidential election: Implications for practice and policy. *Vaccine* 35, (2017).
- [15] Stefano Ferretti, Marco Furini, and Manuela Montangero. 2019. Diabetes: what are Italian Twitter users talking about?. In *Proceedings of the IEEE International Conference on Computer Communications and Networks*.
- [16] Jim Finkle and Caroline Humer. 2014. Community Health says data stolen in cyber attack from China. *Reuters*. Available at: <https://www.reuters.com/article/us-community-health-cybersecurity/community-health-says-data-stolen-in-cyber-attack-from-china-idUSKBN0G16N20140818> (2014).
- [17] Susannah Fox. 2014. The social life of health information. *Pew Research* (Jan. 2014).
- [18] Marco Furini. 2014. Users Behavior in Location-aware Services: Digital Natives vs Digital Immigrants. *Advances in Human-Computer Interaction* 2014 (2014).
- [19] Marco Furini, Federica Mandreoli, Riccardo Martoglia, and Manuela Montangero. 2017. *IoT: Science Fiction or Real Revolution?* Springer International Publishing, Cham, 96–105. https://doi.org/10.1007/978-3-319-61949-1_11
- [20] Marco Furini and Gabriele Menegoni. 2018. Public Health and Social Media: Language Analysis of Vaccine Conversations. In *Proceedings of the ACM/IEEE International Conference on Internet of Things Design and Implementation*.
- [21] Marco Furini and Valentina Tamanini. 2015. Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications* 74, 21 (2015), 9795–9825. <https://doi.org/10.1007/s11042-014-2151-7>
- [22] Andrea L. Hartzler, Bridget Weis, Carly Cahill, Wanda Pratt, Albert Park, Uba Backonja, and David W. McDonald. 2016. Design and Usability of Interactive User Profiles for Online Health Communities. *ACM Trans. Comput.-Hum. Interact.* 23, 3 (2016).
- [23] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky. 2015. Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System. *IEEE Transactions on Parallel and Distributed Systems* 26, 11 (Nov 2015), 3108–3121.
- [24] Philip Henson, Gary David, Karen Albright, and John Torous. 2019. Deriving a practical framework for the evaluation of health apps. *The Lancet Digital Health* 1 (2019). [https://doi.org/10.1016/S2589-7500\(19\)30013-5](https://doi.org/10.1016/S2589-7500(19)30013-5)
- [25] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak. 2015. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* 3 (2015), 678–708. <https://doi.org/10.1109/ACCESS.2015.2437951>
- [26] C. Kotronis, G. Minou, G. Dimitrakopoulos, M. Nikolaidou, D. Anagnostopoulos, A. Amira, F. Bensaali, H. Baali, and H. Djelouat. 2017. Managing Criticalities of e-Health IoT systems. In *2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB)*. 1–5. <https://doi.org/10.1109/ICUWB.2017.8251004>
- [27] D. Kotz. 2011. A threat taxonomy for mHealth privacy. In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*. 1–6.
- [28] J. Sathish Kumar and Dhiren R. Patel. 2014. Article: A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications* 90, 11 (March 2014), 20–26. Full text available.
- [29] H. Lin, J. Jia, J. Qiu, Y. Zhang, G. Shen, L. Xie, J. Tang, L. Feng, and T. Chua. 2017. Detecting Stress Based on Social Interactions in Social Networks. *IEEE Transactions on Knowledge and Data Engineering* 29, 9 (Sept 2017), 1820–1833. <https://doi.org/10.1109/TKDE.2017.2686382>
- [30] Jian Mou, Dong-Hee Shin, and Jason F. Cohen. 2017. Tracing College Students' Acceptance of Online Health Services. *International Journal of Human-Computer Interaction* 33, 5 (2017), 371–384. <https://doi.org/10.1080/10447318.2016.1244941>
- [31] Yvonne O'Connor, Wendy Rowan, Laura Lynch, and Ciara Heavin. 2017. Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science* (2017). <https://doi.org/10.1016/j.procs.2017.08.329> International Conference on Emerging Ubiquitous Systems and Pervasive Networks.
- [32] A. B. Pawar and S. Ghumbre. 2016. A survey on IoT applications, security challenges and counter measures. In *International Conference on Computing, Analytics and Security Trends*.
- [33] Koustuv Saha and De Choudhury Munmun. 2017. Modeling Stress with Social Media Around Incidents of Gun Violence on College Campuses. *Proc. ACM Hum.-Comput. Interact.* 1 (2017). <https://doi.org/10.1145/3134727>
- [34] Reijo M. Savola, Habtamu Abie, and Markus Sihvonen. 2012. Towards Metrics-driven Adaptive Security Management in e-Health IoT Applications. In *Proceedings of the 7th International Conference on Body Area Networks*. 276–281.
- [35] Michael Schukat, D McCaldin, Kai Wang, Günter Schreier, Nigel H. Lovell, Michael Marschollek, and Stephen James Redmond. 2016. Unintended Consequences of Wearable Sensor Use in Healthcare. *Yearbook of medical informatics* 1 (2016), 73–86.
- [36] Eliza Strickland. 2012. The FDA Takes On Mobile Health Apps. *IEEE Spectrum* (2012).
- [37] Atif Sulleyman. 2017. NHS Cyber Attack: why stolen medical information is so much more valuable than financial data. *Indepented*.
- [38] A. Tanner. 2017. *Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records*. Beacon Press.