IRIE
International Review of Information Ethics Vol. 22 (12/2014)

Kashif Habib:

Ethical Aspects of the Internet of Things in eHealth

Abstract:

While the current Internet has brought comforts in our lives, the future of the Internet that is the Internet of Things (IoT) promises to make our daily living even much easier and convenient. The IoT presents a concept of smart world around us, where things are trying to assist and benefit people. Patient monitoring outside the hospital environment is one case for the IoT in healthcare. The healthcare system can get many benefits from the IoT such as patient monitoring with chronic disease, monitoring of elderly people, and monitoring of athletes fitness. However, the comfort may bring along some worries in the form of people's concerns such as right or wrong actions by things, unauthorised tracking, illegal monitoring, trust relationship, safety, and security. This paper presents the ethical implications of the IoT in eHealth on people and society, and more specifically discusses the ethical issues that may arise due to distinguishing characteristics of the IoT.

Agenda:

Author:

Kashif Habib

- Norsk Regnesentral/Norwegian Computing Center,
  P.O. Box 114 Blindern, NO-0314 Oslo, Norway
- ☎ + 47 - 22 85 25 00 , ✉ Kashif.Sheikh@nr.no, 💻 www.nr.no

Acknowledgment

The work presented here has been carried out in the research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway. The author would like to thank Sven Arntzen, Arild Torjusen, and Wolfgang Leister for their comments and for helpful discussions.

Introduction

The IoT envisions merging the physical world with the digital world. The IoT provides new ways of communication between people and things and between things themselves. According to CISCO systems, the IoT combines data, people, processes, and things together to enrich the networked connectivity[1]. The IoT is a network of interconnected things such as sensors, Near Field Communication (NFC) tags, Radio Frequency Identification (RFID) tags, actuators, smartphones, tablets, computers, etc. In the IoT, all kind of things will exchange information[2], work in synergy[3], and embed real world information into networks[4]. Communication and the capability to perceive information from surroundings can provide many benefits to domains like transportation, healthcare, personal, social, home, office and industry[5].

In this article, we highlight the ethical implications of the IoT in eHealth on people and society, and more specifically discusses the ethical issues that may arise due to distinguishing characteristics of the IoT.

IoT in eHealth

Patient monitoring outside the hospital environment is one case for the IoT in healthcare[6]. While monitoring patient's health parameters with on-body sensors, the IoT may allow a patient to be at different locations such as home, office, public place, or in a vehicle but medical sensors still connected and transmitting information to the doctor's office. The healthcare system can get many benefits from the IoT, such as patient monitoring with chronic disease, monitoring of elderly people, monitoring of athletes fitness, and in terms of getting quick medical response from the medical practitioner while suffering from intense condition.

The main objective of the IoT in eHealth system is to assist the existing healthcare system by monitoring the vital signs of patient's health data in real time. From systems point of view, complete and accurate information transfer from a patient to the medical centre is always necessary. Failure to do so may cause a threat to the patient's life. Also, other people with bad intentions can send wrong data to the hospital by miss utilising the devices. Transferring a patient's health data to a remote medical centre opens for security threats that may impact the patient's privacy and trust, confidentiality of data transmission, integrity of received data, and data availability. Patient's privacy and trust are certainly the important challenges in the deployment of patient monitoring system. Although, trust can be defined[7] for different purposes and application areas in several disciplines, one way of defining trust in the eHealth system is simple. If the patient monitoring system can ensure that the patient's data is used and accessible by only authorised users and system interruption may not endanger patient's life or lead into wrong treatment, then it may serve the purpose. Protection, safety, privacy, and trust establishment in the IoT in eHealth is a major challenge due to the dynamic and complex nature of the system. In such systems, safety and privacy requirements are affected by the changes in the internal and external conditions of the system.

[1] Evans, D.: Internet of Everything (IoE), CISCO Blogs, (2013), http://blogs.cisco.com/ioe/.

[2] Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S.:Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, (2010) 1-236.

[3] Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, (2010) 1-73.

[4] Vermesan, O. et al.: Internet of Things Strategic Research Roadmap 2011, European Research Cluster on the Internet of Things, (2011) 1-44.

[5] Atzoria, L., Ierab, A., Morabito, G.: The Internet of Things, A survey, Computer Networks (54), (2010) 2787-2805.

[6] Habib,K., Torjusen,A., and Leister, W.: A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth,(2014) 32-37.

[7] Leister,W., and Schulz, T.:Ideas for a trust indicator in the Internet of Things, (2012), 31-34.

Ethical Issues

With the passage of time, science and technology have a greater impact and influence on human lives that seems a strong case in the IoT as well. Ethics can be considered to be the systematic theory about moral principles, values and codes. The word ethics comes from the Greek word ethos that can mean beliefs, customs, and character. It is very often interchangeably used with the term morals, beliefs or principles as well. At the same time, when we hear the word ethics automatically we think about rules that would distinguish right from wrong. The ethical theories can be considered as guidelines for people to behave rationally and according to moral values. The ethical theories can help us in many ways, such as understanding of right versus wrong, acknowledging moral values, our moral responsibilities, awareness of our own actions, and who and how people can be affected by our actions. Uses of Information and Communication Technologies (ICT) are usually actions that belong to a traditional repertoire of human action; with ICT traditional actions can be performed much more efficiently and relatively independently of previous constraints in space and time. At the same time, this is conducive to the individual losing sight of what he/she is actually doing, which is a condition for being a moral agent, charged with ethical responsibility. The IoT may embed the technology in the environment in such a way that in many cases the user may even not know that he/she is interacting with technology.

The comfort may bring along some worries in the form of people's concerns regarding ethical issues such as right or wrong actions by things implicating into their privacy breach, unauthorised tracking, illegal monitoring, trust relationship, safety, and security. Weiser in his seminal paper argued[8]:

> *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".*

The IoT envisages a deeply interconnected world beyond our imagination. The technological developments for the IoT are quite visible but ethics seems to be supressed. This is truly reflected in a quote by Ernest Benda[9]:

> *"The problem is the possibility of technology taking on a life of its own, so that the actuality and inevitability of technology creates a dictatorship. Not a dictatorship of people over people with the help of technology, but a dictatorship of technology over people".*

If we look at the technological developments in the recent past, we observe that technology helps us accomplishing complex task in a simpler and efficient manner. In a way, technology has become inevitable for us because people mostly think in terms of involving any available technology to help them doing their tasks. In the IoT, it is expected that billions of devices connected to the Internet will easily out number many times the total human population on earth. In such situation, technology not only becomes inevitable for people but also their daily living may be dictated according to the advancements in technology.

[8] Weiser, M.: The Computer for the 21st Century. Scientific American, vol. 265, no. 3, (1991) 66-75.

[9] Benda, E.: German Federal Constitutional Court (Chief Justice), on the court's decision to stop the 1983 census and create the novel basic right on 'Informational Self- Determination'. Cited by Rob Van Kranenburg, Ethics Report Venice IoT week, (2012).

Ethical Assessment

Accessing the ethical aspects of the IoT for technologist can be a challenging task. One can use analytic approach of philosophy to understand the moral problems of the technology[10]. While accessing the ethical aspects of the IoT in eHealth, the questions presented by Mason et. al. can give good focus to ethical reasoning[11]:

> *"(a) Who is the agent? (b) What action was taken or is being contemplated? (c) What are the results or consequences of that action? (d) Are those results fair or just?"*

We present the distinguishing characteristics of the IoT that may help us to answer the above questions. The IoT is characterised by some distinguishing features[12], such as heterogeneous, ubiquitous, anonymous, dynamism, intelligence, communication, distributed environment, uncertainty, autonomous, miniaturisation, and virtual identities, etc. The fundamental characteristics of the IoT are interconnectivity between things, things-related services within the constraints of things, dynamic changes in the environment and in the state of devices, and heterogeneity. The high level requirements for the IoT are identification-based connectivity, autonomic networking, autonomic service provisioning, location based capabilities, privacy protection, and security[13]. In the rest of this section, we put forward and analyse the ethical implications of specific features and characteristics of the IoT in the eHealth domain.

Heterogeneous

The IoT in eHealth can establish a heterogeneous network environment connecting things (sensors, smartphones, tablets, computers, etc.) using various operating systems, hardware, software, and protocols across multiple networks. In such a heterogeneous environment, sometimes network boundaries may become unknown making linkability a major ethical concern. Linkability here means to associate information with specific thing in the IoT. For instance, difficulties in terms of knowing about data linkability may result in deniability or non-repudiation by things. In order to strengthen the accountability mechanisms in the IoT, a comprehensive identity management system may counter the problem.

Ubiquitous

The IoT in eHealth envisions a ubiquitous environment providing anytime and everywhere connectivity concept for things. Due to ubiquity, things can be vulnerable against misuse cases of monitoring, tracking, and marketing technologies. Imagine a scenario where our personal belongings (things) equipped with electronic tags and sensors communicating with other things. For instance, medical sensors attached to a patient's body transmitting health parameters, communicating with our personal belongings in handbag. Although electronic tags and sensors may bring comfort in our lives but it may reveal our personal information and thus affecting privacy.

Anonymous

Anonymity refers to namelessness. Although anonymity can be quite useful to address privacy and confidentiality issues for the IoT in eHealth, but at the same time it may create accountability issues. Anonymity may allow bad people to hide themselves by masking their identities. Cyber bullying is an important ethical aspect related to anonymity. Although face-to-face interactions has been an accepted practice in societies to establish trust among people, but at the same time anonymity can be used as a tool in undemocratic societies to express views anonymously that may save lives. However, people with bad intentions may exploit anonymity feature

[10] Helping ICT professionals to assess ethical issues in new and emerging technologies, http://www.bcs.org/upload/pdf/assessing-ethical-issues.pdf.

[11] Mason, R., Mason, F., Culnan, M.: Ethics of Information Management, SAGE series on business ethics, vol.2 (1995).

[12] Hoven, J. V. D.: Fact sheet- Ethics Subgroup Internet of Things - Version 4.01, Delft University of Technology, European commission (2012) 1-21.

[13] Recommendation ITU-T, Y.2060, Overview of Internet of Things, 06/2012.

to hide themselves while trying to harm patients in an eHealth system. Hence, anonymity is a challenge and a trade-off for the standard making organisations.

Dynamism

The IoT in eHealth can be considered dynamic not only in terms of its underlying technologies but also in terms of data sources, patient's behaviour, environment, and applications. The dynamic features of the IoT creates dynamic environment that demands the ethical considerations to be dynamic as well. In our opinion, context awareness becomes a key factor in such dynamic environment to understand the ethical implication of a particular action. For instance, if we treat some action ethically correct in a particular context, but due to dynamic network environment and changed context that same action can turn into an unethical action. To further illustrate the case, we consider remote patient monitoring scenario in the IoT, where sensors are attached to a patient's body monitoring health parameters. Suppose two patients 1 and 2 are in close vicinity to each other at some place. In a general context, the communication between the sensors of these patients may be treated ethically wrong due to the privacy concerns of patients. However, if the sensors of patient 1 are unable to transmit data due to low battery power or transmission may lead to further drain in battery. In such context, the sensors of patient 1 may send data through the sensors of patient 2. Due to the changed context, this action may now be treated ethically correct provided the sensitivity of not transmitting the data at all. The situation can become more complex if sensors of patient 1 cause battery drain of patient 2 sensors, resulting in no transmission of own data.

Intelligence

Embedding intelligence into things enables the IoT to turn an ordinary object into a smart thing. The smart things in the IoT may create a smart eHealth system. Due to the inflow of smart technologies, patients may find themselves restrain by the technology confining their freedom. Although smart things may help patients to overcome the barriers of time and place in accomplishing a task, but the smart things also have monitoring and recording capabilities. The actions of patients including their movements, purchases, browsing habits, and work habits may be somehow recorded. This implies that actions may become traceable leading into privacy issues or invading patient's freedom.

Communication

Anytime and anywhere connectivity concept in the IoT demands successful transfer of patient's information. The smart things may generate huge amount of patient's data. The usual way to protect confidentiality of the sensitive information is to use suitable security mechanisms. However, things in the IoT have resource constraints and implementing complex security mechanisms can be cumbersome. Thus, communication requirements sometimes may force to compromise on security requirements. Such cases can be disastrous for privacy and confidentiality concerns of a patient. For instance, to address confidentiality, encryption is a popular technique for which there are number of good cryptographic algorithms already available. Mostly the strength of such algorithms relies upon the complexity, and size of cryptographic keys. However, things in the IoT have constraints in terms of energy, processing power, and storage capacity. Thus, sometimes it may be difficult to use these algorithms that may result in a compromise of privacy or confidentiality of a patient.

Distributed Environment

The huge amount of patients' data, large number of things, and mobility features envisage a distributed environment in the IoT. The governance and management of distributed environment can be a challenging task to hold someone responsible for a particular action. The distributed environment in the IoT may pose several challenges while holding someone responsible for several actions such as, modification of software or firmware causing harm to a patient's data and system, illegal retrieval of patient's data, and unauthorised access to remote medical system. Hence, the accountability mechanism is a key to tackle non-repudiation related issues[14].

Uncertainty

The complex environment of the IoT can raise many uncertainties in the mind of patients. Patients may not be certain about the flow and handling of their information. When a remote medical centre receives patient's data, uncertainty about data origin, and uncertainty regarding data correctness. Patients may be uncertain regarding with whom and what information is shared. The uncertainty about unknown surveillance may cause discomfort and uneasiness to patients in their freedom of movement.

Autonomous

The smart things in the IoT may not only interact with patients but also autonomously exchange information among them. Things may also react autonomously to the events with or without direct involvement of patients. The autonomous act of smart things may affect the moral rights and obligations of patients. For instance, when things do the shopping by themselves such as, photocopying machine orders the papers itself or a doll orders its new cloths autonomously[15]. Similarly, smart things may order unnecessary stuff that can have monetary damage for patients. To fix the responsibility of business transaction in such cases can be a challenging problem.

Miniaturisation

The miniaturisation of computer technology in the IoT will possibly integrate the smart objects much more into our daily living. The traditional computer technology may vanish due to miniaturisation in technology. Somehow we will be in a scenario where patients communicate with smart objects and smart objects communicating with each other. This kind of environment may have social implications on society such as transparency, dependability, acceptability, accountability, and reliability. For instance, consider a surveillance case in the IoT. The miniaturisation in technology has already produced nearly invisible cameras that bring forward an interesting question: "How much 'life logging' could you tolerate[16]?"

Virtual identities

In the IoT, unique identification number of things embedded in invisible tags would allow consumers to access the virtual representation of things in information world. This information world could provide information to the user about thing such as product review, ingredients, and links to the shop selling the item. Things will be identified by virtual identities, whether such things are people, device, software, or a service. The digital representation of things will be in the form of virtual identity where things may have many virtual identities representing various personas and aspects of their services. According to Roman[17] et. al.:

> *"In the IoT vision, every physical object has a virtual component that can produce and consume services. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use".*

In our opinion, it is very important to consider that, what implications it may have when patients interact with machines instead of with people even without knowing it.

[14] Xiao, Z., Kathiresshan, N., Xiao, Y.: A survey of accountability in computer networks and distributed systems Security and Communication Networks, John Wiley & Sons, Ltd, (2012) 1-26.

[15] Bohn, J., CoroamÄƒ, V., Langheinrich, M., Mattern, F., Rohs, M., Weber, W., Rabaey, J., Aarts, E. (Eds.) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing Ambient Intelligence, Springer Berlin Heidelberg, (2005) 5-29.

[16] Hudson, A.: How much 'life logging' could you tolerate? BBC click, (2013), http://www.bbc.co.uk/news/technology-22193299.

[17] Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer, vol. 44, no. 9, (2011) 51-58.

Ethical Discussion

The IoT presents the concept of smart world through the integration of smart objects into our daily living, such as smart cities, smart environment, smart logistics, smart industrial control, smart agriculture, smart animal farming, and smart e-Health. Here, the term smart refers to an environment where things have certain capabilities such as sensing, monitoring, computing, intelligence, and decision making. These applications can help us in effective energy management, enhanced healthcare, and more independent living. On the other hand, if we look closely at these environments, we see sensors monitoring and collecting bundles of data that have many identity and privacy based implications. Gérald Santucci in his speech on the governance of the IoT said[18]:

> *"In the future, the right to privacy, whatever we do to implement it with technology and/or regulations ("right to be forgotten", "right to oblivion", "right to silent chips", etc.), will become a subset of ethics. The future is (largely) about ethics-by-design".*

Rafael Capurro and Michael Nagenborg performed ethical evaluation of European institutes to estimate the likelihood of ethical issues due to emerging information and communication technologies[19]. Amongst their findings they indicated the potential conflict with the values and principles of EU charter, the opinion of European group on ethics in science and new technologies, other national bio-ethics committees, and other official EU documents. They included human dignity, freedom of research, privacy, and justice for their analysis. They concluded that emerging technologies have high likelihood of becoming an ethical issue such as ambient intelligence, human machine symbiosis, neuro electronics, robotics, affective computing, artificial intelligence, and bioelectronics. Interestingly all of these technologies are part of the IoT. They also highlighted the lack of ethical research on animals and environment as they think that the recent efforts are mainly human centred.

However, many professional societies, organisations, and technology related standard making organisations consider ethics as an essential element in technology development as it is reflected in their code of ethics. In the IEEE (Institute of Electrical and Electronics Engineers) code of ethics[20], they commit themselves, "to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment; to improve the understanding of technology; it's appropriate application, and potential consequences; or after full disclosure of pertinent limitations; to seek, accept, and offer honest criticism of technical work; to acknowledge and correct errors, and to credit properly the contributions of others; to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin". Also, according to the ACM (Association for Computing Machinery) code of ethics[21] and professional conduct, "avoid harms to others, be fair and take action not to discriminate, respect the privacy of others, and honour confidentiality".

An important aspect inside the IoT objective is to narrow the rich and poor gap[22]. That implies that the opportunity to access the IoT must not treat rich and poor differently. However, there are countries where families will have difficulties to afford the smart devices. The inability to purchase smart devices may keep them away from the goods of the IoT.

[18] Kranenburg, R. J., Jaromil D. R., Carrez, F.: The Internet of Things Initiative (2012) 1-66. http://www.iot-i.eu/public/public-deliverables/d2.5-ethicsinside.eu/at_download/file.

[19] Carsten, B. S.: Ethical issues of emerging ICT applications, the magazine of the European innovation exchange, issue 6, (2011) 1-36, http://www.ethics.ccsr.cse.dmu.ac.uk/etica/EIEX06ETICA2.pdf.

[20] IEEE Code of Ethics. (2006), http://www.ieee.org/about/corporate/governance/p7-8.html.

[21] ACM Code of Ethics and Professional Conduct, (2013), http://www.acm.org/about/code-of-ethics/#sect1.

[22] The Internet of Things. https://sites.google.com/a/cortland.edu/the-internet-of-things.

Conclusion

The future of the current Internet is the Internet of highly connected digital world where patients will be fenced by tiny smart things. In such an environment the actions taken by things to comfort a patient may have serious ethical implications as well. While people are keen to develop standards and technologies for the IoT, the ethical aspects of these developments must not be ignored for later analysis rather it may be incorporated in the system development life cycle. The claimed benefits of the IoT may not be realised, unless ethical implications of such claims on people, society, and environment are justified. Also, there is a strong need to formulate solutions to potential ethical issues in the IoT before it is irreversibly adopted by society.

References

Evans, D.: Internet of Everything (IoE), CISCO Blogs, (2013), http://blogs.cisco.com/ioe/.

Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S.:Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, (2010) 1-236.

Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, (2010) 1-73.

Vermesan, O. et al.: Internet of Things Strategic Research Roadmap 2011, European Research Cluster on the Internet of Things, (2011) 1-44.

Atzoria, L., Ierab, A., and Morabito, G.: The Internet of Things, A survey, Computer Networks (54), (2010) 2787-2805.

Habib, K., Torjusen, A., and Leister, W.: A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth, (2014) 32-37.

Leister,W., and Schulz, T.:Ideas for a trust indicator in the Internet of Things, (2012), 31-34.

Weiser, M.: The Computer for the 21st Century. Scientific American, vol. 265, no. 3, (1991) 66-75.

Benda, E.: German Federal Constitutional Court (Chief Justice), on the court's decision to stop the 1983 census and create the novel basic right on 'Informational Self- Determination'. Cited by Rob Van Kranenburg, Ethics Report Venice IoT week, (2012).

Helping ICT professionals to assess ethical issues in new and emerging technologies, http://www.bcs.org/upload/pdf/assessing-ethical-issues.pdf.

Mason, R., Mason, F., Culnan, M.: Ethics of Information Management, SAGE series on business ethics, vol.2 (1995).

Hoven, J. V. D.: Fact sheet- Ethics Subgroup Internet of Things - Version 4.01, Delft University of Technology, European commission (2012) 1-21.

Recommendation ITU-T, Y.2060, Overview of Internet of Things, 06/2012.

Xiao, Z., Kathiresshan, N., and Xiao, Y.: A survey of accountability in computer networks and distributed systems Security and Communication Networks, John Wiley & Sons, Ltd, (2012) 1-26.

Bohn, J., CoroamÄƒ, V., Langheinrich, M., Mattern, F., Rohs, M., Weber, W., Rabaey, J., and Aarts, E. (Eds.) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing Ambient Intelligence, Springer Berlin Heidelberg, (2005) 5-29.

Hudson, A.: How much 'life logging' could you tolerate? BBC click, (2013), http://www.bbc.co.uk/news/technology-22193299.

Roman, R., Najera, P., and Lopez, J.: Securing the Internet of Things. Computer, vol. 44, no. 9, (2011) 51-58.

Kranenburg, R. J., Jaromil D. R., and Carrez, F.: The Internet of Things Initiative (2012) 1-66. http://www.iot-i.eu/public/public-deliverables/d2.5-ethicsinside.eu/at_download/file.

Carsten, B. S.: Ethical issues of emerging ICT applications, the magazine of the European innovation exchange, issue 6, (2011) 1-36, http://www.ethics.ccsr.cse.dmu.ac.uk/etica/EIEX06ETICA2.pdf.

IEEE Code of Ethics. (2006), http://www.ieee.org/about/corporate/governance/p7-8.html.

ACM Code of Ethics and Professional Conduct, (2013), http://www.acm.org/about/code-of-ethics/#sect1.

The Internet of Things. https://sites.google.com/a/cortland.edu/the-internet-of-things.