Framework for Dependable and Pervasive eHealth Services

Ulrico Celentano and Juha Röning
Biomimetics and Intelligent Systems Group
University of Oulu
Oulu, Finland
{ulrico.celentano,juha.roning}@ee.oulu.fi

***Abstract*—Provision of health care and well-being services at end-user residence, together with its benefits, brings important concerns to be dealt with. This article discusses selected issues in dependable pervasive eHealth services support.**

Dependable services need to be implemented in a resource-efficient and safe way due to constrained and concurrent, pre-existing conditions and radio environment. Security is a must when dealing with personal information, even more critical when regarding health. Once these fundamental requirements are satisfied, and services designed in an effective manner, social significance can be achieved in various scenarios. After having discussed the above viewpoints, the article concludes with the future directions in eHealth IoT including scaling the system down to the nanoscale, to interact more intimately with biological organisms.

***Index Terms*—Dependability; diagnostics; inclusive health care; nanoscale; preventative health care; privacy; remote patient monitoring; resource use efficiency; robustness; safety; security; treatment.**

I. Introduction

Internet of things (IoT) technologies have huge potential for realizing the supporting solutions for provision of remote health care, sometimes termed as eHealth, or mHealth when mobile devices are involved. Compared with other IoT application scenarios, eHealth services require additional, critical requirements to be met. Some of them are discussed in this article, leading to a discussion of the social significance of eHealth services.

Fig. 1 depicts our example eHealth system where the key players and the relevant issues discussed in this paper are represented. At user's residence is deployed a multi-sensor system. Sensors, wearables or not, are used to monitor medical data such as blood pressure, blood glucose level, blood oxygen saturation or body temperature, and may include electrocardiogram (ECG), electromyogram (EMG) or electroencephalogram (EEG), or video-based inspection of retina. Other sensors may be used to track physical activity including falls and sleep, or to follow medications intake (e.g., by using radio-frequency identification, RFID, or quick response technologies, QR-codes). In addition, self-assessment reports may also be gathered, and remote home diagnostics (furniture sensors, videocameras) for detection of abnormal conditions and anomalies may be added. Information is gathered by caregivers and personnel and/or machines at hospitals, where the conditions are tracked, and from where coaching, counseling and treatments may be administered. For all this, health care sites make use of data repositories. Externally to the health care ecosystem (dash-lined box in Fig. 1), are other players that are potentially interested in health data, of use in forensics for investigations, or in smart insurance industry to customize rates, for example, or also part of governmental institutions to follow population well-being level.

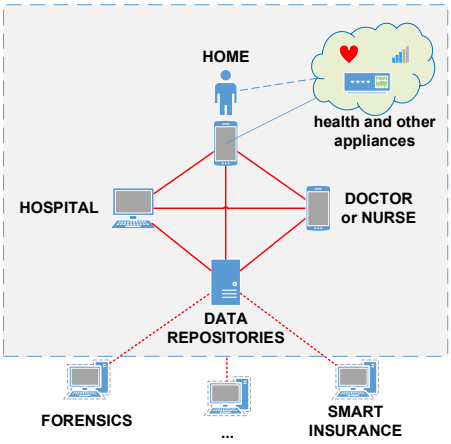

Fig. 1. An example eHealth system with its key internal and additional external players.

An architecture for knowledge integration for such a multi-sensor system is proposed in [1].

Two important nonfunctional requirements, dependability of the health care system ("how") and privacy of user sensitive data ("what"), are discussed in the following. Together with the necessary functional requirements they allow building an effective system, as discussed later.

Thorough surveys exist in the literature. For example, [3] identifies features and services that IoT health care may provide, as well as reports on current industry visions and some proposed architectures and candidate supporting technologies. Reference [4] also addresses tools and technologies services, going deeper into how they can provide the target services, including decision-making over gathered data. Book chapters [5] and [6] report about outcomes from European Union (EU) projects about security and privacy in IoT. We do not repeat such a review but focus on critical hard and soft enablers

of IoT health care: security, in particular privacy, and social aspects.

The rest of the article is structured as follows. Sect. II briefly discusses some dependability issues in pervasive health care. Among them, privacy is more deeply addressed in Sect. III, where also design options and constraints are discussed. To fully empower the IoT health care, its services need to be effectively adopted. Sect. IV moves the discussion to the related softer requirements. In Sect. V the social significance IoT health care may achieve once all the previous requirements are met is discussed. Sect. VI looks into the advances in both communication technology and biology when moving to the nanoscale, and the related openings offered to both diagnostics and treatment. Finally, Sect. VII draws the conclusions and summarizes this article.

II. Safety and Dependability

As depicted at the top of Fig. 1, an eHealth system may include wireless communication technologies, for local (WiFi, Bluetooth, etc.) and/or remote connectivity (cellular, satellite, etc.). An important problem is to ensure smooth coexistence of all these concurrent radio technologies, avoiding any form of interference in uncontrolled, heterogeneous operating environments, such as homes and emergency sites, as well as any detrimental effects with on-body or in-body sensors. All radio devices are expected to be compliant to relevant regulations and in principle (or, in ideal conditions) there should be no problems with their coexistence. However, for critical applications such as health care, also abnormal conditions should be expected and anticipated. For example, a malfunctioning device may emit a power larger than allowed and sensitive devices should be protected, with proactive or reactive safety solutions, sensing and possibly controlling those potentially harmful devices [7, e.g.].

As an IoT system includes battery-operated and otherwise resource-constrained devices, resource use (including spectrum and electrical energy) efficiency is among the vital requirements. Energy efficiency design must be applied at circuital, protocol, topology and architecture levels, by targeting the maximization of the lifetime of the entire system.

All the dependability measures discussed above contribute to ensuring safe operations and improving system robustness.

For eHealth IoT system, resource use efficiency should be pushed as far as possible, both for anticipating abnormal conditions, see above, and, as it has been observed [1], to bring room for the necessary security overheads. This crucial aspect of dependability is covered in more detail in the following section.

III. Privacy and Security

Gathering medical personal data at health centers is a regular practice to which are associated established protocols, such as informed consent retrieval from the subjects under analysis. However, the collection of such data from distributed, remote, and potentially unprotected sites is a relatively new problem. Although with another scope and with a different target for the gathered information, eHealth systems share some similarities with online social networks. In both cases, information from a remote point is fed to an external system and in both cases sensitive information needs to be shared to some extent in order to use the service. By combining the learnt lessons and experience in these two fields and further developing the practices, suitable protocols can be specified.

In any case, privacy by design (preventative) is a better approach than the addition of patches (remedial): these important questions must be addressed as early as possible in the system design phase.

The EU is dealing with legal issues regarding data analysis [8, e.g.]. Modifying a definition in [8], data analysis can be defined as "the automated processing of materials, which may include digital or digitalized texts, sounds, images, facts or other elements, or combination of these, in order to recognize and uncover new knowledge or insights". Here we use *facts* to include also metadata. Data analysis comprehends data mining, but it is a more general and a technology-neutral term that includes many other activities done on them (crawl, copy, extract, process, compare, interpret, sort, parse, remove) [8].

A. Concept of Privacy

Privacy issues are getting increasingly important, as demonstrated by the introduction of the Data Protection[1], or Privacy[2], Day yearly celebrated from 2007, and the standardization of privacy requirements (ISO 15408).

Privacy in general can be defined as[3] the "freedom from interference or intrusion", but in information technology it goes further, as the right of an individual to determine how, when and what information is accessed by whom [9]. In other words, the user should remain in control of the data gathered and transferred [10]. More, privacy is not only an individual's right, it also is a safety critical concern [11] – consider the leakage of sensitive data and their misuse, or the access to and control of critical equipment gained by malicious users – and this is particularly true for health data and eHealth IoT.

B. Data Minimization

Of course, in order to allow some actions, like health management in our case, to be performed, an individual must accept that sensitive information needs *to some extent* to be released, leading to the concept of *contextual* privacy [12].

Data minimization spans across three levels: first, occasions for collection of sensitive data should be minimized; second, when needed, the extent of data collection should be minimized; finally, the time duration of data storage should be minimized [9].

Although secure multiparty computation involves computationally intensive operations and communication overhead, it

[1] http://www.coe.int/dataprotection. Last accessed 22 Oct 2015.

[2] https://www.staysafeonline.org/data-privacy-day/. Last accessed 22 Oct 2015.

[3] privacy, n. Oxford English dictionary, online version, Oxford University Press. URI: http://www.oed.com/view/Entry/151596. Last accessed 22 Oct 2015.

is capable of ensuring security and privacy in presence of a certain fraction of so-called semi-honest users (curious players passively misusing the system) or even of malicious users (nefarious parties actively infringing the system) [13]. Hence, it is worth considering as a secure means for data analysis for some eHealth applications, e.g. in case of infrequent readings transmission. For example, to routinely send physiological parameter readings to a health center without transmitting explicitly the value of that parameter. Only upon identification of an abnormal value, a weaker but explicit method could be used after automatic interrogation.

Analysis on minimized data is still possible, as it has been shown in [12], where machine learning has been used to process records and identify patterns and behaviors on minimized versions of records, with entries replaced by hash-keyed pseudonyms. Pseudonyms allow identifying (internally) a subject without revealing (externally) the actual identity [9].

What is searched here is the anonymization of features of known users, not making users anonymous. Anonymization is generally not feasible – or it may be useless since data traces may be used to infer the user identity [14] – but minimization, i.e. limiting the disclosure of sensitive information to the amount absolutely necessary for the service (see below), possibly also exploiting distributed paths [14] (see Sect. III-D) may help.

C. Authentication

On the other hand, authentication should be ensured, as needed, to securely identify users or data producers, and to this end it should be done properly, possibly distinguishing data from metadata. For example, in some developing countries mobile phones are shared among people for health care [15]: proper security measures need to be adopted, since the univocal correspondence between user and owner may be lost.

D. Architectural Choices

In information security, the risk related to sensitive information can be denoted by the product of the probability of the unwanted event (e.g., threat success probability) by its severity. Both factors need to be considered.

Privacy of the user's sensitive data must be ensured throughout all the communication chain and data repositories (see Fig. 1), together with the protection against malicious users and data modification (sabotage, identity theft). End-to-end encryption and secure server are needed to protect from security threats at proximal network or remote device: information disruption and modification/fabrication, induced malfunctions (safety), interception and tampering (privacy), cheating (safety and privacy) [3].

A trade-off on the architectural options about where data storage and computation are assigned, centralized or distributed, is faced (see Table I and Table II). On one hand, a centralized option offers more powerful computation, possibly also exploiting the availability of broader data, and a more professional software and data management, but it also exposes data to weaker privacy protection. On the other hand, a distributed option offers potentially better privacy protection by assigning more emphasis at user's local resources (keeping information as local as possible improves user's control on data), but it also is generally less powerful and potentially less protected due to possibly missing or less regular software updates and automated data back-ups. Scattered solutions are generally intrinsically more robust due to their nature, but in a distributed architecture the larger number of threat targets may increase also its vulnerability.

Probably a good approach is hybrid where different options are used on different data subsets (cf. Sect. III-B), see Fig. 2.

TABLE I
ADVANTAGES AND DISADVANTAGES WITH RESPECT TO DATA ANALYSIS AND SECURITY THREATS FOR DATA STORAGE AND PROCESSING AT CLOUD AND USER SIDE.

	centralized	distributed (local)
computing power	stronger	weaker
data analysis (learning)	possible	not possible
physical privacy	all data shared	complete data only local
software updates	generally better	potentially poorer
automated back-ups	generally done	not always done

TABLE II
ADVANTAGES AND DISADVANTAGES WITH RESPECT TO DATA ANALYSIS AND SECURITY THREATS FOR CENTRALIZED AND SCATTERED REPOSITORIES.

	centralized	distributed
reliability	no redundancy	redundancy possible
vulnerability to attacks	poorer (single point)	better (scattered)
failures over chain	smaller	larger

E. Example Private Data Structure

The above concepts of data minimization (Sect. III-B) and architectural choices (Sect. III-D) can be formally represented as follows (see Fig. 2). Data set attributes $\mathcal{S}$ are partitioned according to N domains

$$\mathcal{S}_i : \cup \mathcal{S}_i = \mathcal{S}; \mathcal{S}_i \cap \mathcal{S}_j = \emptyset, \forall i, j \in [0, N-1] \qquad (1)$$

so that $\mathcal{S} = \{\mathcal{S}_0, ..., \mathcal{S}_{N-1}\}$. Subsets are stored at scattered locations and/or only some of the subsets is exchanged between remote locations. Moreover, identity of the user I is not attached explicitly subsets, but the logical association can be restored by different keys $\mathbf{k} = f(I)$:

$$I \rightarrow \{k_0, ..., k_{N-1}\}; k_i \neq k_j, \forall i \neq j; i, j \in [0, N-1] \qquad (2)$$

so that

$$\mathcal{S}^{(I)} \leftrightarrow \{\{k_0, \mathcal{S}_0\}, ..., \{k_{N-1}, \mathcal{S}_{N-1}\}\} \qquad (3)$$

where pairs $\{k_i, \mathcal{S}_i\}$ can be located at different repositories and only some of them may be exchanged. More generally, access rights to domains $\mathcal{S}_i$ are not uniform and can be dynamically conditionally modified.

In addition, keys k_i do not need to be fixed but they can be dynamically changed: $k_i = k_i(n)$, $n \in \mathbb{N}$, for example

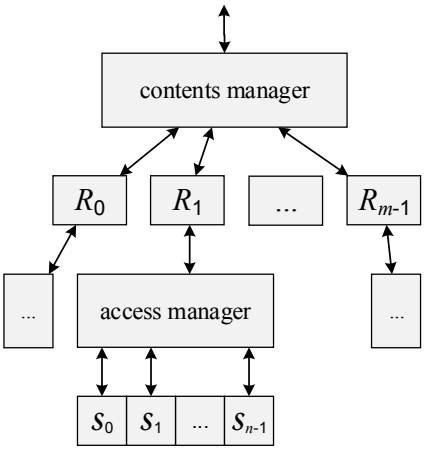

Fig. 2. Access (from top of figure) to information at generally scattered repositories R_i. Data at repository is partitioned into domains $\mathcal{S}_i$, with distinct access rights to them (bottom).

according to pseudo-random table entries, at some event, such as time, access counter, etc.

Allowing operations only on a sub-scheme not only ensures integrity of data, but it also supports data minimization.

IV. Efficacy and Serviceability

As seen above, privacy is a concern for an increasing fraction of users and sense of privacy is potentially a favorable factor for the successful adoption of a service. Although crucial, confidence or trust in the system is not enough. In addition for the system to be functional (Sect. II) and sustainable (Sect. III), it is necessary to make sure that the system is serviceable, i.e., it responds to the needs and it is also actually used, so that the benefits, discussed below in Sect. V, could be achieved.

Business models, requirements and final objectives for eHealth and commercial systems are very different, and development protocols may need to be complemented to take those peculiarities into account [16]. In particular, usability of technologies and services by the users, caregivers and persons under care, must be ensured. To this end, it is important to consider all the involved stakeholders [16].

Other user-related aspects to be contemplated, in general and for eHealth services, are also the actual validity of informed consent through understandable privacy policies. In a word, users should understand what they should do and what they are doing.

V. Social Significance

As population is aging in developed countries, the need of health care is broadening with a pressure for more cost-efficient health care system. In some cases this can be achieved by deistitutionalization, transferring health care from hospitals to residences, improving quality of life for chronic diseases and enabling early diagnosis, preventive care and well-being interventions for medical and psychological possibly emerging disturbances.

Fig. 3 shows our model for the progress of a disease, access to health care and outcome. On the left is represented the progressive degeneration of healthy conditions from bottom up. At some earlier stage it is possible to care the disease (central column) by a visit to a doctor, but in later stages it is needed to go to a hospital. Treatments at hospitals are more expensive and, importantly, staying for prolonged time at a hospital is felt by patients as less comfortable or pleasant compared to home. At the right of the figure are represented the outcomes. The aim is to keep the status of a person as low as possible on the stack, which is enabled by early detection and care of diseases made possible by monitoring, alerts and interventions by eHealth.

Smartphones and mobile phones are widely used in both developed and developing countries: patients but also caregivers (doctors/nurses) may use regular smartphones/tablets. Users are getting familiar to fitness bands. It is therefore natural exploiting all those as enablers of pervasive eHealth. In addition to that, it has been observed that the threshold for participation to online services is lower. As a consequence, some form of integration of eHealth services with online social networks may be effective, although security issues need to be carefully studied in this case.

Forms of access to health care (e.g., counseling) happen in developing countries using mobile phones [15]. In these cases, initial (simpler) forms of eHealth services may foster more inclusive health care provision globally. Other applications of eHealth service are as quick deployment in emergency scenarios.

In all the examples above, the most important benefits of eHealth solutions are cost-efficiency and a more inclusive health care system, and, as a result, an improved quality of life.

For remote care sites, for example in developing countries, complementary requirements include the availability of battery charge of communication devices and coverage for service availability [15]. Investments in network coverage and electricity in developing countries improve quality of life in general but in particular they enable a more inclusive health care provision.

VI. Future Directions

Privacy and security solutions discussed in Sect. III are suitable to eHealth services but they are not peculiar to them. Unique possibilities offered by this particular environment can be exploited, like using bodily features not only for monitoring health status but also for security [17, e.g.].

Where a developing path of IoT, and eHealth IoT in particular, is ensuring its security, an evolving path of eHealth IoT includes going down to smaller dimensions, towards the nanoscale [18]. This in turn comprehends two distinct but eventually converging paths, those going through communications technologies and biology advances, respectively.

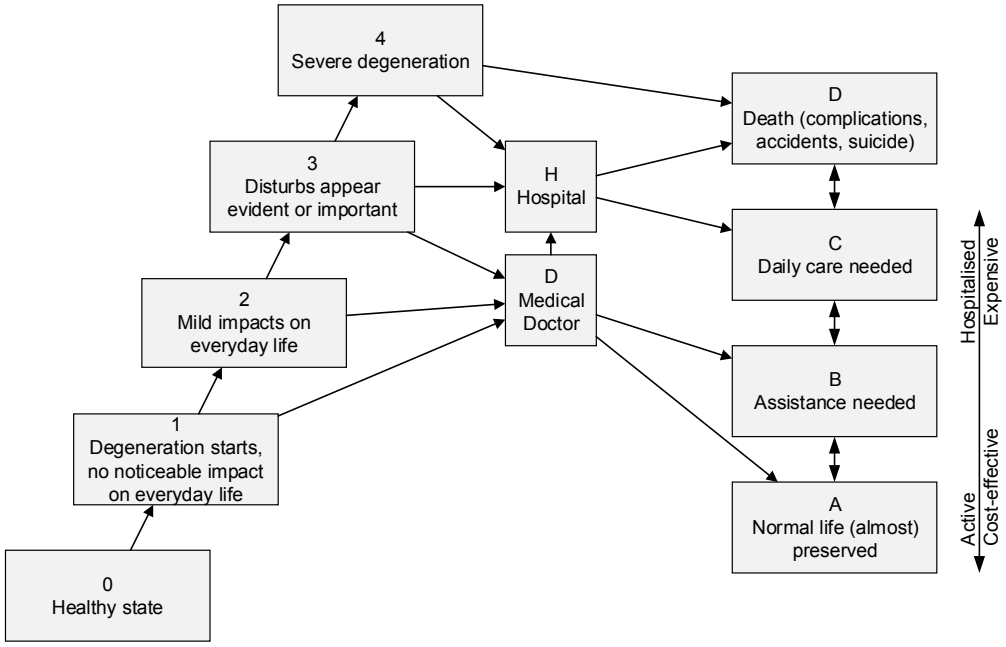

Fig. 3. Progress of a disease, access to health care and outcome.

A. Nanoscale communications

Existing communication paradigms are scaling down to nanoscale by extending legacy communication technologies. New challenges are due to small physical dimension of devices like antenna size, operating frequency and channel models. Nanomaterials and graphene in particular are considered for the electronics. Together with communication devices, nanomachines and nanorobots, possibly adopting bio-inspired features, are also under study. The scaling process will open novel biomedical applications, including in-body monitoring, drug delivery, bio-hybrid implants [19], as well as directly interacting with natural biological signaling, see following Sect. VI-B.

B. Biological signaling

Exosomes is the term given in 1987 by Johnstone, who discovered the related mechanisms in 1983 [20] to membrane-enclosed vesicles having size of $(30 \div 100)\mathrm{nm}$ released by cells and found in biological fluids such as blood, urine and saliva [21]. In the last years they are gaining tremendous attention due to their potentialities. Indeed, exosomes are key in various physiological and pathological processes [22] and in the related intercellular and system-level communication in organisms. Exosomes carry information about the cell-state, carrying biomarkers [23] for both healthy and disease conditions. Due to their signaling capabilities, exosomes are also currently studied for therapeutic applications (drug delivery vehicles, for example). Exosomes can also control both ways the immune response at target cells. [21]

C. New Venue

Putting the two above research paths together allows interacting more intimately with organisms.

Depending on the method, communication may be short-range ($\sim \mu\mathrm{m}$) when based on molecular diffusion, or long-range ($\sim \mathrm{m}$) exploiting pheromones [19], but delay may be as large as tens of seconds [24], still feasible in many applications. Bio-nanomachines interacting with their environment include DNA (deoxyribonucleic acid) sequences, genetically programmed bacteria and engineered cells [25]. Bacteria may act as DNA carriers. Functionalities of a bio-nanomachine are listed in [25] together with open research issues in this emerging area. Among the most interesting interactions is the brain-machine interface [26].

Open research issues include the control of nanomachines, robustness to deterioration (consistency of behavior) of bio-nanomachines subject to decline, and dismissal of nonfunctioning machines [25].

Relevant to the subject of the core of this article are security threats, brought to another level and moving into the human body with the possibility to hack directly into it (e.g., transplants, etc.).

In addition to safety and security, also important are ethical issues. New specificities need to be analyzed, although, despite their new nature, the above new technologies touch fundamentally the same ethical problems as old and current ones, so that we possibly can use the new offered possibilities [27].

VII. Conclusions and Discussion

This article presents a holistic view on the eHealth services.

Focusing on the peculiarities of pervasive IoT eHealth services, three dependability aspects crucial for successful service deployment are here analyzed: safety, security and serviceability.

Safety – Reliability in presence of other concurrent systems and availability of a partially resource constrained IoT eHealth system must be ensured, especially considering the wireless environment and the uncontrolled environment represented by homes. Security – Confidentiality to protect privacy of user's data and integrity of eHealth system information flow, both health data and system control, to shelter from sabotage and other threats are fundamental. Data minimization, including pseudonymization (but remembering that authentication of the end user, e.g., patient, is also required in some form), and possibly secure multiparty computation are identified as promising elements of the architecture. The system architecture and the data structure in particular need be designed to ensure the target crucial objectives: a hybrid architecture (partially centralized and partially distributed) should provide a balance between user control and a powerful and professional system management. Serviceability – The final service should respond to the need of all stakeholders; in particular, empowering end users with capabilities and willingness to use the system is a success key for improvement of healthy status. Efficacy and cost-effectiveness are inclusive health care enablers.

Developments in communication technologies and biology, with their currently open challenges, converge to bio-nanosystems, opening unprecedented possibilities for on-body and in-body devices in medicine but also introducing new security threats to fight.

Acknowledgement

The research leading to these results was derived from the Wireless Innovation between Finland and US (WiFiUS) project SOCRATE (Exploiting Social Structure for Cooperative Mobile Networking), jointly funded by Tekes, the Finnish Funding Agency for Innovation, and the US National Science Foundation, NSF.

References

[1] A.J. Jara, M.A. Zamora, A.F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of things", Proc. IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom), p. 1811–1818, Liverpool, UK, 25–27 Jun 2012.

[2] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyberphysical systems", Proc. IEEE, vol. 100, no. 1, p. 283–299, Jan 2012.

[3] S.M.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.-S. Kwak, "The Internet of things for health care: A comprehensive survey", IEEE Access, vol. 3, p. 678–708, 2015.

[4] D. Uniyal, V. Raychoudhury, "Pervasive healthcare - A comprehensive survey of tools and techniques", arXiv:1411.1821, 2014.

[5] G. Baldini, T. Peirce, M. Handte, D. Rotondi, S. Gusmeroli, S. Piccione, B. Copigneaux, F. Le Gall, F. Melakessou, P. Smadja, A. Serbanati, J. Stefa, "Internet of Things Privacy, Security and Governance", in: Internet of things – Converging technologies for smart environments and integrated ecosystems, O. Vermesan, P. Friess, eds., River Publishers, Aalborg, 2013, Chapt. 4: p. 207–224.

[6] J.M. Bohli, P. Langendörfer, A.F. Skarmeta, "Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities", in: Internet of things – Converging technologies for smart environments and integrated ecosystems, O. Vermesan, P. Friess, eds., River Publishers, Aalborg, 2013, Chapt. 5: p. 225–244.

[7] U. Celentano, Dependable cognitive wireless networking – Modelling and design, Doctoral thesis, Acta Universitatis Ouluensis C 488, Oulu, Finland, 2014.

[8] J.P. Triaille, J. de Meeûs d'Argenteuil, A. de Francquen, Study on the legal framework of text and data mining (TDM), European Union Studies KM-03-13-426-EN-N, Mar 2014.

[9] A. Pfitzmann, M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management", Version v0.34, 10 Aug 2010. Archive: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[10] A. Sawand, S. Djahel, Z. Zhang, F. Naït-Adbesselam, "Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring system, Proc. IEEE/CIC ICCC Symp. on Privacy and Security in Communications, p. 187–192, Shanghai, China, 13–15 Oct 2014.

[11] I. Oliver, Privacy engineering: A dataflow and ontological approach, CreateSpace, 2014.

[12] S. Hofbauer, G. Quirchmayr, K. Beckers, "A privacy preserving approach to call detail records analysis in VoIP systems", Proc. Int. Conf. on Availability, Reliability and Security (ARES), Prague, Czech Republic, 20–24 Aug 2012.

[13] Y. Lindell, B. Pinkas, "Secure multiparty computation for privacy-preserving data mining", J. of Privacy and Confidentiality, vol. 1, no. 1, p. 59–98, 2009.

[14] S. Gürses, C. Troncoso, C. Diaz, "Engineering privacy by design", Proc. Conf. Computers, Privacy and Data Protection (CPDP), Brussels, Belgium, 25–27 Jan 2011.

[15] K. Hampshire, G. Porter, S.A. Owusu, S. Mariwah, A. Abane, E. Robson, A. Munthali, A. DeLannoy, A. Bango, N. Gunguluza, J. Milner, "Informal m-health: How are young people using mobile phones to bridge healthcare gaps in Sub-Saharan Africa?", Social Science & Medicine, vol. 142, p. 90–99, Oct 2015.

[16] L. Van Velsen, J. Wentzel, J EWC Van Gemert-Pijnen, "Designing eHealth that matters via a multidisciplinary requirements development approach". JMIR Research Protocols, vol. 2, no. 1, 2013.

[17] P. Campisi, D. La Rocca, "Brain waves for automatic biometric-based user recognition", IEEE Trans on Information Forensics and Security, vol. 9, no. 5, May 2014, p. 782–800.

[18] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, Y. Koucheryavy, "The Internet of bio-nanothings", IEEE Communications Magazine, p. 32–40, Mar 2015.

[19] I.F. Akyildiz, J.M. Jornet, M. Pierobon, "Nanonetworks: A new frontier in communications", Communications of the ACM, vol. 54, no. 11, p. 84–89, Nov 2011.

[20] B.T. Bin, R.M. Johnstone, "Fate of the transferrin receptor during maturation of sheep reticulocytes in vitro: selective externalization of the receptor", Cell, vol. 33, no. 3, Jul 1983, p. 967–978.

[21] M. Krause, A. Samoylenko, S.J. Vainio, "Exosomes as renal inductive signals in health and disease, and their application as diagnostic markers and therapeutic agents", Front in Cell and Developmental Biology, vol. 3, Oct 2015.

[22] S. Mathivanan, H. Ji, R.J. Simpson, "Exosomes: extracellular organelles important in intercellular communication", J. of Proteomics, vol. 73, no. 291, p. 1907–1920, 2010.

[23] A.K. Ludwig, B. Giebel "Exosomes: small vesicles participating in intercellular communication", Int. J. Biochemistry & Cell Biology, vol. 44, p. 11–15, 2012.

[24] L.C. Cobo, I.F. Akyildiz, "Bacteria-based communication in nanonetworks", Nano Communication Networks, vol. 1, p. 244–256, 2010.

[25] T. Nakano, T. Suda, Y. Okaie, M.J. Moore, A.V. Vasilakos, "Molecular communication among biological nanomachines: A layered architecture and research issues", IEEE Transactions on Nanobioscience, vol. 13, no. 3, p. 169–197, Sept 2014.

[26] F. Mesiti, I. Balasingham, "Nanomachine-to-neuron communication interfaces for neuronal stimulation at nanoscale", IEEE Journal on Selected Areas in Communications, vol. 31, no. 12, p. 695–704, Dec 2013.

[27] Clausen, Jens. "Man, machine and in between", Nature, vol. 457, p. 1080–1081, 26 Feb 2009.