IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 18, 2017, accepted May 3, 2017, date of publication May 15, 2017, date of current version June 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2704100

Fog Computing in Healthcare–A Review and Discussion

FRANK ALEXANDER KRAEMER, ANDERS EIVIND BRATEN, NATTACHART TAMKITTIKHUN, AND DAVID PALMA

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 7491 Trondheim, Norway

Corresponding author: Frank Alexander Kraemer (kraemer@ntnu.no)

The work of D. Palma was supported by the European Union's Horizon 2020 Research and Innovation Programme through the Software-defined Intermittent Networking Project, the Marie Sklodowska-Curie Grant, under Grant 699924.

ABSTRACT Fog computing is an architectural style in which network components between devices and the cloud execute application-specific logic. We present the first review on fog computing within healthcare informatics, and explore, classify, and discuss different application use cases presented in the literature. For that, we categorize applications into use case classes and list an inventory of application-specific tasks that can be handled by fog computing. We discuss on which level of the network such fog computing tasks can be executed, and provide tradeoffs with respect to requirements relevant to healthcare. Our review indicates that: 1) there is a significant number of computing tasks in healthcare that require or can benefit from fog computing principles; 2) processing on higher network tiers is required due to constraints in wireless devices and the need to aggregate data; and 3) privacy concerns and dependability prevent computation tasks to be completely moved to the cloud. These findings substantiate the need for a coherent approach toward fog computing in healthcare, for which we present a list of recommended research and development actions.

INDEX TERMS Body sensor networks, fog computing, healthcare, health information management, internet of things, sensor devices, wireless sensor networks.

I. INTRODUCTION

As Topol writes in *The Creative Destruction of Medicine* [1], healthcare stands before its most fundamental changes ever. One driver of these changes is wireless sensor technology. Besides giving access to an increasing number of biometric parameters, sensors are also getting smaller, so that they can be worn without obstructing everyday life. This is important when data needs to be collected continuously. The BioStamp [2], for instance, is a sensor the size of a band-aid that can measure various biometric signals and simply be attached to the skin. Further, Kang et. al [3] describe an optimized technique to print sensors directly onto adhesive film that can be attached to skin. Contact lenses also offer possibilities of sensing a number of biometrics [4]. Such advances promote a scenario in which patients are instrumented with dozens of sensors. In addition comes the abundance of fitness trackers. They foreshadow a future in which each human, regardless of health status, is continuously monitored.

Sensory data is only useful if we can derive insights from it. Such insights are provided by other drivers in healthcare, like big data and machine learning, the accuracy of which will soon exceed that of humans [5]. Apart from automatic or assisted analysis of medical images, big data analysis can be used to study the effectiveness of treatments, identify patients at risk for chronic diseases, ensure that patients adhere to treatment plans, optimize processes and personalize care [6].

To monitor patients at this scale, sensors need to be wearable and wireless. This constraints their size, and influences the amount of energy, memory and processing capacity that they can offer. In addition, data is only valuable in context and needs to be aggregated from several sensors. Sensors therefore send it to other, more capable computing devices for analysis, aggregation and storage. The wireless ECG monitoring system *IntelliVue* from Philips [7] for instance, requires its own installation of access points and network switches in order to seamlessly forward ECG data to central servers. However, such vertical approaches do not scale. When many patients should be instrumented, each requiring a high number of sensors, these cannot be supported by their own, dedicated infrastructure, as such individual infrastructures are expensive and hard to maintain.

The Internet of Things (IoT) offers an alternative approach. Sensor devices can use a common infrastructure to forward their data to more comprehensive applications, using standardized protocols such as 6LoWPAN [8] over IPv6 [9].

Connectivity is provided by border routers, that connect the wireless resource-constrained nodes to existing network infrastructures. This enables a device-to-cloud architecture in which the infrastructure between device and cloud is only used as a communication channel. Cloud computing frees the sensors from battery-draining computing tasks and provides virtually unlimited resources. The cloud is also one possible place where data from different sensors can be aggregated, enabling the large-scale data sets required by the analysis tasks mentioned above.

For many applications within health informatics, however, such a simplistic sensor-to-cloud architecture is not feasible. In some cases, regulations do not allow to store patient data outside the hospital. For some applications, relying entirely on remote data centers is also unacceptable because of patient safety in case of network and data center failures.

One possible solution to bridge the gap between sensors and analytics in health informatics is *fog computing*. This is an architectural style for distributed systems in which application-specific logic resides not only in data centers (the cloud) or the devices closest to the users, but also in the infrastructure components between them. Examples of such infrastructure components are gateways, routers and access points. This added flexibility of computation opens new possibilities for solving healthcare challenges. Better patient mobility and increased integration will enable uninterrupted monitoring as introduced above, and also enable entirely new applications, as discussed later.

We observe an increasing number of publications on fog computing principles in general, including applications within healthcare. In most cases, however, little effort is spent to discuss where computation tasks should be placed, or the tradeoffs between different requirements. To advance the application of fog computing in healthcare, it is important to understand such tradeoffs holistically, taking into account the diverse requirements of several, interacting applications and the vision of future medicine as outlined above. This raises three questions:

- Which computational tasks in health informatics can be processed by fog computing?
- Which are potential locations in the Internet of Things where these tasks can be executed?
- Which are the tradeoffs to consider when placing computational tasks in the system?

To find answers to these questions, we performed a systematic review of pervasive health applications relevant for fog computing. We conducted a broad search within international journals, conferences and workshops, using the sources listed in Table 1. We looked for papers addressing personal sensor network applications in general, and wireless healthcare applications in particular. To identify relevant publications, we set up three groups of search terms, summarized in Table 2. The first two groups encompass the terms that the authors use to describe the network topology and the architecture, respectively. They set the technical boundaries for the study. The third group of terms addresses the different phrases that are used to describe healthcare in a wireless or mobile setting. Whenever we found a paper that used a new term relevant to our study, we added that term to the corresponding group, and conducted a new search to find other publications using the same phrase.

TABLE 1. Sources used in the search of relevant publications.

Primary source	URL	Use cases found
IEEE Xplore	ieeexplore.ieee.org	17
ACM Digital Library	dl.acm.org	2
ScienceDirect	sciencedirect.com	2
SpringerLink	link.springer.com	3

The search resulted in 163 papers, published between 2005 and 2016, that we found relevant to our study after reading the abstracts. Out of this pool, we discarded 73 after conducting a full-text review. From the papers left, we identified the network topologies and requirements of the solutions, and extracted 24 relevant use cases for further analysis. The sources of these use cases are listed in Table 1.

Previous reviews have addressed the thematic of healthcare related to wireless sensor networks [10] and body area networks [11], the Internet of Things [12], ubiquitous and pervasive computing [13] and mobile computing [14]. However, to the best of our knowledge, there has not yet been a survey of fog computing within healthcare.

Our review and discussion contributes the following:

- An overview of benefits and challenges of fog computing.
- A review of healthcare applications and the computing tasks that are relevant for fog computing.
- An overview of network and device types in different deployment scenarios.
- A review of where fog computing tasks are placed.
- A discussion of the tradeoffs when placing fog computing tasks, with respect to requirements in healthcare.
- A list of recommended research and development actions.

The paper is structured as follows. In Sect. II, we will present the concept of fog computing and list the main characteristics and benefits discussed in literature. In Sect. III, we present some of the trends and challenges in healthcare, and provide an overview of medical sensors and actuators and their technical requirements. In Sect. IV, we survey healthcare applications, categorized based on deployment scenario and use case class, and provide an inventory of computation tasks that are suitable for fog computing. In Sect. V we provide an overview of the most relevant technologies for wireless health. We then analyze the architecture of applications in literature, and find out in which hierarchy levels of the network fog computing tasks are executed. In Sect. VI we discuss the benefits and challenges of the applications and architectures we have reviewed, and discuss selected tradeoffs. We conclude with an overview of the current state of research, and outline further research and development demands for applying fog computing within healthcare.

TABLE 2. Terms used in search for relevant publications.

Network topology	Architecture		Healthcare	
Wireless sensor network	Fog computing	Pervasive computing	Mobile healthcare	Ubiquitous healthcare
Ubiquitous sensor networks	Edge computing	Wearable computing	IoT Healthcare	Health telemonitoring
Body area network / BAN	Mobile edge computing	Cyber-physical systems	Home healthcare	Critical care monitoring
Personal area network / PAN	Mobile cloud computing	Monitoring systems	Pervasive healthcare	Non-invasive monitoring
Local area networks / LAN	Ubiquitous computing	Ubiquitous mobility systems	Telehealth	
Wearable wireless sensors	Wearable computing	Wireless health		

II. FOG COMPUTING

The term *fog computing* was initially coined by industry [15] as a metaphor for the main architectural idea behind it: fog is somewhere between the cloud (data centers) and the ground, where the users' devices are located. A term often used synonymously is *edge computing*, describing tasks that are placed at the edge of the network in contrast to the cloud. Note that the term *edge* can refer to different tiers of the architecture. In an industrial setting, *edge* often refers to nodes in a production plant and resides on premisses with the user, for instance as part of a machine controller or a network gateway [16]. ETSI's terminology [17] takes the perspective of internet service providers, referring to edge as the border of the operator's network, like for instance an LTE base station. Our understanding of fog covers both of these perspectives.

The main characteristic of fog computing is its topology, i.e., the geographically distributed nodes that perform computation and offer storage and network services. Fog computing resources can be integrated into access points, routers and network gateways alongside the generic network functions. There may also be dedicated fog computing nodes, like the mobile edge computing (MEC) servers deployed at LTE base stations and access points described by ETSI [17]. Other devices can be dedicated gateways deployed at home, like home automation hubs. The specific types of tasks that fog computing performs depend on the specific application and domain. In general, tasks contain filtering, aggregating, analyzing and temporarily storing data.

Fog computing can be performed on a single fog computing node or on several nodes jointly. This can improve scalability and provide redundancy and elasticity, adding more fog nodes when more computing power is needed. Mechanisms like virtualization and sand-boxing can be used to execute applications, which is why fog computing shares many of the principles of cloud computing. Central to fog computing is the concept of computation *offloading*, which has been treated in research for instance by cloudlets [18], and can also be found in what is called *mobile cloud* [19]. Similarly, crowd computing focuses on the utilization of distributed computation power provided by, for instance, mobile devices [20].

There is a consensus in literature that fog computing is not intended to replace cloud computing, but rather view it as an *perfect ally* [21] or an *extension* [15] of it. [22] also points out how many of the technologies and properties like elasticity used for cloud computing also apply for fog computing.

In the following, we explain and exemplify the benefits of fog computing mentioned in literature. We discuss and evaluate these benefits with respect to healthcare later.

A. REDUCED LATENCY

Compared to a device-to-cloud architecture, placing processing closer to the devices can reduce the latency since the physical distance is shorter and potential response time in a data center can be removed. Compared to a device-only architecture, latency can be reduced since computation-intensive tasks that take a long time on resource-constrained sensor devices can be moved to more capable fog computing nodes. The motivation can also be to keep the latency predictable [23].

B. PRIVACY

Compared to the device-to-cloud architecture, fog computing can reduce the propagation of data, for instance by analyzing sensitive data on a local gateway instead of a data center outside of the control of the user. This can improve the privacy of user data [24].

C. ENERGY EFFICIENCY

There are several ways how fog computing can improve energy efficiency within sensor devices. First, gateways can serve as communication proxies, so that devices can increase the length of their sleep cycles. During the sleep mode, the gateway takes care of any requests or updates, which are then processed when the sensor device wakes up. Second, energy-intensive computations and other services can be offloaded from the battery-driven nodes [23].

D. BANDWIDTH

In comparison to a device-to-cloud architecture, fog computing can reduce the volume of data to be sent into data centers. This can happen in several ways: Raw data can be filtered, analyzed, pre-processed or compressed so that only a reduced amount of data needs to be forwarded [25], [26]. Local nodes can also answer requests from devices based on locally cached data, so that communication with data centers is not necessary at all [27].

E. SCALABILITY

Fog computing can improve the scalability of a system. Local computation can reduce the load from more centralized resources, and be expanded as needed.

Vaquero and Rodero-Merino [24] refers to this as ''mini-clouds.''

F. DEPENDABILITY

Fog computing can increase system dependability in two ways. It can be a means to realize redundancy, by letting several nodes in the network provide the same functionality. It can also execute computation closer to the sensor nodes, so that they are less dependent on the availability of a network connection to more centralized resources [21].

G. CONTEXT

In some cases, a fog computing node is the first node in a network that has enough overview to reason about a situation and the context of data. An example is a system that induces the current activity of medical staff from the location and activity of several devices [28].

III. WIRELESS HEALTH INFORMATICS

We briefly review the current challenges in healthcare, give an overview of the variety of sensors and their requirements.

A. CHALLENGES FOR HEALTHCARE

Healthcare systems in most countries face enormous challenges that will increase due to aging population and the rise of chronic diseases. Many countries also experience a growing nursing staff shortage. At the same time, there is a demand to reduce costs while maintaining high-quality care to patients [29]. As a consequence, healthcare industry promotes an information-centric healthcare delivery model [30]. Part of this delivery model enables remote monitoring of patients, which leads to increased accessibility, quality, efficiency, and continuity of healthcare to patients, and also reduces the overall cost of healthcare [31].

Today, much time is wasted in hospitals by manually measuring biometric parameters and transferring the data between systems, often involving pen and paper. Remote monitoring will free time for caretakers. Other improvements include automated supervision that can replace manual supervision. Bertini *et al.* [32] report benefits of remote monitoring compared to in-hospital follow-ups, including even a positive impact on survival. Another area is the improvement of processes within the hospital. Many processes are planned manually, and therefore done sequentially, instead of using resources more effectively. In addition, sensors will make it simpler to gain correct information about the current status and location of equipment, caretakers and patients. Sensors will also provide a more precise picture of patients, as they can capture data continuously and allow an insight into increasing variety of biometric parameters. This will revolutionize diagnostics and treatment. Topol [1] calls this ''digitizing humans.'' Once this new picture of patients is matched with analytical techniques, new insights will transform early detections, diagnostics, medication and treatment of diseases. One precondition for this is that data is not treated in isolated silos, but that it is combined with other sources and seen in context.

Another trend is the departure from reactive treatment, where patients are treated in a hospital only after an incident, towards a more preventive medicine [33]. This starts by monitoring healthy people, to keep them out of hospital for as long as possible. Additionally, increasing the possibilities to monitor patients at home facilitates releasing them earlier from the hospital. In general, this means that the borders between hospital, home, and other points of care get increasingly blurred: healthcare happens continuously and everywhere.

B. MEDICAL DEVICES: WIRELESS SENSORS AND ACTUATORS

There is a wide variety of sensors, in different stages of technology readiness. Tanaka *et al.* [34], for instance, developed an incontinence sensor integrated in diapers. The sensor uses urine as an electrolyte between two electrodes, which allows it to send an ID signal with a range of 5 meters once coming into contact with urine. A similar principle is used for drug prescription. A digestible microchip the size of a sand particle is integrated into a pill that generates a signal once in contact with digestive juices [35]. This signal is detected by a skin patch, which relays it further to a mobile phone. Examples for actuators are hearing aids, medication dispensers (both intra- and extra-body) or pace makers. The iPill from Philips [36], for instance, is a small device swallowed by a patient, which senses the acidity of its surroundings, in order to release drugs via a pump at the right place in the gut.

C. REQUIREMENTS OF HEALTHCARE APPLICATIONS

All of the potential benefits of fog computing listed in Sect. II are relevant for healthcare. We now exemplify the corresponding requirements and, where appropriate, quantify them.

1) BANDWIDTH

The bitrates of different physiological signals depend on the number of leads, the quantization step-size of the analog-to-digital converter (ADC) in bits, and the sampling frequency [37]. Body temperature, for instance, requires only a low sampling frequency of 0.2 Hz. With a 12-bit ADC, this results in a bitrate of 2.4 bit/s [38]. Blood pressure sampled at 120 Hz with 12-bit ADC yields 1.44 kbit/s [38]. Pulse oximetry needs to be sampled at 600 Hz and requires 7.2 kbit/s [38]. Electrocardiograms (ECG) usually require more than one lead. For clinical applications, a 5-lead ECG needs between 36 to 216 kbit/s, depending on the sampling rate and step size [37], [39]. Electromyograms (EMG) represent electrical signals generated by muscles and can be used in several applications such as food chewing recognition [40] and prosthetic finger control improvement [41]. These use cases require a bandwidth of at least 20.48 kbit/s and 96 kbit/s, respectively. Electroencephalogram (EEG) measures electrical activities from the brain and requires a lot of leads. A 192-lead EEG can demand 921.6 kbit/s bandwidth. This shows that the bitrates of physiological signals vary considerably.

2) LATENCY

With regard to latency, the requirements also vary considerably with the intended use for the data. For ECG, Alesanco and García [39] found through experiments with cardiologists that latencies of up to 2 to 4 seconds in real-time monitoring are acceptable. These are relatively lax requirements from a technical point of view. Stricter requirements are necessary for applications within the realm of the Tactile Internet [42], for instance for the control of exoskeletons which allow paralyzed patients to walk. Other examples with latency constraints come from telehealth applications operating in rural areas, where the network infrastructure itself is often restricted [43].

3) ENERGY-EFFICIENCY

Energy-efficiency is a major concern, because replacing batteries impedes the use of sensors. While some in-body sensors rely on energy-harvesting, either by heat or kinetic energy [11], some sensors may require an operation of the patient when a battery needs replacement.

4) DEPENDABILITY

Depending on what data is used for, system failures have different consequences, from minor inconvenience to serious threat to the patients' lives. Thus, dependability is one of the most important requirements to consider, tightly interconnected with resilience against security threats.

5) SECURITY

Because of the sensitivity of patient data and the potentially severe consequences of tampered or manipulated devices and systems, the security requirements in healthcare are high. With respect to remote monitoring, increased connectivity of devices results in larger attack surfaces. This requires procedures for detection and fixes of security vulnerabilities that are complex. Requirements go beyond technologies implemented in the devices and surrounding systems, but also require routines that need to be in place in organizations, regulators and manufacturers. See, for instance, [44] for an overview.

6) INTEROPERABILITY

Systems, even when provided by different vendors, should be interoperable with each other. This is often not the case. Cardiology patients, for instance, who should be transported between hospitals and who require close monitoring via ECG, need to be attached to different equipment during the transfer due to incompatibilities [37].

D. THE VISION OF FOG COMPUTING IN HEALTHCARE

The apparent match between healthcare challenges, the resulting requirements, and the benefits of fog computing as presented in literature suggests a potential for fog computing as a driver for pervasive, ubiquitous computing in healthcare:

1) FLEXIBILITY OF COMPUTATION LOCUS

Where scalability, privacy and dependability issues prevent a cloud-only solution, fog computing can offer the needed computational resources within the network to meet both regulatory and technical requirements. For such approaches to be effective, it is not only important to have computational resources between sensors and cloud, but also to optimally manage them. This includes transparency of execution for application, as well as a flexibility regarding *where* computation can be executed. With fog computing, the location can be dynamic and depend on the current context, environment and application requirements.

2) INTEGRATION

In the current landscape, the introduction of new sensor devices often requires the simultaneous introduction of a support infrastructure. An example is the heart rate monitoring system mentioned in the introduction, which requires dedicated infrastructure. This is a considerable burden when introducing new, innovative devices. Within a fog computing architecture, new sensors can be added to the existing infrastructure. Fog computing can also serve as a compatibility layer to translate between various standards.

3) PATIENT MOBILITY

Application-specific infrastructure also limits the area where patients can be monitored. This is especially relevant when patients are about to leave the highly instrumented infrastructure of a hospital. Current use cases often do not cover this transition, which can effectively prolong a patient's stay at the hospital. With fog computing resources in place, the transitions between different environments can be managed more gradually.

4) NEW APPLICATIONS

Fog computing will also enable entirely new applications: By adding higher levels of autonomy and intelligence at the edge, fog computing will provide latency and response time improvements, as well as energy savings for wearable and low-cost devices, while performing complex tasks such as fall detection [45]. The next generation of healthcare devices will replace costly and complex devices, without resorting to simple algorithms with limited accuracy. These devices will be enabled by fog computing, ultimately leading to the "Internet of Healthcare Things."

IV. HEALTH APPLICATIONS

In this section, we start with a description of deployment scenarios, give concrete examples of each type of scenario, and categorize healthcare applications into different use case classes. We then present an inventory of computation tasks that are candidates for fog computing.

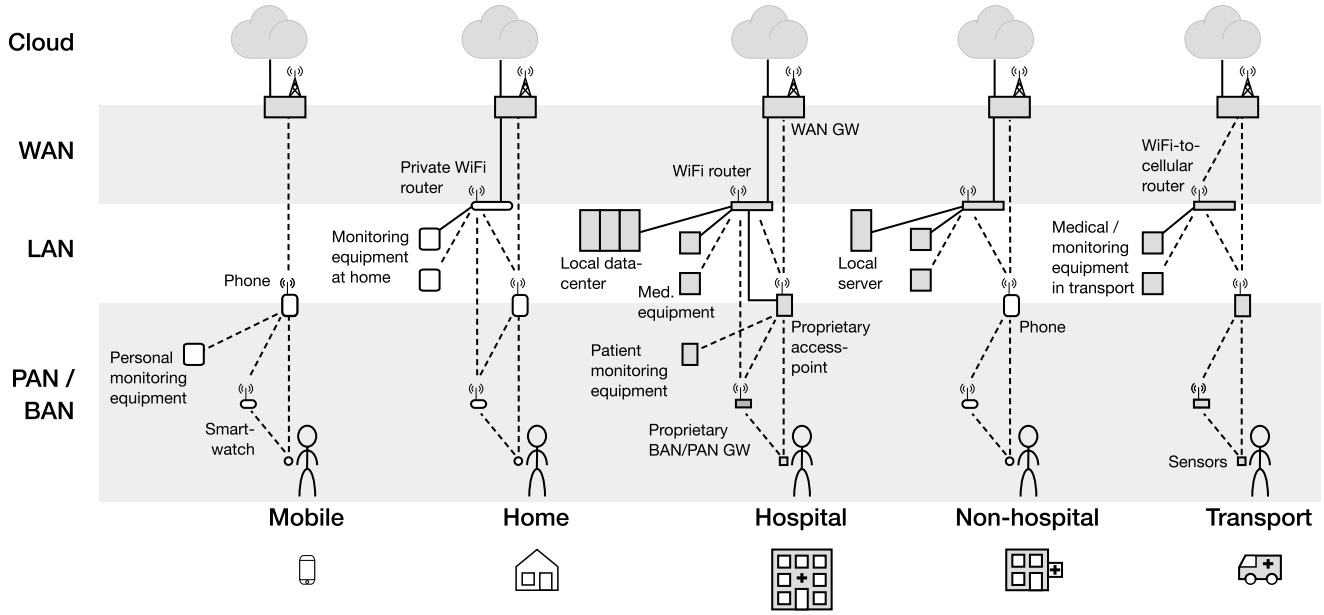

FIGURE 1. Deployment scenarios in healthcare. Devices are used in different network layers. Examples are sensors and actuators, gateways, routers, access points, servers and data centers. We distinguish between devices and infrastructure owned or controlled by the health institutions (grey), and devices and infrastructure owned or controlled by the patient (white).

A. DEPLOYMENT SCENARIOS

From the reviewed papers, we extracted five deployment scenarios, illustrated in Fig. 1. The scenarios differ in terms of involved users and stakeholders, devices and connectivity:

- **Mobile:** In this scenario, the mobile phones of users act as hub between sensor devices and cloud.
- **Home Treatment:** When at home, connectivity is often provided through the patient's internet access. This has influence on device ownership, required usability and maintainability, and how disturbances can be mitigated.
- **Hospital:** Within a hospital, devices are often proprietary, and are usually owned and maintained by the hospital itself. The systems are considerably more complex, which in turn requires the users of the applications to be qualified professionals.
- **Non-Hospital Premises:** Like hospitals, this scenario covers professional points-of-care, but with less staff and infrastructure. Examples are clinics, doctor's offices or nursing homes. Core devices are owned and maintained by the clinic, but patients are sometimes required to connect personal equipment to the network.
- **Transport:** This scenario covers connectivity in an ambulance or helicopter. It is similar to the non-hospital deployment scenario, but with the added complexity that the infrastructure needs to be mobile, for instance using a cellular connection.

.

B. EXAMPLE USE CASES FOR DEPLOYMENT SCENARIOS

In the following, we present example use cases that are typical for their respective deployment scenario. They are also illustrated in Fig. 2.

- **Mobile:** An example for the mobile deployment scenario is the monitoring system for chronic obstructive pulmonary disease (COPD) patients in [46]. A mobile phone acts as mobile base unit and collects data from several sensing devices, processes it and sends it to a back end server. The purpose of placing fog computing on the mobile device is to increase battery life of the wearable sensor device.
- **Home Treatment:** The Parkinson speech analysis solution in [47] is an example for the home deployment scenario. A fog node is placed on the LAN-level in the network hierarchy. Like in the mobile scenario, fog computing is used to collect, store and process raw data, before sending it to the cloud for permanent storage. The main motivation for fog computing is to reduce network traffic and latency. Another example of a home deployment scenario is described in [48], where data from patient- and environmental sensors are used to detect if a patient falls, and raise alerts about gas leaks and fires.
- **Hospital:** In [49] we see a typical example of a setup used in the hospital deployment scenario. Smart shirts, coupled with beacons, are used to monitor physiological data and the location of patients. Fog computing is distributed among several nodes. The data acquisition and processing board (DAPB) collects, processes and merges data from the sensors, and sends them to the wireless transmission board (WTB). The WTB collects data from the beacon points (BPs), merge them with the data from the DAPB and sends them in a single packet to the management subsystem, located at

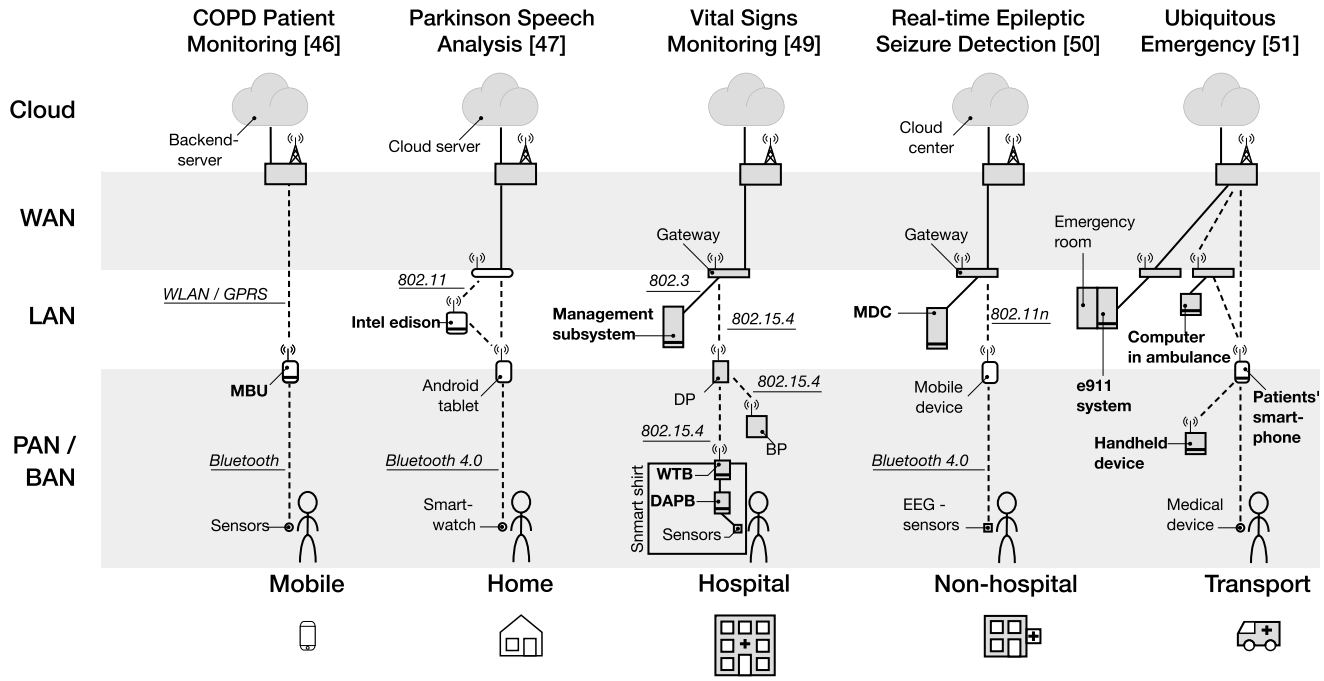

FIGURE 2. Examples of actual deployment in heathcare. Mobile scenario: COPD Patient Monitoring [46]. Home scenario: Parkinson Speech Analysis [47]. Hospital scenario: Vital Signs Monitoring [49]. Non-hospital scenario: Real-time Epileptic Seizure Detection [50]. Transport scenario: Ubiquitous Emergency [51]. Fog computing nodes are marked with a black line at the bottom.

LAN level. The management subsystem uses the data from the DAPB and BPs to monitor the medical parameters of the patients, locates the patient within the hospital and verifies if an alarm has been activated.

- **Non-Hospital Premises:** The real-time epileptic seizure detection system [50] is an example of the non-hospital deployment scenario. A three-tier architecture is proposed, where filtering, preprocessing, feature extraction, feature selection and classification of EEG patterns are performed on the mobile device cloud (MDC), which is placed in the middle tier. Two advantages of using fog computing are mentioned: Providing sub-second real-time responses with minimal communication overhead, and reducing traffic between the local area network and the seizure detection system located in a cloud center.
- **Transport:** The transport deployment scenario is used in the ubiquitous e-health information interchange solution, described in [51]. The authors describe how physiological and contextual data can be collected in an emergency situation from a patient wearing a medical device, and how this information can be duplicated and shared between different devices on-site, in the ambulance and in the hospital. Fog computing is only concerned with the collecting and sending of data, the complexity lies in the distribution of data among many fog nodes.

C. USE CASE CLASSES

To facilitate our discussion, we have synthesized five use case classes, summarized in Tab. 3. The table's columns show whether the use case class requires significant, application-specific *computing*, short response times (*real-time*), the *criticality* for the patient's health, and ability to provide *feedback* to control medical devices.

TABLE 3. Use case classes with their properties.

Use Case Class	Computing	Real-time	Critical	Feedback
Data Collection	-	-	-	-
Data Analysis	✓	-	-	-
Critical Analysis	✓	✓	✓	-
Critical Control	✓	✓	✓	✓
Context Management	✓	(✓)	-	-

- **Data Collection.** This class of use cases only deals with the collection of data, which is then further examined by a doctor when needed. Examples are the logging of training activity, weight or body posture. The criticality of such data is low. If the system fails to log some data points, the patient is still safe.
- **Data Analysis.** This class extends the data collection with some automatic analysis of the data to gain further insights. An example is the speech analysis for Parkinson's patients [47]. Similarly to the data collection, the criticality of the data is low. This use case, however, requires considerable computation of data.
- **Critical Analysis.** These use cases analyze data for critical conditions. Examples are cardiac monitoring via

ECG with automatic alarms once critical situations are detected [27]. The criticality also implies a certain maximum response time, i.e., real-time properties.

- **Critical Control.** In this class of use cases, detected events are not only used to alert personnel, but also to control devices. An example is a device that regulates the amount of oxygen provided to a patient [52].
- **Context Management.** This class of use cases is different from the ones above. It merely observes patients, devices, or employees to figure out their context and help by improving planning or taking proper decisions. This usually requires data analysis, but no or only lax real-time constraints. Examples are systems to figure out the context of healthcare workers [28].

D. COMPUTING TASKS

Table 4 lists the healthcare applications we examined, grouped by use case classes. If an application has several functions, we show it only once under the use case class with the most critical requirements. The third column describes which computing tasks are to be executed and subject to fog computing. Column four shows to which deployment scenario an application belongs. The final column summarizes at which levels of the network fog computation happens, explained later in Sect. V-D.

We will now illustrate some of the computation tasks listed in Table 4. The *data collection* use case class is exemplified by the ubiquitous emergency scenario presented in [51], in which data is aggregated and exchanged among involved parties only in emergency cases. As a side effect, energy consumption due to the transmission of data is also reduced, increasing the effective operating time of the device. The *data analysis* class is exemplified by the speech tele-treatment system for Parkinson's patients described in [47]. The speech analysis, performed on a local gateway, reduces processing time and traffic to the cloud, while remote doctors can still retrieve the analyzed data from the cloud. The *critical analysis* class can be seen in [50], which describes a solution for real-time epileptic seizure detection. During a seizure, patients are usually unable to press a button, but automatic detection ensures that healthcare personnel is alerted and the treatment can be started quickly. The analysis for the seizure detection is done on local servers for low latency, while big data analysis is offloaded to the cloud. A *critical control* use case is found in [52], where an automatic oxygen-controlling system for COPD patients is proposed. An example of the *context management* class is [28], which determines the activity of staffs based on their location and devices being used.

V. FOG COMPUTING ARCHITECTURES

Before we discuss the placement of fog computing tasks, we discuss the types of networks and devices typically found in healthcare.

A. NETWORK TYPES

The reviewed pervasive health use cases employ combinations of four network types to bridge the gap between medical devices and the cloud: wireless personal area networks (WPANs), wireless body area networks (WBANs), local area networks (LANs), and wide area networks (WANs). The hierarchy of these networks is shown on the vertical axis of Fig. 1. Some sensor devices are directly connected to the WLAN via Wi-Fi [25], [46]. Especially in the mobile deployment scenario, devices are directly connected to a WAN via cellular connections [20], [59].

Another way to connect sensors is by WPAN technology, as provided by Bluetooth, IEEE 802.15.4, or ZigBee. These typically have a lower range than Wi-Fi or cellular connections, but are also more energy efficient. However, WPAN technologies have limitations. For some applications, they do not offer the necessary bitrates for the biomedical signals, such as EEG or ECG (cf. Sect. III), especially if patients wear several sensors. Furthermore, electromagnetic signal transmissions are blocked by the body in some postures [11]. This either reduces the quality of the link or makes communications with in-body devices impossible.

To mitigate the challenges with WPANs, a specific standard for wireless body area networks (WBAN) was introduced with IEEE 802.15.6 [64]. It uses a one- or two-hop star topology with only one hub as gateway to other networks [11]. In addition, IEEE 802.15.6 proposes three different physical layers that can be chosen for different applications [64]. The *narrow band physical layer* provides longer communication range, with slightly lower data rates than some WPAN technologies [65]. The narrow band utilizes existing frequency bands such as 402–405 MHz medical device radiocommunications band (MICS) and 2.4–2.45 GHz industrial, scientific and medical band (ISM). The *ultra wide band physical layer* offers higher data rates than the narrow band with low transmission power. This layer can also be designed to achieve better energy consumption per bit than the narrow band [66]. The *human body communication layer* utilizes the galvanic coupling on the surface of the human body for data transmissions. This eliminates antennas and signal propagation problems. Additionally, it is considered to be the most energy-efficient physical layer for high-data-rate requirements [67].

Devices compliant with IEEE 802.15.6 devices are, to the best of our knowledge, still under development [67], [68]. Existing systems referring to WBANs therefore usually utilize WPAN standards, e.g. Bluetooth or IEEE 802.15.4, which may be sufficient for some applications that do not require high data rates or communications with in-body devices.

B. DEVICE TYPES IN HEALTHCARE

Depending on the deployment scenarios of Fig. 1, different devices and network nodes are involved. In the *mobile*

TABLE 4. Reviewed healthcare applications, grouped by use case classes.

REF.	APPLICATION	COMPUTING TASKS	DEP. SCENARIO	FOG COMP.
Data Collection *Data gathering from devices*				
[34]	Urinary Incontinence Detection	Detect signal from sensor, forward information into the system.	Non-hospital	PAN
[53]	Priority-Based Health Data Aggregation	Temporarily cache sensor data, analyze data to classify its priority, select which data to forward.	–	PAN + BAN
[51]	Ubiquitous Emergency Scenario	Forwarding of emergency calls and aggregation of patient data.	Transport	PAN
Data Analysis *Data analysis of the collected data*				
[20]	Activity Monitoring	Analysis of movement data in context of the location. Forwarding of relevant data into the system.	Mobile	PAN
[26]	ECG Data Compression	Encoding of ECG data to compress it and save transmission energy, decoding at the receiver.	–	BAN + PAN + LAN
[47]	Parkinson Speech Analysis	Caching of audio files and local feature extraction on audio files to analyze data. Forward analysis results, not raw data.	Home	PAN + LAN
[54]	Patient State Monitoring	Local analysis of video and audio data to figure out if a patient is in pain. No forwarding of raw data, only processed results.	–	–
[55]	UV Radiance Measurement	Analysis of camera data to measure UV level, aggregation of data from several phones to determine UV level in a specific area.	Mobile	–
[56]	Speech Recognition and ECG Monitoring	Analysis of speech data as in [47]. Analysis of ECG data to detect arrhythmic beats, compression and forwarding of relevant data.	Mobile	PAN + LAN
[57]	Image-Based Healthcare Analysis	Local processing of image data to assess wounds, detect skin cancer and detect heart rate.	Mobile	–
Critical Analysis *Data analysis for critical conditions with alarms when critical situations are detected*				
[25]	Fall Detection	Local analysis of accelerometer data for falls, with filtering of false positives, based on training data received from the cloud.	Mobile	PAN
[27]	ECG Monitoring	Feature extraction of ECG data based on wavelet analysis. Real-time notification and enrichment of data with location.	Home	BAN + LAN
[46]	COPD Patient Monitoring	Analysis of ECG data, local analysis and enrichment with GPS and activity, forwarding of relevant data in compressed form.	Mobile	PAN
[48]	Dementia and COPD Patient Monitoring	Real-time analysis of environmental and patient sensors to detect and alert users about fires and gas leaks. Monitoring a range of patient behavior, including fall detection.	Home	LAN
[58]	Arterial Blood Pressure Monitoring	Low-pass filtering to reduce noise.	Hospital	–
[59]	ECG Monitoring	Feature extraction of ECG data. Classification and detection of anomalies with local alarms. Filtering, transmission of results into the system.	Transport	PAN
[60]	Vital Signs and Environment Monitoring	Capturing and encoding of various types of biometrical and environmental sensor data. Authentication and encryption of data before transmission.	Hospital	PAN + LAN
[49]	Vital Signs Monitoring	Preprocessing and merging of data from a smart shirt, to add activity and location as context.	Hospital	BAN + LAN
[61]	ECG Monitoring	Applying low-pass and high-pass filters on ECG data to remove noise and baseline wandering.	–	BAN + LAN
[50]	Real-time Epileptic Seizure Detection	Analysis and preprocessing of EEG data, local analysis based on wavelet transformation, classification based on machine learning and notification of local staff.	Non-hospital	PAN + LAN
Critical Control *Control of actuators that are critical for patients*				
[52]	Oxygen Level Control	Analysis of oxygen level and patient activity to adjust the appropriate oxygen dose for the patient in real-time, also taking location and environmental data into account.	Mobile	–
[62]	Pacemaker Monitoring and Configuration	Monitoring and visualization of current pacemaker parameters. Local support to remotely update of pacemaker parameters.	Hospital	LAN
Context Management *Observation to deduce the context of a patient or healthcare personnel*				
[28]	Activity-Awareness of Medical Staff	Analysis of location, equipment usage and time to derive the current activity and availability status and improve planning and collaboration.	Hospital	PAN
[63]	Activity Monitoring	Local analysis of heart rate, acceleration and altitude to classify activity, like driving, resting or different types of walking.	Mobile	PAN + LAN

deployment scenario, mobile phones act as WPAN gateways that connect directly to the WAN through cellular networks. WBAN gateways, such as smartwatches, can be used as intermediate nodes. Off-path nodes, for instance environmental sensing equipment, are connected at the WPAN-level. In the *home deployment* scenario, wireless routers act as gateways from Wi-Fi to WAN. The sensing devices communicate via a gateway on BAN- or PAN-level. This can be a specialized device, for instance mounted in a belt or another item of clothing, or it can be a mobile phone. Off-path computation

nodes, like fall detection devices, are placed at LAN-level. In the *hospital deployment* scenario, local data centers are often available. On both LAN- and PAN-level there are other off-path computation nodes like localization devices and stationary equipment in labs or operation rooms. Patients wear proprietary devices which connect to specialized gateways connecting WBAN or WPAN to the LAN. In the *non-hospital deployment* scenario, e.g., a doctor's office or a nursing home, we typically see small local servers. Lab equipment or environmental sensing devices act as off-path computation nodes. Patients wear the same kind of non-intrusive sensing equipment as identified in the home scenario. A patient in the *transport deployment* scenario wears the same kind of proprietary sensing equipment as in the hospital scenario. This connects to a gateway on a WPAN network that acts as a bridge to a WLAN router in the vehicle. The WLAN router connects to the WAN through a cellular network while in transit. Medical equipment and wired monitoring devices are connected on LAN-level.

C. DEVELOPMENT PLATFORMS

For research and development, there is a wide variety of hardware development platforms with wireless communication with small form factors and low energy consumption. We list some of them that are frequently referred to in literature.

- The Arduino is a low-cost platform used in many application domains. It requires additional hardware modules for wireless communication [48]. nRF24L01 is a low-cost radio transceiver module that can be used with Arduino and other platforms. It is designed for the 2.4 GHz ISM band and optimized for low energy consumption [69].
- The MC13213 system is also based on an 8-bit processor, but has a higher clock rate of 4 MHz. It integrates a 2.4 GHz transceiver module on the chip that supports 802.15.4 and ZigBee [49].
- Intel Edison is another system-on-chip (SoC) with integrated Wi-Fi and Bluetooth 4 radio modules. With its 400 MHz processor it is suitable for computing power-demanding applications like audio processing [47].
- CSEM's Icycom is a platform with a 900 MHz ISM band transceiver unit and a 16/32-bit microprocessor. Its form factor is about 1×1 cm with low energy consumption [70].
- Another SoC suitable for WPAN applications is the nRF51822. This chip supports 2.4 GHz BLE and can communicate with nRF24L01 providing that a BLE stack is implemented for nRF24L01. Unlike nRF24L01, the nRF51822 has an integrated 32-bit processor, yet it still consumes low energy and comes in a tiny package comparable to the nRF24L01 [71].

D. POSITIONING OF FOG COMPUTING TASKS

We also examined at which level of the network and in which devices the reviewed papers place computation tasks. This is summarized in the last column of Table 4. (A dash indicates authors did not reveal enough information.)

Numerous approaches ([20], [25], [28], [34], [48], [51]) place their computation task on a single node at either PAN- or LAN-level. At this level, data is processed and forwarded to higher levels and eventually to the cloud. There is a wide variety of tasks. A typical use case is to collect and analyze time-critical data, in order to achieve critical monitoring, like fall detection [48]. Another example is [20], which describes a sensing platform where a global task scheduler in the cloud is offloading a computation strategy to a worker node in the fog. This instructs the worker node to collect and filter only the most important and relevant data.

Other approaches ([26], [27], [47], [49], [53], [56], [61], [63], [72]) utilize two or more fog-nodes on a direct path between the sensor device and an access point to the cloud. An example is described by López *et al.* [49]. They have developed shirts with embedded sensors that collect physiological data about the patient. The shirts include a wearable data acquisition device that also acts as a BAN-gateway. The device processes the data and sends it to a management system at LAN level, where the data is further processed and permanently stored. In addition, the management receives data from a separate off-path location system, that collects positioning data. In cases where several fog computing nodes are used, we observe that the node closest to the sensor device is typically used for pre-processing or filtering. In-depth analysis, contextualisation and local storage is usually done on a node located closer to the cloud, often at LAN level.

We also observed approaches ([46], [60]) which use a gateway node at PAN or BAN-level for computation, and where the node is capable of connecting to either LAN via Wi-Fi or WAN via a cellular network connection. This is especially useful for applications which need a high degree of mobility, and where flexibility with regard to network connectivity is important. Wac *et al.* [46] describe a scenario where a patient is wearing one or more sensors along with a mobile base unit, connected in a BAN. The base unit collects, synchronizes, filters and processes the data, before sending it further to a back-end server for storage via either WLAN or a cellular network. Huang *et al.* [60] describe a wearable sensor system where physiological data about the patient are captured by on-body biomedical sensors, and then encrypted locally before the data is sent to a mobile computing device (MCD) on a higher network tier. A separate system of sensor motes sends environmental data. The combined data sets are then captured and analyzed by the MCD before the data is eventually sent to a back-end system for permanent storage. The MCDs are also able to communicate with each other via a cellular network. This case also shows that a fog node can use different types of networks, depending on the type of data it is sending.

VI. DISCUSSION

After performing our review and going through the use cases, we conclude that fog computing, despite its potential, is still in an early phase within healthcare, and only implemented

partially, if at all. The main shortcoming of the collective literature is that many of the works focus on isolated use cases, and often only discuss infrastructures that are accordingly specialized. Most use cases also only cover a single deployment scenario. This leads to the lack of a unified view, one that is required by the grander vision of fog computing for healthcare as introduced earlier. We will come back to this shortcoming, after discussing the various aspects of fog computing in health care.

A. LOCUS OF COMPUTATION

Our survey in the previous section shows that computing tasks occur at several levels of the network, from BAN to cloud. This suggests that the distribution of computational tasks should not simply be focused on a node's hierarchical level. The placement of offloading computing tasks within an infrastructure is rather non-trivial. The different roles and computing resources of available devices require a careful consideration of the tradeoffs and complementarity between possible options, bearing in mind target-levels of performance like computational performance, latency limitations, energy consumption and security, to name a few [23]. Even though for some operations it may seem obvious that a resource-powerful environment as provided by cloud computing is preferred to another with fewer capabilities, constraints such as privacy may limit the number of available options, and for instance block information from leaving the hospital premises.

We have also observed that the health-specific deployment scenarios have a significant impact on decisions related to the implementation of the fog concept, despite the generalized acceptance of fog computing anywhere between the cloud and a device (c.f. IV-A). In health informatics, clear examples of this impact are noticeable when comparing computation of fog tasks within hospital premises, with other locations where healthcare activities are also provided but where less resources may be available (e.g., doctors' offices and nursing homes). Other examples include first-responders' interventions in areas where access to typical communication and computing infrastructures may be extremely limited, creating new challenges and opportunities for fog computing.

When considering the different levels at which offloading can be performed, from the device to the cloud, enforcing local processing (e.g., within a facility) may be of paramount importance when reliability is discussed (c.f. VI-C). This local processing does not invalidate the cooperation between local nodes and outbound servers. In fact, they could overlap, but it does provide additional guarantees in case of connectivity loss to the exterior and may be a requirement for critical systems. Privacy and regulations that can be coupled to a given scenario, particularly in health informatics, may however raise stricter constraints and require offloading tasks to take place within certain restrictions (see VI-D).

B. LATENCY AND THROUGHPUT

Previous works shows that computation offloading offered by fog computing, in nodes in the vicinity of constrained devices, can reduce latency up to 2.88 times [73], when compared against offloading to the cloud. This result is strongly influenced by the existing local resources and the ones used in the cloud which, with the steady increase of available data bitrates and a wide coverage of 3/4th generation cellular networks, should only depend on the amount of used servers (i.e., access to the network infrastructure is almost negligible). Nonetheless, the increasing number of nodes and highly specialized sensors raises scalability concerns and latency-sensitive applications may require improved mechanisms to handle the delay between the sensors and the cloud [23].

Theoretically [74], using dedicated servers at the edge of the network (e.g., cloudlets [75]), performance improvements have been achieved but they disregard the pervasiveness of IoT devices and their distinct characteristics. Additionally, while it is intuitive that performing computing tasks locally should improve latency, throughput and even energy consumption [76], several technical challenges have to be considered (e.g. VM or container deployment time, resource management, among other aspects). In fact, these mechanisms may be responsible for adverse effects, becoming a burden to fog nodes and hindering the desired improvements [22]. In many cases, we see that the benefit of reduced latency is taken as granted, without a precise quantification of the specific requirements and an evaluation of different solutions.

Latency and throughput may be improved by fog computing through the reduction of the amount of data transmitted between source and destination, relieving the core of the network and the overall system [77]. This load reduction may also reduce the likelihood of transmission errors and can be achieved by performing computing tasks such as filtering, feature extraction or even prediction [27], [76], [78]. Applications related to face and speech recognition require large amount of data and it is shown that local computations can reduce latency [54]. However, the performance improvement of resource-constrained devices will also rely on devices being capable of bridging network technologies (e.g. 802.15.4/6 with 802.11). Fog computing must be able to leverage on the diversity of resource-constrained nodes and their capabilities, throughout the hierarchy of network infrastructures, in order to scale and provide faster response times [74].

Even though the cloud is typically seen as the endpoint for the data transmitted by a node, this data may actually begin a new life-cycle within the cloud. For instance, it often needs to be delivered to another node (e.g. an actuator or doctor's computer), after being appropriately processed. This process within the cloud is prone to additional latency, but fog computing can significantly increase the performance of bandwidth-intensive and latency-sensitive applications

when compared against a pure ''node to cloud to node'' solution [22], [27]. Ultimately the impact of latency and related metrics (e.g. jitter), must be considered in the Quality of Experience (QoE) registered by doctors and patients in general.

C. DEPENDABILITY

The dependability of health applications is crucial, especially for the use case classes of critical monitoring and critical control (Sect. IV-C). Any single point of failure requires careful consideration. With regard to cloud-based solutions, the general availability of data centers is high, but outages are still a problem, even with redundancy in place [79].

The network towards data centers may also be subject to failures. Ultimately, any of the connections towards a central data center in the different deployment scenarios (Sect. IV-A) can fail, although some are more exposed than others. Ambulances can drive through areas without cellular coverage, or patients at home may loose connection to their Wi-Fi routers. This raises the question to which degree cloud services can be used for critical use cases. In the description of many use cases we believe that these aspects are not sufficiently addressed.

Local computation can be used to either completely replace critical tasks done in data centers, or to use local processing when there are limitations in the cloud [80]. An example is feature extraction to analyze patient ECG data in real-time [27], [49]. If caretakers rely on this function to monitor the well-being of patients, the analysis must not be interrupted. When done on a nearby gateway, it can also be performed when the data center or the connection towards it are down. For the use case class of data collection, where it is only important that data *eventually* arrives at some data base, fog nodes may also buffer data locally until it can be transferred further.

Like the cloud, fog computing nodes are also subject to failure. However, consequences and nature of failure are different from that of cloud computing. Failures in the cloud or the network towards it can affect an entire hospital. In contrast, when resources of a lower network hierarchy fail, consequences affect a smaller area, like hospital sections or single wards. Such minor incidents are often easier to handle with respect to re-equipment or re-staffing. Also, fog computing can lead to architectures with built-in redundancy on a local level, with several fog computing nodes acting as fault tolerant sets [80], which increases dependability.

D. SECURITY

Davies *et al.* [81] argue that privacy concerns due to ''over-centralisation'' of IoT systems are a critical obstacle to their growth. Even though data can be protected on its way into the cloud and within data centers, a suitable strategy to protect data is to avoid sending it off premisses in the first place, and process it closer to its source [24]. The proximity of fog devices, which can be placed within ones infrastructure, may introduce the required trust and enforce the necessary privacy mechanisms that threat cloud computing in critical scenarios. An example is an application to analyze speech from patients with Parkinson's disease [47]. Instead of sending audio recordings into a data center, analysis happens locally, and only result metrics are forwarded. Privacy, though, still remains an issue in more decentralized solutions such as fog computing. Trust and authentication need to be handled, particularly when considering multi-vendor equipment and purely wireless devices. The decoupling between nodes and access points, or gateways, opens the possibility for rogue or compromised fog nodes to hinder the benefits of locality [82], [83]. In order to achieve a decentralised network between fog nodes and mobile nodes or sensors, interoperable trust models must be established, as well as software and physical security mechanisms to protect the networks and their nodes. Another way to make offloading of computation work on untrusted fog nodes is verifiable computing [84], given that the computational tasks can be efficiently mapped to the operations available under these conditions.

Fog nodes can also contribute to security functions. As they often have more computational power than constrained sensor devices, they may assist with cryptographic operations [85]. A link between a sensor device and a BAN gateway may be protected by symmetric encryption, which is supported by many embedded sensor nodes. The patient data may be further secured by the BAN gateway using schemes as proposed in [86], before sent further into the network. Fog nodes may also host other security functions such as intrusion detection [87], or explicit control of which information may leave a location [81].

The pervasiveness of things and fog-capable technologies will also introduce a new era for Human-Computer Interaction (HCI) and its relationship with the security of users and their nodes. In addition to the wireless nature of devices, which limits the users' ability to identify the ''next hop in the loop,'' the size or the lack of input/output peripherals in some of them, creates new challenges. These systems will require simple, yet robust, Authentication, Authorisation and Accounting (AAA) mechanisms that do not compromise the functionalities of devices and their mobility between different networks.

E. AUTONOMIC FOG COMPUTING

Fog computing adds flexibility regarding where computation can be placed. To mitigate the increased complexity coming with this, dynamically managed behaviours are expected in the IoT and fog computing paradigms [22], [24], availing existing resources and coordinating actions for overall improved performance. Context and scenario-specific requirements are fundamental for enabling efficient and autonomic management in fog computing, being aligned with IoT in order to fully exploit its potential [88]. The use of big data is particularly relevant as an enabler for context-aware management [89], taking into account nodes and their different roles in the infrastructure [90]. However, these considerations must handle the heterogeneity of devices and vendors without introducing unbearable overheads.

Overall, the consideration of multiple parameters for improving management in fog computing should scale with the dissemination IoT devices and their distinct uses. This requires nodes to take part in the decision-making process when flexible reconfigurations are needed, without compromising their own purpose in the system. Such process should promote node autonomy or self-awareness, together with dynamic procedures triggered by standard pre-defined protocols [63]. These standard mechanisms are important for guaranteeing interoperability between devices [88], [91] and ''cross the chasm'' of the Internet of Things [81].

F. ENERGY EFFICIENCY

Besides the energy spent for the actual sensing procedure, the main energy consumers on sensor devices are computation and the transmission of data. Fog computing facilitates energy-efficient sensor devices by offloading expensive computation. Hu *et al.* [75] show how offloading functionalities to cloudlets improves the energy-consumption of mobile devices significantly. These results are for mobile applications. For BANs, the cost for sending may be different, so that the energy gains through less processing can be reduced by increased cost for sending. Usually, fog computing nodes are energy-rich, which is why they are suitable for offloading in the first place. However, if fog nodes are mobile, like a mobile phone in the mobile deployment scenario, there is also a tradeoff between the energy consumption of the mobile phone and the sensor device. Tradeoffs like these may require autonomic reasoning in the device to determine in which situation which strategy is most efficient.

G. INSIGHTS AND FUTURE DIRECTIONS

Despite some of the identified flaws and shortcomings in literature, fog computing emerges as a necessary architectural ingredient for ubiquitous computing. Due to the wide range of applications and use cases that can be considered, the extent to what offloading computing tasks can benefit health informatics has still not been fully explored. But fog computing has already proven its effectiveness in terms of bandwidth utilization and latency, for example when considering ECG feature extraction [27]. This is also backed by previous work showing improvements in latency and energy consumption resulting from offloading tasks from constrained devices to more powerful nodes, using common networking solutions such as Wi-Fi and 3/4G [68], [69]. The other main driver for fog computing is dependability. No matter how connectivity improves, outages can ultimately only be covered by computing and storage closer to the sensors, which corresponds to fog computing. Employing fog nodes enables the usage of smarter and autonomous decisions at the fog layer, regardless of cloud availability. This, however, presupposes interoperability between heterogeneous devices and systems.

The possibility of introducing local data processing, adaptation and storage, enabled by fog computing, has also an impact beyond security, latency and interoperability. It also creates new possibilities for actuation, autonomous reconfiguration, devices discovery, mobility and even energy efficiency [92]. Examples of these new prospects include robotic prescription dispensing and medication delivery [93], which must consider medical data collection, formatting, analyzing and storing, as well as the administration of medication according to patients' medical records, as we have seen for instance with the COPD treatment system [52].

The successful dissemination of fog computing in healthcare will not only be influenced by its advantages. An additional driver are restrictions such as regulations imposed by, for example, the Organization for Economic Cooperation and Development (OECD). Fog computing may help users and service-providers to overcome these restrictions. Fog nodes may be used for providing a layer between the end-users, service providers and the cloud, confining private or sensitive health information within trusted devices [94].

We have seen the demand for computation between sensor and cloud in virtually all use cases related to ubiquitous healthcare. However, our review also revealed the lack of a unified strategy or overall architecture for fog computing in healthcare, and pervasive healthcare applications in general. This lack of cohesion undermines the potential of IoT and fog computing. Systems are often seen in isolation, since creators of a specific system focus on isolated use cases, deployment scenarios or sensor technology. Based on these insights and identified shortcomings, we see demand in the following areas for research and development:

1) STANDARDIZATION WITHIN HEALTHCARE

The challenge with most of the use cases we reviewed is that they span across several devices, systems and deployment domains, and therefore lack a single, well-defined stakeholder. Even hospitals, which cover many use cases, may not be sufficient since much of healthcare will also happen outside of their scope. The Continua Alliance [95] is one example for such standardization with special focus on personal health devices. In this context, it should be explored whether and how fog computing can be utilized to increase interoperability through its flexibility to offer computation, i.e., by enabling a heterogeneous, service-based architecture in which computation can take care of interoperability tasks.

2) STANDARDIZATION OF FOG COMPUTING MECHANISMS

The effort above will be facilitated with the availability of standards and protocols for advertising and discovering computing resources within fog environments, as well as offloading computation. The OpenFog consortium [96], for instance, though not a standardizing organization itself, works towards this goal.

3) AUTONOMIC FOG MANAGEMENT

One challenge of the presented use cases is their complexity regarding the system structure and components involved. To be successful, such complexity must not lead to high maintenance costs or come at the expense of usability. Instead, solutions must be able to manage themselves, which implies a degree of autonomy. Similar to the issue of inter-

operability, fog computing can be both the subject of autonomic management, and also contribute with solutions, for instance by hosting the computation processes necessary for autonomy. This represents both opportunities and challenges for the area of autonomic computing.

4) CONNECTIVITY

The heterogeneity of devices and their communication technologies raise several challenges regarding connectivity. This should be seamless between different solutions, coping not only with mobility but also with existing bitrate and delay constraints. Additionally, networks should be non-intrusive, requiring for instance the sharing of networking resources or infrastructures.

5) SECURITY AND TRUST

Fog computing leads to more complex relationships among the system nodes, especially sensor devices and fog computing nodes. Associations between nodes are dynamic. Apart from all security questions relating to privacy of data and safety of patients, this requires some form of trust management between these devices. Though trust models have been applied in various areas, these also need to work with the given complexity and dynamics of fog computing in healthcare.

To fully exploit the fog computing concepts and provide better integrated health applications and their specific requirements, the points above must be considered, both across use case classes and across different deployment scenarios.

VII. CONCLUSIONS

Our review shows that there is a considerable number of computing tasks, across different deployment scenarios and application use cases, that can benefit from fog computing. In fact, our review shows that computation is a necessary element in almost all pervasive healthcare applications, and that these tasks often need to be executed somewhere between the sensors and the cloud. We provided an inventory of such computing tasks, and have shown in which nodes within a network they can be executed. The reviewed papers also show that there is potential for computation at all network levels.

We have further discussed tradeoffs when placing computation tasks in the network, and discussed benefits and challenges of fog computing related to pervasive health applications. Sensor devices are often not powerful enough to do such computation on their own, which is why they need to offload computing tasks. On the other hand, cloud computation is often not a suitable solution for such offloading due to restrictions regarding dependability, privacy concerns or regulations. Fog computing, with its flexibility to add computation as part of a network infrastructure, appears therefore as a suitable concept to meet the requirements of healthcare. Fog computing tasks can filter data, to help preserve privacy or reduce load on the network. The locus of execution can be adjusted to the current deployment scenario, regulations and other requirements. Fog computing tasks can also act as interoperability components, adapting specific sensor needs to standardized and harmonized interfaces. In addition, with their ability to act closely to the users, fog computing tasks add an important component to make systems more dependable. To make these benefits effective, however, it is necessary to lift focus from the individual use cases towards more comprehensive architectures, as discussed above. This review and discussion is a signpost into this direction, summarizing the wide span of deployment scenarios, variety of requirements in future healthcare and the variety of fog computing tasks.

REFERENCES

[1] E. Topol, *The Creative Destruction of Medicine*. New York, NY, USA: Basic Books, 2013.

[2] (Nov. 2016). *BioStamp*.[Online]. Available: https://www.mc10inc.com

[3] D. Y. Kang, Y.-S. Kim, G. Ornelas, M. Sinha, K. Naidu, and T. P. Coleman, "Scalable microfabrication procedures for adhesive-integrated flexible and stretchable electronic sensors," *Sensors*, vol. 15, no. 9, pp. 23459–23476, Sep. 2015.

[4] N. M. Farandos, A. K. Yetisen, M. J. Monteiro, C. R. Lowe, and S. H. Yun, "Contact lens sensors in ocular diagnostics," *Adv. Healthcare Mater.*, vol. 4, no. 6, pp. 792–810, Apr. 2015.

[5] Z. Obermeyer and E. J. Emanuel, "Predicting the future—Big data, machine learning, and clinical medicine," *New England J. Med.*, vol. 375, no. 13, pp. 1216–1219, Sep. 2016.

[6] I. Corporation, "Bigger data for better healthcare," Tech. Rep., Oct. 2016.

[7] *IntelliVue Telemetry System Infrastructure Installation and Service Guide*, 2nd ed, Philips, New York, NY, USA, Jun. 2007. [Online]. Available: https://manualslib.com

[8] G. Montenegro, J. Hui, D. Culler, and N. Kushalnagar, *Transmission of IPv6 Packets Over IEEE 802.15.4 Networks*, document RFC 4944, Oct. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc4944.txt

[9] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, document RFC 2460, Dec. 1998. [Online]. Available: https://rfc-editor.org/rfc/rfc2460.txt

[10] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, Oct. 2010.

[11] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart., 2014.

[12] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The Internet of Things in healthcare: An overview," *J. Ind. Inf. Integr.*, vol. 1, pp. 3–13, Mar. 2016.

[13] C. Orwat, A. Graefe, and T. Faulwasser, "Towards pervasive computing in health care—A literature review," *BMC Med. Informat. Decision Making*, vol. 8, no. 1, p. 26, 2008.

[14] B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, "Mobile-health: A review of current state in 2015," *J. Biomed. Informat.*, vol. 56, pp. 265–272, Aug. 2015.

[15] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, New York, NY, USA, 2012, pp. 13–16.

[16] "Predix architecture and services," General Electric, Boston, MA, USA, Whitepaper, Sep. 2015, accessed on Nov. 11, 2016. [Online]. Available: https://cloudfront.net

[17] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," Eur. Telecommun. Standards Inst., Sophia Antipolis, France, White Paper 11, 1st ed., Sep. 2016. [Online]. Available: http://etsi.org

[18] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[19] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generat. Comput. Syst.*, vol. 29, no. 1, pp. 84–106, 2013.

[20] C. Perera, D. S. Talagala, C. H. Liu, and J. C. Estrella, "Energy-efficient location and activity-aware on-demand mobile distributed sensing platform for sensing as a service in IoT clouds," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 4, pp. 171–181, Dec. 2015.

[21] M. Yannuzzi, R. Milito, R. Serral-Gracia, D. Montero, and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog computing, cloud computing, and more fog computing," in *Proc. 19th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Dec. 2014, pp. 325–329.

[22] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb)*, Nov. 2015, pp. 73–78.

[23] R. Deng, R. Lu, C. Lai, and T. H. Luan, "Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 3909–3914.

[24] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, 2014.

[25] Y. Cao, S. Chen, P. Hou, and D. Brown, "FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation," in *Proc. IEEE Int. Conf. Netw., Archit. Storage (NAS)*, Aug. 2015, pp. 2–11.

[26] K. Xu, Y. Li, and F. Ren, "An energy-efficient compressive sensing framework incorporating online dictionary learning for long-term wireless health monitoring," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Shanghai, China, May 2016, pp. 804–808.

[27] T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare Internet of Things: A case study on ECG feature extraction," in *Proc. IEEE Int. Conf. Comput. Inf. Technol., Ubiquitous Comput. Commun., Dependable, Auto. Secur. Comput., Pervasive Intell. Comput. (CIT/IUCC/DASC/PICOM)*, Oct. 2015, pp. 356–363.

[28] M. Tentori and J. Favela, "Activity-aware computing in mobile collaborative working environments," in *Proc. 13th Int. Conf. Groupw., Design Implement. (CRIWG)*, Berlin, Germany, Sep. 2007, pp. 337–353.

[29] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2016.

[30] The Cloud Standards Customer Council (CSCC), "Impact of cloud computing on healthcare," Reference architecture, Version 1.0, Needham, MA, USA, May 2016. [Online]. Available: http://cloud-council.org

[31] G. J. Mandellos, G. V. Koutelakis, T. C. Panagiotakopoulos, M. N. Koukias, and D. K. Lymberopoulos, "Requirements and solutions for advanced telemedicine applications," in *Biomedical Engineering*. Rijeka, Croatia: InTech, Oct. 2009.

[32] M. Bertini, L. Marcantoni, T. Toselli, and R. Ferrari, "Remote monitoring of implantable devices: Should we continue to ignore it?" *Int. J. Cardiol.*, vol. 202, pp. 368–377, Jan. 2016.

[33] E. MacIntosh, N. Rajakulendran, Z. Khayat, and A. Wise. (Mar. 2016). *Transforming Health: Shifting From Reactive to Proactive and Predictive Care*. [Online]. Available: https://www.marsdd.com/news-and-insights/transforming-health-shifting-from-reactive-to-proactive-and-predictive-care/

[34] A. Tanaka, F. Utsunomiya, and T. Douseki, "Wearable self-powered diaper-shaped urinary-incontinence sensor suppressing response-time variation with 0.3 V start-up converter," *IEEE Sensors J.*, vol. 16, no. 10, pp. 3472–3479, May 2016.

[35] (Jul. 2012). *Digital Pills Make Their Way to Market*. [Online]. Available: http://blogs.nature.com/news/2012/07/digital-pills-make-their-way-to-market.html

[36] (Nov. 2008). *'Philips' Intelligent Pill Targets Drug Development and Treatment for Digestive Tract Diseases*. [Online]. Available: http://phys.org/news/2008-11-philips-intelligent-pill-drug-treatment.html

[37] R. Eide, "Low energy wireless ECG: An exploration of wireless electrocardiography and the utilization of low energy sensors for clinical ambulatory patient monitoring," M.S. thesis, Dept. Comput. Inf. Sci., Norwegian Univ. Sci. Technol., Trondheim, Norway, Jun. 2016.

[38] M. Paksuniemi, H. Sorvoja, E. Alasaarela, and R. Myllyla, "Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit," in *Proc. 27th Annu. Int. Conf. Eng. Med. Biol. Soc. (IEEE-EMBS)*, Jan. 2005, pp. 5182–5185.

[39] Á. Alesanco and J. García, "Clinical assessment of wireless ECG transmission in real-time cardiac telemonitoring," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 5, pp. 1144–1152, Sep. 2010.

[40] R. Zhang, S. Bernhart, and O. Amft, "Diet eyeglasses: Recognising food chewing using emg and smart eyeglasses," in *Proc. IEEE 13th Int. Conf. Wearable Implant. Body Sensor Netw. (BSN)*, Jun. 2016, pp. 7–12.

[41] R. N. Khushaba, S. Kodagoda, M. Takruri, and G. Dissanayake, "Toward improved control of prosthetic fingers using surface electromyogram (EMG) signals," *Expert Syst. Appl.*, vol. 39, no. 12, pp. 10731–10738, 2012.

[42] G. P. Fettweis, "The tactile Internet: Applications and challenges," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 64–70, Mar. 2016.

[43] R. Steele and A. Lo, "Telehealth and ubiquitous computing for bandwidth-constrained rural and remote areas," *Pers. Ubiquitous Comput.*, vol. 17, no. 3, pp. 533–543, Mar. 2013.

[44] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015.

[45] Y. Cao, S. Chen, P. Hou, and D. Brown, "Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation," in *Proc. IEEE Int. Conf. Netw., Archit. Storage (NAS)*, Aug. 2015, pp. 2–11.

[46] K. Wac, M. S. Bargh, B. J. F. V. Beijnum, R. G. A. Bults, P. Pawar, and A. Peddemors, "Power- and delay-awareness of health telemonitoring services: The mobihealth system case study," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 525–536, May 2009.

[47] A. Monteiro, H. Dubey, L. Mahler, Q. Yang, and K. Mankodiya, "Fit: A fog computing device for speech tele-treatments," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP*, May 2016, pp. 1–3.

[48] R. Craciunescu, A. Mihovska, M. Mihaylov, S. Kyriazakos, R. Prasad, and S. Halunga, "Implementation of Fog computing for reliable E-health applications," in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 459–463.

[49] G. López, V. Custodio, and J. I. Moreno, "LOBIN: E-textile and wireless-sensor-network-based platform for healthcare monitoring in future hospital environments," *IEEE Trans. Inf.Technol.in Biomed.*, vol. 14, no. 6, pp. 1446–1458, May 2016.

[50] M.-P. Hosseini, A. Hajisami, and D. Pompili, "Real-time epileptic seizure detection from eeg signals via random subspace ensemble learning," in *Proc. IEEE Int. Conf. Auto. Comput. (ICAC)*, Jul. 2016, pp. 209–218.

[51] E. A. Oladimeji, L. Chung, H. T. Jung, and J. Kim, "Managing security and privacy in ubiquitous ehealth information interchange," in *Proc. 5th Int. Conf. Ubiquitous Inf. Manage. Commun. (ICUIMC)*, New York, NY, USA, 2011, pp. 26:1–26:10. [Online]. Available: http://doi.acm.org/10.1145/1968613.1968645

[52] X. Masip-Bruin, E. Marín-Tordera, A. Alonso, and J. Garcia, "Fog-to-cloud computing (F2C): The key technology enabler for dependable e-health services deployment," in *Proc. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, Jun. 2016, pp. 1–5.

[53] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Inf. Sci.*, vol. 284, pp. 130–141, Nov. 2014.

[54] M. S. Hossain and G. Muhammad, "Cloud-assisted speech and face recognition framework for health monitoring," *Mobile Netw. Appl.*, vol. 20, no. 3, pp. 391–399, Jun. 2015.

[55] B. Mei, W. Cheng, and X. Cheng, "Fog computing based ultraviolet radiation measurement via smartphones," in *Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb)*, Nov. 2015, pp. 79–84.

[56] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, "Fog data: Enhancing telehealth big data through fog computing," in *Proc. ASE BigData SocialInform. (ASE BD&SI)*, Oct. 2015, p. 14.

[57] H. Nejati, V. Pomponiu, T.-T. Do, Y. Zhou, S. Iravani, and N.-M. Cheung, "Smartphone and mobile image processing for assisted living: Health-monitoring apps powered by advanced mobile imaging algorithms," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 30–48, Jul. 2016.

[58] K. Øyri, I. Balasingham, E. Samset, J. O. Høgetveit, and E. Fosse, "Wireless continuous arterial blood pressure monitoring during surgery: A pilot study," *Anesthesia Analgesia*, vol. 102, no. 2, pp. 478–483, 2006.

[59] H. Chen and H. Liu, "A remote electrocardiogram monitoring system with good swiftness and high reliablility," *Comput. Elect. Eng.*, vol. 53, pp. 191–202, Jul. 2016.

[60] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 400–411, May 2009.

[61] J. Granados, A.-M. Rahmani, P. Nikander, P. Liljeberg, and H. Tenhunen, "Towards energy-efficient HealthCare: An Internet-of-Things architecture using intelligent gateways," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare (ICST)*, Nov. 2014, pp. 279–282.

[62] C. Rotariu, V. Manta, and H. Costin, "Wireless remote monitoring system for patients with cardiac pacemakers," in *Proc. Int. Conf. Expo. Elect. Power Eng. (EPE)*, Oct. 2012, pp. 845–848.

[63] J. S. Preden, K. Tammemäe, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015.

[64] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Computer Society, IEEE Standard 802.15.6-2012, Feb. 2012.
[65] R. Vauche, S. Bourdel, J. Gaubert, N. Dehaese, and H. Barthelemy, "Emitters and receivers for impulse radio ultra-wideband and their healthcare applications," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Oct. 2015, pp. 1–5.
[66] R. K. Dokania, X. Y. Wang, S. G. Tallur, and A. B. Apsel, "A low power impulse radio design for body-area-networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 58, no. 7, pp. 1458–1469, Jul. 2011.
[67] H. Lee, H. Cho, and H.-J. Yoo, "A 33 μw/node duty cycle controlled hbc transceiver system for medical ban with 64 sensor nodes," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2014, pp. 1–8.
[68] P. K. Manchi, R. Paily, and A. K. Gogoi, " Design and implementation of low-power digital baseband transceivers for IEEE802.15.6 standard," in *Proc. 29th Int. Conf. VLSI Design 15th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2016, pp. 581–582.
[69] K. Nair *et al.*, "Optimizing power consumption in iot based wireless sensor networks using bluetooth low energy," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, 2015, pp. 589–593.
[70] S. Mijovic, R. Cavallari, and C. Buratti, "Experimental characterisation of energy consumption in body area networks," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 514–519.
[71] C.-C. Chen *et al.*, "Low-cost electronic dose counter for pressurized metered dose inhaler," in *Proc. IEEE Int. Conf. Consum. Electron.-Taiwan*, Jun. 2015, pp. 400–401.
[72] K. Øyri, "Feasibility of short-range wireless monitoring in critical care environments," Ph.D. dissertation, Inst. Clinical Medicine, Univ. Oslo., Oslo, Norway, Aug. 2015.
[73] M. S. Gordon, D. A. Jamshidi, S. A. Mahlke, Z. M. Mao, and X. Chen, "COMET—Code offload by migrating execution transparently," in *Proc. OSDI*, 2012, pp. 93–106.
[74] Y. Xu, V. Mahendran, and S. Radhakrishnan, "Towards SDN-based fog computing: MQTT broker virtualization for effective and reliable delivery," in *Proc. 8th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2016, pp. 1–6.
[75] W. Hu *et al.*, "Quantifying the impact of edge computing on mobile applications," in *Proc. 7th ACM SIGOPS Asia–Pacific Workshop*, New York, NY, USA, 2016, pp. 1–8.
[76] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," in *Proc. ASE BigData SocialInform. (ASE BD&SI)*, New York, NY, USA, 2015, pp. 28:1–28:6.
[77] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. 2nd Int. Conf. Future Internet Things Cloud (FiCloud)*, May 2016, pp. 464–470.
[78] A. S. Gomes *et al.*, "Edge caching with mobility prediction in virtualized LTE mobile networks," *Future Generat. Comput. Syst.*, vol. 70, pp. 148–162, May 2016.
[79] H. S. Gunawi *et al.*, "Why does the cloud stop computing?" in *Proc. 7th ACM Symp.*, New York, NY, USA, 2016, pp. 1–16.
[80] C. C. Byers and P. Wetterwald, "Fog computing: Distributing data and intelligence for resiliency and scale necessary for IoT," in *Proc. Ubiquity*, Nov. 2015, pp. 1–12.
[81] N. Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, "Privacy mediators: Helping IoT cross the chasm," in *Proc. 17th Int. Workshop Mobile Comput. Syst. Appl. (HotMobile)*, New York, NY, USA, 2016, pp. 39–44.
[82] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. WASA*, 2015, pp. 685–695.
[83] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *Proc. Fed. Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Sep. 2014, pp. 1–8.
[84] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, vol. 6223. 2010, pp. 465–482.
[85] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based authentication and authorization for the IP-based Internet of Things," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2014, pp. 284–292.
[86] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 3–16, Sep. 2015.
[87] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in *Proc. 3rd IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Mar. 2015, pp. 109–118.
[88] V. Cerf and M. Senges, "Taking the Internet to the next physical level," *Computer*, vol. 49, no. 2, pp. 80–86, Feb. 2016.
[89] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 603–608.
[90] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, and P. Dutta, "The Internet of Things has a gateway problem," in *Proc. 16th Int. Workshop*, New York, NY, USA, 2015, pp. 27–32.
[91] M. Zhanikeev, "A cloud visitation platform to facilitate cloud federation and fog computing," vol. 48, no. 5, pp. 80–83, 2015.
[92] A. M. Rahmani *et al.*, "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generat. Comput. Syst.*, Feb. 2017. [Online]. Available: http://sciencedirect.com
[93] O. Bibani *et al.*, "A demo of IoT healthcare application provisioning in hybrid cloud/fog environment," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2016, pp. 472–475.
[94] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in Internet of healthcare things," *IEEE Access*, vol. 4, pp. 8418–8441, 2016.
[95] *About Continua*, accessed on Aug. 30, 2016. [Online]. Available: http://www.continuaalliance.org/about-continua
[96] *Openfog Consortium*, accessed on Nov. 24, 2016. [Online]. Available: http://www.openfogconsortium.org/

FRANK ALEXANDER KRAEMER received the Dipl.-Ing. degree in electrical engineering and the M.Sc. degree in information technology from the University of Stuttgart, Germany, and the Ph.D. degree in model-driven development of systems from the Department of Telematics, Norwegian University of Science and Technology (NTNU), in 2008. He is currently an Associate Professor with the Department of Information Security and Communication Technology, NTNU. His current research interests include architecture and development of Internet of Things applications, as well as adaptive and autonomic sensor systems and their application in various domains, including healthcare.

ANDERS EIVIND BRATEN received the degree in computer engineering from the Sor-Trondelag University College in 2000, and the Cand.Scient. degree in computer science from the Norwegian University of Science and Technology (NTNU) in 2006. He is currently pursuing the Ph.D. degree in telematics with the Department of Information Security and Communication Technology, NTNU. He was a Consultant in the IT-Industry, and he has been involved in numerous development projects in Norway. His research interests include constrained network applications in the Internet of Things, software adaption, self-management, and autonomic computing.

NATTACHART TAMKITTIKHUN received the B.Sc. degree in information and communication technology and the M.Sc. degree in computer science from the Faculty of Information and Communication Technology, Mahidol University, Thailand, in 2009 and 2015, respectively.

He is currently pursuing the Ph.D. degree in telematics with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway. His current research interests include Internet of Things technologies, wireless sensor systems, and energy-efficient embedded systems.

DAVID PALMA received the Ph.D. degree in information science and technology from the University of Coimbra. He was a Researcher and a Project Manager at OneSource, as well as an invited Assistant Professor with the University of Coimbra. He is an H2020 Marie Curie Post-Doctoral Fellow at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology. His current research interests are on routing, IoT, cloud-computing, and software-defined networks, subjects on which he has authored and co-authored multiple papers in refereed conferences and journals. He has participated in several TPCs, national and international research projects, including European Projects (FP6/FP7/H2020) and the preparation of successful research proposals.