IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 2, 2017, accepted November 6, 2017, date of publication November 29, 2017,
date of current version December 22, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2775180

Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities

STEPHANIE B. BAKER[1], WEI XIANG[2], (Senior Member, IEEE), AND IAN ATKINSON[3]

[1]College of Science and Engineering, James Cook University, Townsville, QLD 4811, Australia
[2]College of Science and Engineering, James Cook University-Cairns Campus, Cairns, QLD 4870, Australia
[3]eResearch Centre at James Cook University, Townsville, QLD 4811, Australia

Corresponding author: Stephanie B. Baker (stephanie.baker@my.jcu.edu.au)

ABSTRACT Internet of Things (IoT) technology has attracted much attention in recent years for its potential to alleviate the strain on healthcare systems caused by an aging population and a rise in chronic illness. Standardization is a key issue limiting progress in this area, and thus this paper proposes a standard model for application in future IoT healthcare systems. This survey paper then presents the state-of-the-art research relating to each area of the model, evaluating their strengths, weaknesses, and overall suitability for a wearable IoT healthcare system. Challenges that healthcare IoT faces including security, privacy, wearability, and low-power operation are presented, and recommendations are made for future research directions.

INDEX TERMS Biomedical engineering, body sensor networks, intelligent systems, Internet of Things (IoT), communications standards, security, wearable sensors.

I. INTRODUCTION

Healthcare is an essential part of life. Unfortunately, the steadily aging population and the related rise in chronic illness is placing significant strain on modern healthcare systems [1], and the demand for resources from hospital beds to doctors and nurses is extremely high [2]. Evidently, a solution is required to reduce the pressure on healthcare systems whilst continuing to provide high-quality care to at-risk patients.

The Internet of Things (IoT) has been widely identified as a potential solution to alleviate the pressures on healthcare systems, and has thus been the focus of much recent research [3]–[7]. A considerable amount of this research looks at monitoring patients with specific conditions, such as diabetes [5] or Parkinson's disease [6]. Further research looks to serve specific purposes, such as aiding rehabilitation through constant monitoring of a patient's progress [7]. Emergency healthcare has also been identified as a possibility by related works [8], [9], but has not yet been widely researched.

Several related works have previously surveyed specific areas and technologies related to IoT healthcare. An extensive survey is presented in [10], with focus placed on commercially available solutions, possible applications, and remaining problems. Each topic is considered separately, rather than as part of an overarching system. In [11], data mining, storage, and analysis are considered, with little mention of integration of these into a system. Sensor types are compared in [12], with some focus placed on communications. However, it is hard to draw an image of a complete system from this paper. Finally, in [9], sensing and big data management is considered, with little regard for the network that will support communications.

This paper therefore makes a unique contribution in that it identifies all key components of an end-to-end Internet of Things healthcare system, and proposes a generic model that could be applied to all IoT-based healthcare systems. This is vital as there are still no known end-to-end systems for remote monitoring of health in the literature.

This paper further provides a comprehensive survey of the state-of-the-art technologies that fall within the proposed model. Focus is placed on sensors for monitoring various health parameters, short- and long-range communications standards, and cloud technologies. This paper distinguishes itself from the previous major survey contributions by considering every essential component of an IoT-based healthcare system both separately and as a system.

Further original contribution is made by placing focus on LPWANs, highlighting their unique suitability for use in IoT systems. The upcoming licensed-band standards, such as NB-IoT, are compared with the competing unlicensed-band standards, with particular interest in suitability for healthcare applications.

The remainder of this paper is structured as follows. Section II investigates the field of Internet of Things, placing focus on the provision of healthcare using IoT technologies. Section III examines common sensors that could be used in an IoT healthcare systems, presenting several state-of-the-art sensors that have been developed in recent research. Section IV reviews communications standards for both short- and long-term communications, including a thorough analysis of the new NB-IoT standard for long-range machine-to-machine (M2M) communications. Section V discusses cloud technologies and the ways in which they can be used in IoT healthcare systems. Section VI highlights areas requiring further research and provides recommendations for this research. Section IX concludes the paper, summarizing the key findings and reiterating the areas where further research is required.

II. HEALTHCARE AND THE INTERNET OF THINGS

The Internet of Things remains a relatively new field of research, and its potential use for healthcare is an area still in its infancy. In this section, the Internet of Things is explored and its suitability for healthcare is highlighted. Several pioneering works towards developing healthcare IoT systems are discussed. Building on the recurring themes from these works, a generic and standardized model for future end-to-end IoT healthcare systems is proposed, with the aim of guiding the future development of such systems.

A. THE INTERNET OF THINGS

Many definitions of the Internet of Things exist, but at the most fundamental level it can be described as a network of devices interacting with each other via machine to machine (M2M) communications, enabling collection and exchange of data [7], [10], [11]. This technology enables automation within a large range of industries, as well as allowing for the collection of big data.

Hailed as the driver of the Fourth Industrial Revolution [13], Internet of Things technology has already found commercial use in areas such as smart parking [14], precision agriculture [15], and water usage management [16]. Extensive research has also been conducted into the use of IoT for developing intelligent systems in areas including traffic congestion minimization [17], structural health monitoring [18], crash-avoiding cars [19], and smart grids [20].

While the aforementioned fields appear vastly different to healthcare, the research conducted within them verifies the plausibility of an IoT-based healthcare system. Existing systems in other fields have proven that remote monitoring of objects, with data collection and reporting, are achievable. This can therefore be expanded and adapted for monitoring the health of people and reporting it to relevant parties such as caretakers, doctors, emergency services, and healthcare centers.

B. INTERNET OF THINGS HEALTHCARE

Research in related fields has shown that remote health monitoring is plausible, but perhaps more important are the benefits it could provide in different contexts. Remote health monitoring could be used to monitor non-critical patients at home rather than in hospital, reducing strain on hospital resources such as doctors and beds. It could be used to provide better access to healthcare for those living in rural areas, or to enable elderly people to live independently at home for longer. Essentially, it can improve access to healthcare resources whilst reducing strain on healthcare systems, and can give people better control over their own health at all times.

In fact, there are relatively few disadvantages of remote health monitoring. The most significant disadvantages include the security risk that comes with having large amounts of sensitive data stored in a single database, the potential need to regularly have an individual's sensors recalibrated to ensure that they're monitoring accurately, and possible disconnections from healthcare services if the patient was out of cellular range or their devices ran out of battery. Fortunately, these issues are all largely solvable, and are already being addressed in the literature, as will be highlighted throughout the remainder of this paper. As progress continues to be made to reduce the disadvantages, IoT-based systems for remote health monitoring are becoming an increasingly viable solution for the provision of healthcare in the near future.

As a result of the many benefits of remote health monitoring, many recent researchers have identified the potential of the Internet of Things as a solution for healthcare. In several works, IoT healthcare systems have been developed for specific purposes, including rehabilitation, diabetes management, assisted ambient living (AAL) for elderly persons, and more. While these systems have been designed for many different purposes, they are each strongly related through their use of similar enabling technologies.

Rehabilitation after physical injury has been a topic of particular interest for several researchers. In [7], a system has been developed that generates a rehabilitation plan tailored to an individual based on their symptoms. The patient's condition is compared with a database of previous patients' symptoms, ailments, and treatments to achieve this. The system requires a doctor to manually enter symptoms, and approve the recommended treatment; in 87.9% of cases, the doctor agreed completely with the system, and no modifications were made to the treatment plan it proposed.

Meanwhile, in [21], mathematical models for the measurement of joint angles in physical hydrotherapy systems are proposed, enabling the improvement of joint movement to be tracked through therapy.

In [6], existing IoT technologies are evaluated for their usefulness in a system for monitoring patients suffering from Parkinson's Disease. Their work concludes that wearable sensors for observing gait patterns, tremors, and general activity levels could be used in combination with vision-based technologies (i.e. cameras) around the home to monitor progression of Parkinson's Disease. Furthermore, the authors suggest that machine learning could lead to enhanced treatment plans in the future.

A practical system for the monitoring of blood-glucose levels in diabetic patients was proposed in [5]. This system requires patients to manually take blood-glucose readings at set intervals. It thereafter considers two kinds of blood-glucose abnormalities. The first is abnormal blood-glucose levels and the second is a missed blood-glucose reading. The system then analyses the severity of the abnormality, and decides who to notify; the patient themselves, caregivers and family members, or emergency healthcare providers such as doctors. This system is practical and has been proven realizable, though could be further improved by automating blood-glucose measurements.

A system aimed at detecting heart attacks was built using ready-made components and a custom antenna in [22]. An ECG sensor is used to measure heart activity, which is processed by a microcontroller. This information is forwarded via Bluetooth to the user's smartphone, where the ECG data is further processed and is presented in a user application. The authors identify that developing heart attack prediction software would improve the system. Further improvements could be made by measuring respiratory rate, which is known to aid in the prediction of heart attack [23].

SPHERE [4] is a system under continuing development that utilizes wearable, environmental, and vision-based (i.e. camera) sensors for general activity and health monitoring purposes. The aim of this project it to allow older and chronically ill patients to live in the comfort of their own homes, while their health continues to be monitored. This allows for intervention by caretakers and doctors if any issues arise. Researchers working on the project have identified that machine learning would be beneficial for learning about conditions and for making decisions about the patient's healthcare.

C. A MODEL FOR FUTURE INTERNET OF THINGS HEALTHCARE SYSTEMS

After reviewing this wide range of existing IoT-based healthcare system, several requirements for the design of such systems become apparent. Each of these papers emphasize the use of sensors for monitoring patient health. All regard wearable sensors, namely wireless and externally-wearable sensors, as essential to their respective systems. Several works [4], [6] also suggest the use of environmental or vision-based sensors around the home. However, this restricts the usefulness of the system to one physical location. It would be preferable to implement all essential sensors as small, portable, and externally wearable nodes. This would provide patients with a non-intrusive and comfortable solution that is capable of monitoring their health wherever they go. This would make patients more receptive to using health monitoring technology than they would be if implantable sensors or cameras were required. Additionally, repairing or replacing externally wearable nodes would be simple when compared to implanted sensors or vision-based sensors installed in the home.

Existing systems highlight that communications are also essential for an Internet of Things healthcare system. In several existing system models [5], [6], [22], short-range communications, such as Bluetooth, are suggested for transferring sensor data to a smartphone to be processed. Long-range communications such as LTE can then be used to transfer the processed information from the patient to the healthcare provider, typically a doctor, through SMS or the Internet. The key limitation of this is that smartphones typically have limited battery life, requiring frequent recharging; a patient with a flat battery would be a patient disconnected from healthcare providers. A low-powered node designed specifically for managing healthcare information would be preferable.

Cloud storage capable of storing high volumes of varying data was also shown to be essential to a big data healthcare system by several previous works [9], [11], [24]. If even a thousand people wore a single pulse sensor that communicated hourly with a cloud storage database via an LPWAN, there would be 168,000 new data points per week. This number increases drastically as more people wear sensors connected to the cloud storage framework, and as more kinds of sensors are introduced. Using the big data that will rapidly form and continue to grow in cloud storage, machine learning algorithms can be implemented in the high-computing environment of the cloud. These algorithms could be designed to mine through the large amount of data, identify previously unknown disease trends, and provide diagnostics, treatment plans, and much more.

Based on these recurring trends in the literature to date, we propose and recommend a four-part model as highlighted in Figure 1 that will aid in the development of future Internet of Things healthcare systems, discussed below. In the following sections, each of the components of the proposed model are discussed in further detail. Existing works are presented and evaluated in the relevant sections. Strengths and weaknesses of the current technologies are presented, and recommendations for future directions of research are provided.

1) WEARABLE SENSOR & CENTRAL NODES

Wearable sensor nodes are those that measure physiological conditions. Recommended sensors are those that measure the vital signs - pulse, respiratory rate, and body temperature - as these are the essential signs for determination of critical health. Further sensors that could be implemented are blood pressure and blood oxygen sensors, as these parameters are often taken alongside the three vital signs. Special-purpose sensors such as blood-glucose, fall detection, and joint angle sensors could also be implemented for systems targeting a specific condition.

The central node receives data from the sensor nodes. It processes this information, may implement some decision making, and then forwards the information to an external location. A dedicated central node would be preferred to a smartphone as battery life could be improved by having only functionality relevant to a healthcare IoT system.

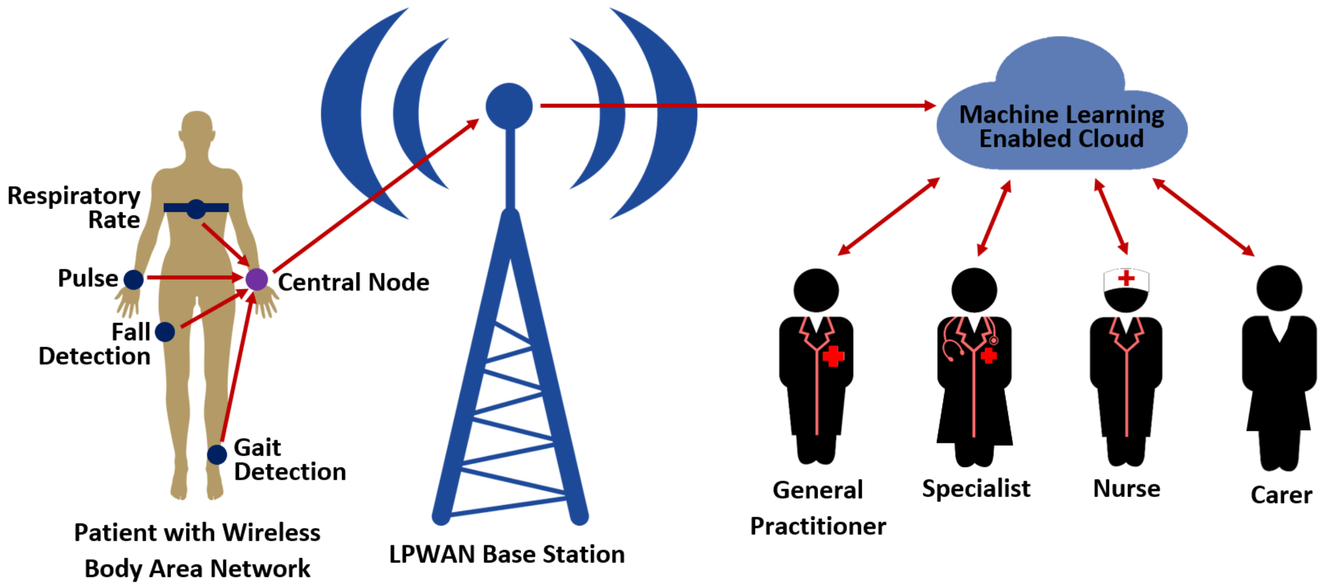


FIGURE 1. Overview of the proposed model.

2) SHORT-RANGE COMMUNICATIONS

For sensors to communicate with the central node, a short-range communications method is required. There are several important requirements to consider when choosing a short-range communications standard, including effects on the human body, security, and latency.

The chosen method should have no negative effects on the human body, as any such effects could cause additional health concerns for patients. It should also provide strong security mechanisms to ensure that sensitive patient data cannot be accessed by an attacker. Finally, low-latency is essential for time-critical systems, such as a system that monitors critical health and calls for an ambulance if the need arises. In such systems, time delays could be the difference between life and death. In applications that are not time-critical, low-latency would not need to be prioritized as highly, but is still preferable.

3) LONG-RANGE COMMUNICATIONS

Data obtained by the central node is not useful unless something can be done with it. This data should be forwarded to a database where relevant parties (such as caretakers or doctors) can securely access it. There are again several considerations when selecting a suitable long-range communications standard for use in a healthcare system, including security, error correcting capabilities, robustness against interference, low-latency, and high availability.

As with short-range communications, strong security is important to ensure that sensitive patient data remains private and cannot be altered or imitated. Low-latency is again important in time-critical applications, such as emergency healthcare, where delays in communication could have detrimental effects on patients. High-quality error correcting capabilities and significant robustness against interference are essential, as these ensure that the message sent is the same as the message received. This is important in all healthcare applications, but particularly in emergency situations. Lastly, high availability is essential to ensure that messages will be delivered at all times, regardless of where the patient is physically located. Again, this is of particular importance to time-critical applications, but is preferable for all systems.

4) SECURE CLOUD STORAGE ARCHITECTURE & MACHINE LEARNING

Medical information obtained from patients must be stored securely for continued use. Doctors benefit from knowing a patient's medical history, and machine learning is not effective unless large databases of information are available to it. Based on the literature, cloud storage is the most viable method for storing data. However, providing accessibility for healthcare professionals without compromising security is a key concern [25], [26] that should be addressed by researchers developing healthcare IoT systems.

Additionally, machine learning has repeatedly been identified in the literature as a means for improving healthcare systems [4], [6], [7], though it has not been widely explored. Machine learning offers the potential to identify trends in medical data that were previously unknown, provide treatment plans and diagnostics, and give recommendations to healthcare professionals that are specific to individual patients. As such, cloud storage architectures should be designed to support the implementation of machine learning on big data sets.

D. POTENTIAL USE CASES FOR THE PROPOSED MODEL

The generic model we have proposed for guiding development of future Internet of Things healthcare systems has a number of use cases. To provide context, this subsection discusses several of these use cases, which include aiding rehabilitation, assisting management of chronic conditions, monitoring changes in people with degenerative conditions, and monitoring critical health for the provision of emergency healthcare.

Following our proposed model, a rehabilitation system for knee injuries could be developed by using wearable accelerometer sensors on either side of the knee, to allow for the position and angle of the knee to be calculated. These measurements could be recorded during several activities, such as normal walking and rehabilitation exercises. They could be communicated via short-range communications to a comfortable, wrist-wearable central node, which could then forward information to the cloud via long-range communications. In the cloud, a record of the patient's progress will continue to expand with each received message. Machine learning algorithms could be implemented to identify the patient's progress, predict when they will be fully rehabilitated, and determine whether any exercises are working better than others. This system could easily be adapted for other or additional injuries by modifying which wearable sensors are used.

Our model could also be used to develop a system capable of assisting with the management of chronic conditions such as hypertension. Blood pressure could be monitored at several locations on the body at set intervals throughout the day and communicated to the cloud via a wrist-worn central node. Again, a comprehensive record of the patient's blood pressure could be built and machine learning could be used to identify trends such as when the patient's blood pressure is highest. This information could also be used to determine optimal times for the patient to take any medication that they may require to manage their condition, and remind the patient of that using a buzzer or alarm on the central node.

Changes in people with progressive conditions such as Parkinson's Disease could also be monitored using a system designed in accordance with our model. Symptoms of Parkinson's Disease include slowed movement, tremors, gait problems, and balance problems [27]. Using a series of wearable accelerometers, sensors could be developed to measure each of these parameters. Readings could be taken at set intervals every day and forwarded to the wrist-worn central node, which in turn forwards the data onto the cloud. As the data from the patient begins to grow, machine learning can be used to identify the rate at which symptoms are worsening for the patient. A doctor could also add records of which treatments are being used, and machine learning could be used to identify which treatments the patient's condition has responded the best to.

Finally, critical health could be monitored using a system comprised of wearable sensors that monitor vital and other important signs, including pulse, respiratory rate, body temperature, and blood pressure. Measurements can be taken regularly, and if any of these parameters fall below the known healthy thresholds then the central node can forward the information to the cloud, which can be used to notify emergency services. Readings at the time of the emergency can be recorded in the patient's health record in the cloud, and the doctor can append information regarding their diagnosis. As more and more people suffer from emergency health conditions and have diagnoses added to their files, machine learning could begin to be used to make connections between symptoms and possible diagnoses. This information could then be provided to responding paramedics, ensuring that patients receive the most appropriate care for their condition, and rapidly. The authors intend to work on this system in their future works.

These are only a few of the possible use cases for systems that could be developed based on the proposed model. Nonetheless, these use cases highlight the versatility of the model, and the number of different situations it could be used to managed.

III. WEARABLE HEALTHCARE SYSTEMS

WBANs have been identified as a key component of a healthcare system founded on Internet of Things technology, and as such the development of accurate sensors with low form factor are essential for the successful development of such a system. In this article, we focus on sensors that are non-obtrusive and non-invasive; we exclude sensors such as implantables. Considered are five fundamental sensors - three for monitoring the vital signs of pulse, respiratory rate, and body temperature, and a further two for monitoring blood pressure and blood oxygen, both commonly recorded in a hospital environment.

A. PULSE SENSORS

Perhaps the most commonly read vital sign, pulse can be used to detect a wide range of emergency conditions, such as cardiac arrest, pulmonary embolisms, and vasovagal syncope. Pulse sensors have been widely researched, both for medical purposes and for fitness tracking.

Pulse can be read from the chest, wrist, earlobe, fingertip, and more. Earlobe and fingertip readings provide high accuracy, but are not highly wearable. A chest-worn system is wearable, but wrist sensors are generally considered most comfortable for a long-term wearable system [28].

Commercially, several fitness tracking chest straps and wrist watches are available with pulse measurement functionality. These include HRM-Tri by Garmin [29], H7 by Polar [30], FitBit PurePulse [31], and TomTom Spark Cardio [32]. However, these companies all disclose that their devices are not for medical use and should not be relied upon for detecting health conditions. As such, the sensing systems employed by these devices cannot be directly implemented into a critical health monitoring system.

Much research has been conducted into suitable methods for sensing pulse. Sensor types developed, used, and analyzed in recent works include pressure, photoplethysmographic (PPG), ultrasonic, and radio frequency (RF) sensors.

PPG sensors operate by an LED transmitting light into the artery, with a photodiode receiving the amount not absorbed

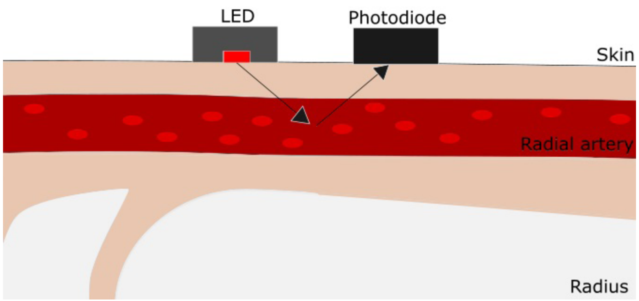


FIGURE 2. Photoplethysmographic pulse sensor.

by the blood, as shown in Figure 2. Changes in the amount of light can be recorded and a pulse rate can thus be determined.

In [28], PPG sensors are used to measure pulse, pulse rate variability, and blood oxygen in one small wrist-wearable sensor. As motion affects the accuracy of pulse readings from PPG sensors, an accelerometer is used to check for movement. When motion is high, the device goes into a low power state and does not record pulse. This is not entirely suitable as pulse may be relevant when motion is high, such as when a person is seizing or suffering cardiac issues during exercise. Improving the accuracy of pulse sensors during motion would be preferred to disregarding readings when movement levels are high.

In [33], the effects of motion on PPG sensors are reduced by using two different LED light intensities and comparing the amount of light received at the photodiode. Significant improvement in signal quality is seen as motion artefacts are greatly reduced through this technique.

Pressure sensors aim to mimic a healthcare professional manually reading the radial pulse by pressing down with their fingers. As shown in Figure 3, the sensor is placed firmly against the wrist, and pressure is continuously measured to acquire a pulse waveform.

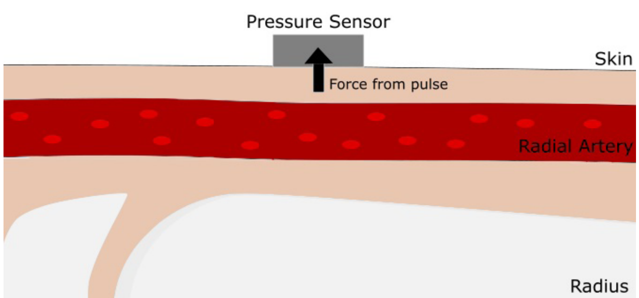


FIGURE 3. Pressure-based pulse sensor.

In [34], a flexible and highly-sensitive pressure sensor for pulse detection is developed and tested, showing promising results. However, increasing the sensitivity to better detect pulse also increases the amount of noise that is detected due to movement of the wearer. This sensor was tested in at-rest conditions, and further research would be required to determine that it performed well during motion.

Pressure sensors and PPG sensors are combined in [35] and [36], where pulse sensor modules are developed with arrays of nine PPG sensors and one pressure sensor. Pulse is taken from multiple points on the wrist, providing clear pulse readings and the potential to use these readings for diagnostics of certain diseases such as diabetes.

Diagnostics through pulse sensing is also investigated in [37], where pressure, PPG, and ultrasonic sensors are compared. Reasonable accuracy was achieved with all three, but the authors concluded that specific diseases required diagnosis using different sensor types; pressure was found to be best for arteriosclerosis, while ultrasonic was superior for diabetes.

An *et al.*, designed a non-conventional pulse sensor using an RF array module in [38], with the aim of measuring several locations on the wrist in case the received pulse signal at one point becomes noisy due to movement. Reasonable pulse readings were achieved when compared to a reference signal, but still do not appear as clear as those obtained with the traditional sensor types. This type of pulse sensor shows promise, but further work is clearly required to make it reliable in a critical healthcare scenario.

Based on these works, it is strongly recommended that PPG sensors are used for pulse sensing. These have repeatedly been proven to be effective for measuring pulse rate, and techniques have already been developed to algorithmically reduce the impacts of noise on the signal quality.

B. RESPIRATORY RATE SENSORS

Another of the vital signs is respiratory rate, or the number of breaths a patient takes per minute. Monitoring respiration could aid in the identification of conditions such as asthma attacks, hyperventilation due to panic attacks, apnea episodes, lung cancer, obstructions of the airway, tuberculosis, and more.

Due to the importance of respiration, many previous works have developed sensors for measuring respiratory rate. In inspecting the previous works, several types of respiratory rate sensor emerge. The first is a nasal sensor based on a thermistor, as is used in [39]. The principle that these sensors are based on is that air exhaled is warmer than the ambient temperature. As such, the sensor uses the rise and fall of temperature to count the number of breaths taken. This is shown to work reasonably well, but accuracy may be compromised by other sources of temperature fluctuations - for example if worn by a chef working in a kitchen. It is also not highly wearable, as it is obstructive and easily noticeable.

Echocardiogram (ECG) signals can also be used to obtain respiration rate. This is called ECG Derived Respiration (EDR), and is used in [40] to determine respiration patterns and detect apnea events. This method reads respiratory rate reasonably well, but is again limited by the wearability. ECG contacts are uncomfortable and would likely cause irritation to the skin if used continuously. Additionally, ECG contacts are not reusable and would need to be regularly replaced.

Respiratory rate can also be calculated using a microphone to detect respiration, as was done in [41]. In this study, focus was placed on detecting wheezing - a symptom common in asthmatics. The limitation of using a microphone is that it would be extremely susceptible to any external noise, and would therefore not be suitable as a long-term wearable.

One study [42] developed a fiber optic sensor in an elastic substrate, that was sensitive enough to measure vibrations caused by respiration. This was shown to work in a single test, but it is not known whether it would work well under all conditions. It is likely that this sensitive material would be susceptible to noise from other sources of vibration, including walking. Further testing should be conducted.

A pressure-type sensor was developed in [43]. Two capacitive plates are placed in parallel, with one resting on the abdomen. During breathing, the plates move further apart and then closer together during inhalation and exhalation respectively, allowing for calculation of respiratory rate. This study showed a 95% confidence in respiratory rate calculations when compared to a nasal sensor. This is fairly accurate, and far more wearable than the nasal sensor it was compared to. However, the nature of a pressure sensor may mean it is susceptible to noise if it is affected by external pressures, such as while walking into wind.

A common method of measuring respiratory rate is to use a stretch sensor, as was done in [44]–[46]. Stretch sensors are those where properties change in response to the application of tensile force, such as being stretched during inhalation.

In [44], the designed sensor was made from a ferroelectric polymer transducer, which generated a charge when a tensile force was applied. Measuring the changes in this charge allow for calculation of respiratory rate. This sensor appeared to obtain a clear signal, but accuracy was not verified through comparison with respiratory rate calculated by other means. In [45] and [46], the respiratory rate sensors were based on changes in resistance. When a tensile force is applied to the sensor, resistance increases. The changes in voltage caused by varying resistances can be used to calculate the breathing rate.

Each of the stretch sensor types was shown to be effective in calculating respiratory rate, but Atalay *et al.* [45] admit that motion artifacts were present during walking and other movements. Additionally, in [46] it was found that breathing was accurate within 3.3 breaths per minute when sitting at a desk; the margin of error increased when movement was introduced. Therefore, a limitation of these sensors is that other movements can cause tensile force to be applied to the sensor in such a way that the sensor mistakes the movement for breathing.

Evidently, many different sensor types exist for measuring respiratory rate. The main factor in choosing a sensor type for a WBAN thus becomes the wearability. Therefore, stretch sensors are strongly recommended for implementation into future systems. Future work should focus on developing algorithms and techniques to improve robustness against motion using these sensors, rather than on developing new sensors entirely.

C. BODY TEMPERATURE SENSORS

The third vital sign is body temperature, which can be used to detect hypothermia, heat stroke, fevers, and more. As such, body temperature is a useful diagnostics tool that should be included in a wearable healthcare system.

Recent works surrounding the measurement of body temperature all use thermistor-type sensors. In [46] and [47], the common negative-temperature-coefficient (NTC) type temperature sensors were used, while positive-temperature-coefficient (PTC) sensors were considered in [48] and [49]. In all studies, the thermistors were shown to measure a suitable range of temperatures for monitoring the human body, with acceptable levels of error. Therefore, it is strongly recommended that these sensor types continue to be used by future system designers.

The accuracy of temperature sensing is limited by how closely the sensor can be placed to the human body. As such, several works [48], [49] focused on developing sensors printed onto thin, flexible polymers with adhesive backing that could be attached directly to human skin. Whilst this is an interesting advancement, the work in [46] shows that temperature can also be measured with relative accuracy using a temperature sensor embedded in textiles. Thus, it is recommended that system designers should use textiles to hold temperature sensors until electronics printed on flexible polymer can be more easily manufactured.

D. BLOOD PRESSURE

Whilst not a vital sign itself, blood pressure (BP) is frequently measured alongside the three vital signs. Hypertension (high BP) is a known risk factor for cardiovascular disease, including heart attack. It is also one of the most common chronic illnesses, affecting 32% of adult Australians. Of those affected, 68% had uncontrolled or unmanaged hypertension [50]. As such, incorporating BP into a WBAN for healthcare would provide vital information for many patients.

Nonetheless, designing a wearable sensor for continuously and non-invasively monitoring blood pressure remains a challenge in the field of healthcare IoT. A significant number of works [51]–[54] have attempted to obtain an accurate estimate of BP through calculation of pulse transit time (PTT) - the time taken between pulse at the heart and pulse at another location, such as the earlobe or radial artery. Another work endeavored to measure this property between the ear and wrist [55], while another looked to calculate it between the palm and the fingertip of a hand [56]. PTT is known to be inversely proportional to systolic blood pressure (SBP), and is typically determined using an electrocardiogram on the chest and a PPG sensor on the ear, wrist, or alternate location.

The outcomes of each of these works indicate that the use of PTT to calculate BP is not yet suitable. PTT is dependent on several other factors, including arterial stiffness and blood density [54]. In ideal conditions, where devices had been calibrated to the individual and the individual remained relatively still during testing, reasonable results were acquired by the aforementioned studies that utilized one measurement at the chest and another at the wrist. Measurements taken between the ear and wrist were shown to be inaccurate in [55]. Additionally, PTT was measured with reasonable accuracy between the palm and fingertip in [56], but the study did not manage to convert this to blood pressure. This should be investigated further, given some promise was shown in measuring PTT and given that the design is the most wearable option for monitoring blood pressure presented in this survey. For systems measuring between the heart and wrist, one study identified that regular recalibration of devices would likely be required as the human body changes over time [51].

Another issue with these types of systems is that, while non-invasive, they are still obstructive. Usually a chest-wearable ECG is required in addition to some other device, and the connection between them may be wired. One study [55] identified this issue and opted to use two easily wearable PPG sensors - one on the earlobe, and one on the wrist - to estimate pulse arrival time (or time taken to travel) between these locations and thus estimate blood pressure. The results were promising, showing reasonable measurements for healthy subjects in different positions (such as sitting and standing). However, the measurements taken were not compared to measurements from a traditional cuff-based sphygmomanometer. Such comparison would aid in analyzing the accuracy of the PPG-based system.

While no system has yet been developed for accurately measuring blood pressure continuously using a comfortably wearable device, this is a field worthy of further research. It is suggested that this could be achieved by developing a device that utilizes two or more PPG sensors placed along the arm to calculate PTT. Blood pressure is certainly a valuable parameter in healthcare, and the ability to monitor it continuously would greatly improve the quality of healthcare that could be provided through a WBAN-based system.

E. PULSE OXIMETRY SENSORS

Pulse oximetry measures the level of oxygen in the blood. Like blood pressure, blood oxygen level is not a vital sign, but does serve as an indicator of respiratory function and can aid in diagnostics of conditions such as hypoxia (low oxygen reaching the body's tissues). As such, pulse oximetry is a valuable addition to a general health monitoring system.

Pulse oximeters measure blood oxygen by obtaining PPG signals. Usually, two LEDs - one red, one infrared - are directed through the skin. Much of this light is absorbed by the hemoglobin in the blood, but not all. The amount of light not absorbed is measured by receiving photodiodes, and the difference between the received lights is used to calculate blood oxygen. As highlighted in Figure 4, LED lights can either be passed through an appendage (normally a finger) to a photodiode on the opposite side, or can be directed at an angle so that some light reflects to a photodiode on the same side of the appendage. These are called absorbance-mode and reflectance-mode PPG sensors respectively.

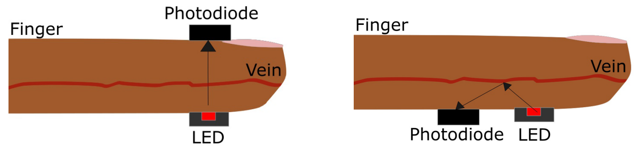


FIGURE 4. Absorbance-mode vs. reflective-mode PPG sensors for pulse oximetry.

Classically, pulse oximeters are worn as a finger clip wired to a medical monitor. Several recent works have attempted to make more portable devices. In [57], a low-power pulse oximeter is designed with the aim of improving wearability. Two techniques are used to reduce power consumption. The first - named ''minimum SNR tracking'' - continuously calculates the current signal-to-noise-ratio (SNR) and adjusts the length of time that the LED is in the ''on'' state for accordingly - the higher the SNR is, the longer that the LED needs to be on to gain accurate readings. The second, named ''PLL tracking'', estimates when the peaks and troughs of the PPG signal are likely to occur, and samples only at these times to acquire this important information. Up to 6x less power was consumed through implementing both techniques, and the worst error recorded was a 2% difference between actual and measured blood oxygen levels. This is a significant contribution towards making pulse oximeters more wearable, but reductions in the level of error are desirable.

An in-ear reflective pulse oximeter was designed in [58]. This was designed to detect blood oxygen levels even when the patient is suffering from shock, hypothermia, or other conditions that may cause blood centralization and lead to pulse being undetectable at the fingertips. The oximeter sits inside the ear canal without sealing it, ensuring there is no disruption to hearing. Reasonable accuracy in measuring blood oxygen levels was achieved in clinical testing on surgical patients, but the authors concluded that their sensor should be used in addition to finger pulse oximeters, not as an alternative. This is a sensible idea for wearable healthcare systems that are providing remote care, as it would be preferable to detect when centralization is occurring.

The most wearable option would be a wrist-worn sensor, as many people are accustomed to wearing bracelets or watches and would not find this uncomfortable. In [59], a reflective pulse oximeter was designed to be worn on the wrist. The design is concave in shape, blocking out much external light and improving robustness against noise. The trade-off is that it makes the device larger, but size reductions are then made by performing data processing off-node. Overall, it is more wearable than other designs, but would still benefit from being miniaturized and made more wearable. Additionally, it could be used to detect pulse and skin temperature as well - combining three essential sensors into a single, comfortably wearable node.

Overall, the works in improving pulse oximetry do not focus on finding new means to measure blood oxygen saturation, but instead focus on making wearable devices that utilize the well-known existing techniques. Research should continue in this direction, focusing on wrist-wearable pulse oximetry.

F. OTHER WEARABLE SENSORS FOR HEALTHCARE

Aside from the sensors that measure critical health parameters, there are several special-purpose wearable sensors that may be useful in systems focused on monitoring a specific condition. Echocardiograms (ECGs) can be used to evaluate heart health, and several wearable sensors have been developed to acquire these signals. In [60], an armband-based ECG sensor was developed and measures with reasonable accuracy. ECG sensors have also successfully been developed for integration in helmets [61] and more traditional chest-straps [62].

The helmet in [61] also features an electroencephalogram (EEG) sensor. EEGs measure brain activity, and could generally be used to monitor seizures, sleep disorders, and progress after a head injury. Other EEG systems have been developed for specific purposes, such as for detecting driver drowsiness [63] or stress management [64]. Both systems measure EEG through a relatively wearable headband.

Fall detection can be useful for monitoring elderly people, as they are particularly prone to falls and resulting injuries. In [65], a tri-axial accelerometer inside a smartphone is used by machine learning algorithms to classify the user's posture, which the best algorithms showing classification accuracy of 99.01%. A related study found that the classification algorithms used for posture detection were much less accurate when performing fall detection [66], suggesting that further training or alternate algorithms may be required for this purpose. In a more recent work on fall detection, a wearable camera was used in [67], with rapid changes in scenery used to detect falls. This showed an accuracy of 93.78% and 89.8% in indoor and outdoor environments respectively. In their earlier work [68], accelerometer data was combined with an earlier version of their wearable camera system, showing 91% accuracy in detecting falls. An accelerometer, a gyroscope, and a magnetometer were used to accurately detect falls in [69], with the authors then adding a barometer to even more accurately detect changes in height in [70]. The latter work showed that fall detection was performed with no lower than 99.38% accuracy and up to 100% accuracy across a series of tests. This is an exceptional result, and suggests that this fall detection system could be implemented into healthcare applications immediately.

Gait detection can also be useful in monitoring the elderly, as well as those with specific conditions such as Parkinson's Disease (PD). Gait detection for those recovering from stroke or suffering from PD was considered in [71], with foot-worn sensors designed to measure many parameters including step size and walking speed. A sensor for gait detection in lower limb amputees was developed in [72], with the aim of future use in controlling lower limb prosthetics. Detection of gait events, rather than general gait patterns, has also been considered in several works. In [73], three accelerometers are placed on the hip, knee, and ankle of advanced Parkinson's Disease sufferers. Features are extracted from the data, and an anomaly detection scheme is used successfully detect freezing of gait, a common Parkinson's symptom that causes a temporary loss of motor function and regularly leads to falls. Detection of any gait anomaly is investigated in [74], where a waist-worn device comprised of a microcontroller and tri-axial accelerometer is used to monitor gait. Through the implementation of feature extraction and an advanced anomaly detection algorithm, a system is created that can detect approximately 84% of gait anomaly periods that last for 5 seconds. Accuracy was higher when detecting severe anomalies.

People living with diabetes are considered in several works aiming to develop a non-invasive blood glucose monitor, none of which currently exist on the market. In [75], an optical sensor measures blood glucose levels through the fingertip, while in [76] an ultrawide band microwave technique is used for blood glucose level detection in an earlobe-attached sensor.

These sensors are not the only special-purpose sensors that have been researched or could be researched, but they are some of the key types. They are applicable to many common diseases or conditions, and should be considered for inclusion by designers of systems that will focus on monitoring of specific ailments.

IV. COMMUNICATIONS STANDARDS

Communications related to Internet of Things for healthcare can be classified into two main categories: short-range communications, and long-range communications. The former is used to communicate between devices within the WBAN, whilst the latter provides connection between the central node of the WBAN and a base station (such as a healthcare provider). In this paper, both types of communications are considered with equal importance.

A. SHORT-RANGE COMMUNICATIONS

In the context of wearable healthcare systems, short-range communications are often used between nodes, particularly between sensor nodes and the central node where data processing occurs. Although short-range communications standards can be used for other purposes (i.e. developing mesh networks for smart lighting), this survey focuses on the purpose of developing a small WBAN that is comprised of only a few sensors and a single central node.

Many short-range communications standards exist, but perhaps the most commonly used ones in IoT are Bluetooth Low Energy (BLE) and ZigBee. The key features of these two standards are highlighted in Table 1, and this section further analyzes these standards and considers their suitability for implementation into an IoT healthcare system.

TABLE 1. Comparison of short-range communication standards.

	Bluetooth Low Energy	ZigBee (XBee Module)
Band of operation	2.4GHz	2.4GHz
Topology	Star	Mesh
Range	150m	30m
Data rate	1Mbps	250kbps
Security Features	Secure pairing prior to key exchange Two keys used to provide authentication and identity protection 128-AES encryption	Optional 128-AES encryption Network key shared across network Optional link key to secure application-layer communications
Suitability for healthcare	High	Moderate

1) BLUETOOTH LOW ENERGY

BLE was developed by the Bluetooth Special Interest Group (SIG) to provide an energy-efficient standard that could be used by coin-cell battery operated devices, including wearables. It also aimed to enable IoT, connecting small peripheral devices to processing devices such as smartphones [77].

BLE is used in a star topology, which is suitable for healthcare applications. The central node would act as the center of the star topology, with sensors linked to it. The sensors will have no need to communicate with each other directly.

The range for BLE is 150m in an open field [77]; it would be much less in non-ideal conditions. It also has a low latency of 3ms, and a high data rate of 1Mbps [78]. The range is clearly sufficient for use in a healthcare WBAN where nodes are physically proximal, and the extremely low latency is ideal for applications such as emergency health.

BLE operates in the 2.4GHz band, a band also used by classic WiFi and ZigBee. This may subject it to some noise, but robustness to interference is implemented through frequency hopping across carefully selected channels and a 24-bit cyclic redundancy check (CRC) [79]. This method makes BLE robust enough to noise for use in a healthcare system.

Power consumption in BLE is extremely low. In [77], it is shown that a 180 mAH coin cell battery could run a BLE chip for 18 continuous hours, making 21.6 million transactions. However, if the chip was powered off when not needed, battery would last much longer. If a health sensor transmitted its data every 30 seconds (or 2,880 times per day), then the battery could theoretically run the BLE chip for around 20.5 years if not for the fact that it would die from self-depletion well before then. With careful hardware design and low-energy programming, BLE would clearly be suitable for healthcare applications.

Security has been implemented in a variety of ways for BLE. Firstly, there are four possible pairing models. The newest and most secure of these, LE Secure Connections, implements a numeric comparison method and an Elliptical Curve Hellman-Diffie (ECHD) algorithm, which uses a public key and private keys unique to each device, to secure key exchange. Two keys are exchanged between master and slave - a Connection Signature Resolving Key (CSRK) and an Identifying Resolving Key (IRK). The former is used to provide authentication for unencrypted data, whilst the latter provides privacy and the device's identity [80]

Encryption is also available in BLE, using Advanced Encryption Standard (AES). Specifically, a 128-bit AES cypher is used to protect the data from potential attackers [80].

Man-in-the-middle, eavesdropping, and identity attacks are effectively protected against by the security features of BLE. This is crucial in a healthcare environment where sensitive patient data is being exchanged.

Classic Bluetooth has previously been used in IoT for healthcare works including a blood pressure monitoring system [81] and a system for early detection of Alzheimer's disease [82], as it has been optimized for IoT; unlike Classic Bluetooth.

Overall, BLE is extremely well suited to healthcare applications. It is secure and features good range, low latency, low power consumption, and robustness to interference. This standard is highly recommended to designers, as it is currently the most suitable standard for implementation into wearable healthcare systems.

2) ZIGBEE

The ZigBee standard was designed by the ZigBee Alliance, specifically for providing low-cost, low-power networks for M2M communications. It builds on the IEEE 802.15.4 physical standard [83]. It is commonly known as the standard for mesh networks, but it can also be used in the star topology required of a WBAN with one central node and many sensing nodes.

Different ZigBee modules provide different characteristics in terms of range, data rate, and power consumption. The simplest XBee has a range of up to 30m in an urban environment, and outputs only 1mW of power for transmission [84].

The XBee Pro has a higher range of 90m in the same conditions, but the transmit power output is significantly higher at 63mW [84], the XBee Pro 900 XSC can reach up to 610m in an urban environment, but with 250mW of power being used to transmit [85]. There are ZigBee-based solutions for a wide variety of applications, but for the use case of a healthcare WBAN the XBee 1mW would be suitable. Only a small range is needed for on-body communications, so choosing the lowest-power solution is preferable.

Data rates are also variable. XBee and XBee Pro have a data rate of up to 250kbps [84], while the XBee Pro 900 XSC has a maximum data rate of only 10kbps [85]. Clearly, the latter module has sacrificed data rate in addition to power efficiency to achieve its long range. In a healthcare environment, it would be preferable to opt for a higher data rate, as this will reduce the latency in the system and ensure critical health data is delivered timely.

ZigBee can operate at a range of frequencies, including 868MHz, 900MHz, and 2.4GHz bands, depending on the module chosen. Each of these bands faces interference. The 2.4GHz band is shared by Bluetooth and WiFi, while many long-range communications systems utilize the unlicensed 868MHz and 900MHz bands in Europe and America respectively. ZigBee uses CSMA-CA to reduce collisions, and implements re-transmission if messages sent are not acknowledged [86].

Several security features are provided by ZigBee, though most are optional and must be enabled by the network developer. ZigBee's security model is largely based on 128-AES encryption, and offers types of security keys - a link key, a network key, and a master key. The network key is mandatory. It is shared by all devices on the network, and is a network-layer security mechanism that cyphers all transmissions within the network. The link key is optional, and is used to secure communications at the application layer. Master keys are also optional, and are used to secure the creation and sharing of link keys [87].

Despite these security measures, a recent study [88] found that it was relatively easy to exploit a ZigBee network during a device join, by sniffing the link key being exchanged. This compromises the network key and thus the entire network. The researchers in this study did identify that the security flaws were not to do with ZigBee itself, but rather with the way that manufacturers implemented key exchange and initialization. If ZigBee is to be implemented in healthcare systems, only ZigBee modules with all optional security mechanisms and robust key management should be used.

ZigBee has already been used in several works relating to healthcare. In [89], a system that detects wandering Alzheimer's patients and alerts their caregivers was developed using a ZigBee mesh network. In [62], a wearable ECG sensor was developed using ZigBee to communicate with a central monitoring device. Improving ZigBee for use in biomedical application was considered in [90], where a low-power transceiver was developed with robustness to interference.

Overall, ZigBee is reasonably well-suited to healthcare applications. It provides robustness to interference and several security mechanisms. Several implementations are possible to optimize range, data rate and power consumption for specific applications. XBee modules were examined as a case study, and it was found that low-power, high data rate modules existed with suitable range for healthcare applications.

The main drawback of using ZigBee is that key exchange can be compromised unless implemented extremely well by the manufacturer. This could pose a risk to healthcare systems where sensitive patient data is being exchanged regularly. Additionally, ZigBee is not commonly implemented in devices such as smartphones, while BLE typically is. This makes it less compatible with existing devices, and therefore it is suggested that it would be better suited to fixed-location, standalone purposes such as home automation than it is to wearable healthcare systems. It is therefore recommended that system designers prefer BLE for wearable sensors over ZigBee, particularly in applications where privacy is critical.

B. LONG-RANGE COMMUNICATIONS

Low-Power Wide-Area Networks (LPWANs) are a subset of long-range communications standards with high suitability for IoT applications. The range of a LPWAN is generally several kilometers, even in an urban environment. This is significantly longer than the range of traditional IoT communications types such as WiFi or Bluetooth, whose ranges are in the order of meters and thus would require extensive and costly mesh networking or similar to be plausible for healthcare.

LPWANs also have significant advantage over cellular networks such as 3G in that they are designed to support short bursts of data infrequently. This is suitable for a large number of healthcare applications, including monitoring general health and receiving hourly updates, monitoring critical health and receiving emergency calls, and rehabilitation where updates may only be necessary once daily. This design principle also allows for low-power device design, which in turn ensures that the designed healthcare devices will operate for longer before human interaction is required to recharge or change batteries. This reduces the risk of patients being offline, and provides more convenience to the wearer. Based on these advantages, it is suggested that LPWANs are the best solution for transmitting data from the central node to the cloud for storage or further processing.

The most prominent standards for LPWANs are Sigfox and LoRaWAN. While these standards are well-established, they face competition from emerging standards including NB-IoT. In this section, existing LPWAN standards are considered in terms of suitability for an IoT healthcare system, and recommendations are made. A table summarizing the three main standards discussed is also included in Table 2 to provide a snapshot of their features, enabling easy comparison between these standards.

TABLE 2. Comparison of long-range communication standards.

	SigFox	LoRaWAN	NB-IoT
Licensed band of operation?	✗	✗	✓
Band of operation	868MHz (Eu) 915MHz (US)	868MHz (Eu) 915MHz (US)	Various - can operate in LTE bands (in-band mode), in the guard bands of LTE (guard-band mode), or in re-farmed GSM bands (standalone mode)
Communication directions	Unlimited uplink. Downlink on request, no more than 4x per day	Uplink & downlink	Uplink & downlink
Network capacity	50,000 nodes	40,000 nodes	53,547+ nodes
Range	9.5km	7.2km	15km
Data rate	100bps	0.25-5.5kpbs	250kbps
Security features	Messages signed with a private key Limit of 140 messages per day Encryption and scrambling methods supported	Unique key assigned to each node on the network, known only to the node and base station Data encrypted using the unique key	3GPP S3 security scheme - includes entity authentication, device identification, user identity confidentiality and data integrity as mandatory security features
Suitability for healthcare	Low	Moderate	High

1) SIGFOX

Perhaps the simplest of the LPWAN standards, Sigfox provides limited functionality but is widely deployed compared to other standards listed. It is a protocol developed in the first four layers of the OSI model, and its base stations bear similarity to those in cellular - antennas mounted on towers.

Sigfox uses a star topology, and nodes are designed to be uplink only to improve battery efficiency. It is possible for a node to receive downlink, but it must explicitly request it. As acknowledgement of receipt is important for health data, downlink would have to be requested. Unfortunately, a limitation of Sigfox is that downlink can only be requested 4 times per day [91].

There is a trade-off in design between latency and range. If a receiver has higher sensitivity, it can detect weaker signals; thus, the distance a signal can travel is increased. Sigfox opted to maximize range to around 9.5km in urban areas [92] by using slow D-BPSK modulation and a low bit rate of 100 bits per second (bps) [93]. In rural areas, Sigfox can reach a range of up to 50km [94]. The high latency of Sigfox is a drawback for its use in healthcare applications, as it is important for messages to be delivered quickly in this critical context.

Sigfox operates in the unlicensed bands of 868MHz in Europe and 915MHz in the US. As with other LPWAN technologies operating in the sub-GHz spectrum, no globally available band exists for Sigfox's use. Operating in an unlicensed band allows Sigfox to occupy a wider bandwidth, but comes with the disadvantage of increased interference, which may be an issue in healthcare.

To increase resistance to interference, Sigfox sends payloads in three consecutive frames, each in different pseudo-random sub-carriers and over different propagation paths. This improves the likelihood that the message will be received intact, and thus reduces the disadvantages of increased interference in the unlicensed bands.

Sigfox has a high network capacity and can support approximately 50,000 nodes with a single gateway [92]. This is comparable to NB-IoT's 52,547 nodes, which has been shown to be able to support 40 devices per household assuming a household density equivalent to London's and an inter site distance of 1732m [95]. In rural areas such as Australia's Burdekin Shire, which had a population of 17,784 people in 2011 [96] and is 4880km^2 in area [97], one well-positioned base station would enable every resident of the region to be connected to healthcare providers via Sigfox. This is significant for healthcare applications, especially in regional areas.

Security is implemented in Sigfox by signing each message with the device's private key [91]. This reduces the risk of spoofing attacks or interception, but does not eliminate it.

A sophisticated attack targeting the node hardware or service provider could still reveal the unique keys, compromising a patient's healthcare system.

The limit of 140 messages per day also minimizes the impact that a spoofing attack could have. However, in a healthcare environment, even a small number of fraudulent messages could have significant impacts on the wellbeing of patients.

Encryption and scrambling methods are supported by Sigfox [91], but developers must implement these themselves within the 12-byte payload. If implemented well, these methods could reduce the risk of sensitive patient data being intercepted.

Overall, Sigfox is suitable for non-critical applications where speed of message delivery and acknowledgements of receipt are non-essential, such as in smart parking and automated street lighting. In such an application, a breach of security would cause annoyance rather than danger. However, in healthcare, successfully transmitting messages with relative speed is essential. Any compromise of security could be detrimental for an individual's health, or could affect the integrity of medical databases. For this reason, we recommend that Sigfox not be used for critical healthcare applications. It is therefore strongly recommended that system designers instead consider alternative LPWANs for critical healthcare applications.

2) LoRa & LoRaWAN

Technical information about the LoRa & LoRaWAN standards is presented in [98], written by the LoRa Alliance. This subsection overviews the key components of the standard based on this source, and thus the interested reader is referred to it for further information about LoRa & LoRaWAN.

LoRa is a physical layer protocol that utilizes chirp spread spectrum techniques over a wide bandwidth of at least 125kHz. This provides low-power, long-range communications with high resilience to intentional or environmental interference.

LoRaWAN is built on top of the LoRa standard, in the network layer. It utilizes a star topology, and nodes are asynchronous; they only communicate when they need to, such as after an event or scheduled measurement. Scheduled messages from nodes would suit long-term monitoring applications, while event-driven messages from nodes would suit emergency monitoring.

LoRaWAN also has a high network capacity, ensuring many messages can be passed over the network at the same time. Each gateway can support approximately 40,000 nodes [92]. While this is lower than the capacity of Sigfox, it would still be suitable for use in urban and regional areas if optimal base station positioning was considered thoroughly.

Already, LoRaWAN has been successfully deployed in several areas including parts of Europe, America, and the Asia-Pacific region. With a maximum link budget of 155 dBm, messages can travel over a range of around 7.2km in an urban area at a rate of 0.25-5.5 kbps. This is a significantly faster data rate than Sigfox, with about 2.3km less range. It is suggested that for healthcare, this trade-off is worthwhile as low latency is essential. More range can be obtained by simply installing more base stations.

To allow consumers to choose a solution that suits them best, LoRaWAN specifies three classes of device that can be used. Class A is the most battery efficient, providing downlink for only a small window after uplink. This would be suitable for healthcare, as downlink would only be required to receive acknowledgement that the health data was delivered.

Like Sigfox, LoRaWAN operates in the unlicensed bands of 868MHz in Europe and 915MHz in the US. This carries the advantage of wider spectrum availability, but also the disadvantage of increased exposure to potential interference.

Security is provided by the LoRaWAN standard. A unique key is assigned to each node on the network; this key is known only to the node and to the network provider. Theoretically, this would eliminate man-in-the-middle attacks as intercepted data would be encoded and not decipherable [99].

Unfortunately, a node's unique key could become a single point of failure for the whole system should the key be discovered through sophisticated hardware hacking of the node, or through an attack on the network server. If a key was illicitly obtained, then the attacker could use it to decipher all future messages from the node, or could send false messages to the base station whilst pretending to be the node.

For the most part, LoRaWAN is reasonably well-suited to healthcare applications due to its range, latency, and network capacity. Interference could potentially cause issues while operating in unlicensed bands, but a more significant issue is that of key management. To be truly secure, proper key management must be implemented by the developers and service providers so that sensitive healthcare data and important medical databases are protected from malicious attacks, as LoRaWAN does not provide a complete security solution.

3) NB-IoT

Standardized in the recent 3GPP Release 13, NB-IoT operates in the licensed bands of GSM or LTE and provides long-range, low-power communications. As NB-IoT has been developed based on LTE, much of the existing LTE hardware can be used to deploy it rapidly and effectively [95], [100].

There are three different ways in which NB-IoT can be deployed, allowing easier coexistence with existing networks. These deployment modes are in-band, guard-band, and stand-alone. Using in-band mode involves reserving LTE Physical Resource Blocks (PRBs) from the existing LTE network, for use by NB-IoT. In guard-band mode, NB-IoT utilizes the bandwidth of an existing LTE carrier's guard-band. Finally, in stand-alone mode, GSM carriers can be re-farmed and used for NB-IoT, or NB-IoT can exist in entirely new bandwidth [101], [102].

Operating within licensed bands has the significant advantage of reduced risk of interference. One potential disadvantage is that there will likely be a higher cost to use NB-IoT than there is for unlicensed standards. Just as mobile phone users pay a fee to be able to use LTE, NB-IoT device users will likely have to pay a connection fee for the use of NB-IoT. The exact magnitude of these costs is not yet known as NB-IoT is yet to be widely deployed. Nonetheless, a decrease in interference is likely to be worth the additional cost when considering healthcare systems, as QoS in these applications is critical.

Due to a high receiver sensitivity of 164dB, NB-IoT achieves a range of up to 15km. Despite the long range, speed remains relatively high, with a maximum uplink data rate of 250kbps [103]. The significant data rate and wide range are ideal for healthcare applications, as messages can travel a reasonable distance within an acceptable time frame for even the most critical health events.

Battery life was a fundamental consideration in the design of NB-IoT. The power efficiency has some dependence on which mode NB-IoT operates in. In [95] it was found that the life of 5Wh batteries were 2.6 and 2.4 years in standalone and in-band modes respectively when a 50 byte message was being sent every 2 hours. When a 50-byte message was only sent once per day, the battery lifetime increased to 18.0 and 16.8 years respectively. Applications such as long-term monitoring would likely require several transmissions per day, while emergency health monitoring system would transmit short "heartbeat" messages occasionally. Longer messages would only be sent when an emergency condition is detected. For each of these applications, the energy consumption of NB-IoT is sufficiently low, and allows for minimal interaction by the system wearer.

NB-IoT can also support a minimum of 52,547 nodes per base station. As mentioned in Section IV.B.1., this would be sufficient to support 40 devices per home, assuming a household density equivalent to that of London [95]. With an average household population of 2.47 people [104] and ideal positioning of cell sites, every resident of London could wear over 15 healthcare sensors, each successfully communicating directly with the closest base station. The capacity of NB-IoT is clearly sufficient for providing wide-spread healthcare.

State-of-the-art 3GPP S3 security is used by NB-IoT, with mechanisms on both the transport and application layers [105]. There are several mandatory mechanisms including entity authentication, device identification, user identity confidentiality, and data integrity. Optional mechanisms are also available for ensuring application authentication, data confidentiality, and more. As eavesdropping is a real threat to radio communications, it is recommended that the optional encryption mechanisms are also used to protect sensitive health data. With all mandatory and optional mechanisms in place, NB-IoT will likely be suitably secure for healthcare applications.

Overall, NB-IoT is suitable for healthcare applications. It is secure, supports communications over a long range, has high energy efficiency, and can support many devices. The most significant drawback is the current lack of deployment, though this is expected to occur rapidly due to the reusability of existing LTE infrastructure. This lack of deployment limits the immediate usefulness of NB-IoT, but the standard will likely be deployed rapidly on a large scale due to the ability to reuse existing 3G hardware. When this happens, NB-IoT is highly recommended for use, as it offers many favourable characteristics that make it the most suitable standard for use in healthcare systems.

4) OTHER STANDARDS

Several other LPWAN standards have been developed for operation within unlicensed, sub-GHz bands, but these have been minimally deployed compared to SigFox and LoRaWAN. They also feature unique hardware, making them harder to deploy on the same wide-scale that NB-IoT could be deployed on. These standards include Symphony Link, nWave, Weightless, and NB-Fi. Outside of the sub-GHz bands but still within ISM bands lies Ingenu Random Phase Multiple Access (RMPA). Meanwhile, in the licensed bands, two additional standards besides NB-IoT have been developed by 3GPP. These standards are Extended Coverage GSM for IoT (EC-GSM) and Long-Term Evolution Machine Type Communications Category M1 (LTE-M or eMTC). Each of these standards is briefly discussed in this section.

Symphony Link [106], [107] is a synchronous protocol that uses LoRa as its physical layer, and serves as an alternative to LoRaWAN. It is used in a star topology, but allows for the use of repeaters to provide more hops. All messages sent using Symphony Link are acknowledged, and message length can be longer. It is robust and secure standard, but is less energy-efficient due to the need for nodes to frequently synchronize with the network. The increased power consumption and lack of deployment are the main limiting factors in using Symphony Link for healthcare purposes.

nWave [108] is an ultra-narrow band technology using a star topology. It boasts high capacity and a range of up to 10km. nWave has previously been used for smart farming and smart parking. Little further information is made available by this company with regards to their technology.

Weightless offers three standards to give end users more choice - Weightless-N, Weightless-P, and Weightless-W [109]. Weightless-N was developed through a partnership with nWave [110], and offers uplink-only simplex communications with low battery consumption and a range around 4.1km. Weightless-P offers two-way communications, but with lower range and shortened battery life. Weightless-W has the lowest battery life, but has similar range to Weightless-N whilst enabling two-way communications. Of the Weightless standards, Weightless-P would likely be best suited to most healthcare applications due to its two-way communications and longer battery life. However, the short range of 2km is a limiting factor even in a dense urban environment.

NB-Fi by WAVIoT [111] is another unlicensed UNB technology that operates in a star topology. It is full duplex, with a range of 16.6km in an urban environment. The trade-off made is a high latency of 30 seconds on uplink and 60 seconds on downlink [112]. This may be suitable for non-critical systems, but would not be suitable when an emergency health alarm needs to be transmitted.

Ingenu RPMA [113] is the only well-known LPWAN standard operating in the unlicensed 2.4GHz band. This design choice allows for higher transmission power and antenna gain to be used, but this uses extra power. Additionally, the popularity of the 2.4GHz band means that messages transmitted using Ingenu RPMA are likely to be subjected to interference. Ingenu's range is short compared to its competitors, only reaching 4.6km in urban areas [92]. High capacity and QoS are provided by Ingenu, which would be advantageous in healthcare. However, the low range for high power consumption is not ideal for a battery-powered wearable system. This standard would likely be better suited to IoT applications where permanent power supplies are available for sensor nodes.

EC-GSM is a licensed band standard that was introduced to improve GSM for IoT usage, as GSM has already been widely used for M2M communications due to its high deployment and low cost devices. EC-GSM can be enabled by updating the software on existing GSM gateways. This allows for extremely fast roll-out, and allows operators to extend the useful lifetime of legacy 2G gateways. EC-GSM provides coverage improvements of up to 20dB, and each gateway can support up to 50,000 devices [114]. The data rate offered by EC-GSM is less than 140kbps for both uplink and downlink [103], slower than NB-IoT. Currently, EC-GSM has similar capabilities to that of NB-IoT and thus would be suitable for use in healthcare. However, EC-GSM operates on legacy gateways while NB-IoT operates on modern LTE gateways. It is therefore suggested that NB-IoT will outlast EC-GSM as a widely utilized standard, and thus it would be preferable to develop healthcare systems based on NB-IoT rather than EC-GSM.

LTE-M is another licensed band standard that has been developed to utilize the full capacity of an LTE carrier using multiplexing techniques, whilst improving battery life and coverage. The major difference between LTE-M and classic LTE is that the former introduces new power-saving methods not implemented in the latter [114]. With a data rate of up to 1Mbps [103], LTE-M allows for more advanced IoT applications, but has limited range and can only support around 20,000 nodes per gateway [92]. LTE-M is certainly an ideal solution for a system where high speed, large amounts of data, and advanced features are required. However, this is not the case for healthcare. A healthcare system that is intermittently transmitting small amounts of important data would benefit from long-range, high-capacity gateways, like those seen in NB-IoT. In LTE-M, these features crucial to healthcare are traded off to provide the higher data rate and enhanced functionality. LTE-M is an excellent standard for some applications, but is not suitable for healthcare when compared to other cellular IoT standards.

V. CLOUD-BASED IoT HEALTHCARE SYSTEMS

Cloud technologies have been widely researched due to their usefulness in big data management, processing and analytics. Several related works have surveyed the literature on using cloud technologies for IoT purposes such as smart grid [115] and mobile cloud computing for smartphones [116], [117], where complex computations are offloaded from low-resource mobile devices to the high-power environment of the cloud, before the result is returned to the mobile device. These works consider data storage and data processing as key advantages of cloud technologies.

Further related works have reviewed the state of cloud-centric healthcare. The use of cloud technology for health record storage is considered in [118], which also overviews cloud technologies as a complete field. Storage is considered further [11] and [119], with particular focus on how a large database could be used for data analysis and trend determination.

While each of these related works provides valuable insight into the field of cloud technologies, there is no known article that considers all advantages, disadvantages, challenges, and opportunities that cloud presents to healthcare systems based on WBANs and the IoT. In this section, we bridge the gap in the literature by presenting recent works regarding cloud-centric healthcare, analyzing key challenges, and providing recommendations for future research directions.

A. CLOUD FOR HEALTHCARE

Much research has been conducted in recent years regarding the benefits of cloud for healthcare applications. These benefits stem from the three primary services that can be provided by cloud technologies in healthcare environments:

- Software as a Service (SaaS) - provides applications to healthcare providers that will enable them to work with health data or perform other relevant tasks.
- Platform as a Service (PaaS) - provides tools for virtualization, networking, database management, and more.
- Infrastructure as a Service (IaaS) - provides the physical infrastructure for storage, servers, and more.

These services can be used to achieve a variety of tasks, but two key uses are easily identified in the literature; big data management and data processing. These two different concepts are presented separately in this section. However, it is also highlighted that both are essential for a state-of-the-art IoT healthcare system, and thus should be included together in future cloud system designs.

1) BIG DATA MANAGEMENT

Big data is regularly characterized by the so-called 5 V's - volume, velocity, variety, veracity and value. Volume refers to the amount of data generated, while velocity refers to the speed at which it is generated. Variety is the general variance in data types, while veracity is the uncertainty surrounding what data types may later be added. Finally, value refers to what information can be gained from the big data set.

The challenge in big data management lies in designing a system that can handle the characteristics of a specific big data set. In healthcare, each of the characteristic 5 V's are important to consider, as a wide variety of data from patient name, age and gender to vital sign values as taken at regular intervals would need to be stored for many systems. Regularly measured data would create significant velocity, and lead to an increased volume of total data rapidly. Additionally, new kinds of data may be added regularly as new sensors are developed to measure previously unmonitored health signs. Finally, machine learning to perform diagnostics or provide treatment plans would be extremely valuable in a healthcare context, so a cloud storage framework for healthcare would need to enable value. As all of the characteristics of big data are important to healthcare applications, recent research in this area has focused on storing a wide variety of data generated by voluminous IoT systems in an organized manner that may be useful for later data analysis.

In one recent work [24], volume and variety of healthcare data is considered, and a data storage model suitable for emergency healthcare is developed. It aims to organize heterogeneous physiological data and make it readily accessible to relevant healthcare providers during an emergency. IaaS and SaaS are used to reach these goals. One area of improvement in this work is that access control is only considered on an elementary level. Additionally, high levels of human interaction are required to enter and maintain patient health records. For a WBAN-based system, automation techniques would need to be implemented to store data from sensors in the appropriate areas of the health record.

In [120], cloud technologies for a WBAN system is considered. All three services are used to create the cloud module in this system. SaaS is used to provide applications that allow authorized parties to work with health data, PaaS provides tools for virtualization and database management, and IaaS provides the hardware and required infrastructure. This system is primarily used to create and store health records, and to allow health practitioners to check on their patient's state as required. Patients set up a profile, configure who has access to their data, and decide whether they want monitoring to be continuous, on-request, or periodic. This system appears very sophisticated, but further work needs to be done to ensure that their proposed cloud model would be suitable as the volume and variety of data increased over time. Additionally, further security mechanisms would likely need to be incorporated to ensure that the patient's data is truly secured and private.

Another sensor-based system is designed in [121], with the aim of monitoring patients' emotional states. Big data management is crucial in this system, as they aim to draw links between emotional responses and physiological changes. Large amounts of physiological data are stored in the cloud module, organized sufficiently to enable data mining techniques for the extraction of important information. To maximize storage space, algorithms have been applied to remove redundant or non-useful data from the database. The primary focus of cloud storage in this system is not to maintain a health record, but rather to amass a big data set that machine learning could be applied to. The authors have placed significant focus on managing all the characteristic Vs of big data, but there are still some improvements that could be made. While health data is stored, it appears that patients and doctors cannot easily access a patient's complete medical history. It is suggested that implementing techniques from the systems focusing on storage of health records could further its overall usefulness.

Enabling machine learning through appropriate big data management in the cloud is considered in [122]. The authors identify that cloud storage is useful for storing high volumes of data in such a way that value can be extracted from it. In this system, physiological parameters and frequency of medical visits are both stored in the patient's health record. This information can then be used by machine learning algorithms to determine the patient's condition. To prove this, machine learning was successfully applied for the detection of flu. Accuracy in classifying the flu steadily increased as more sensors were included in the WBAN, reaching 98% accuracy when 14 parameters were measured. This suggests that the authors have implemented data management to a reasonably high standard. However, it is unclear whether the system is capable of rapidly expanding as the velocity and veracity of data increases over time. Further testing would likely be required to ensure that the designed cloud architecture is still suitable when the database is non-static and continuously expanding.

An extremely thorough work on cloud for healthcare is presented in [123]. In this work, all services of cloud technologies are utilized to create a robust system. Patients are monitored by their WBANs, with their data stored in the cloud securely. A signature-based access control mechanism prevents unauthorized users from accessing data in the cloud. PaaS is used to provide virtualization techniques that support resource management and scheduling. Finally, SaaS in the form of a user-friendly application that allows healthcare professionals to access patient data that they are authorized to view. An alert system is also present in the software, triggering alarms when abnormal physiological parameters are detected. To prove that value can be obtained from their big data management scheme, machine learning was applied to ECG signals and was shown to successfully classify congestive heart failure in up to 98.9% of cases. Overall, this is an excellent example of how cloud technologies can be utilized in healthcare. To get more value out of the datasets, further machine learning could be implemented. Additionally, it may be worth considering methods for reducing latency as the velocity and volume of data inflow increases, as currently delay is shown to rise quite rapidly as the dataset expands.

Big data management for healthcare is not just a theoretical concept. It is already being implemented in certain parts of the world. In Australia, the Government has recently introduced the My Health Record scheme [124] , which utilizes cloud storage methods. A patient's My Health Record can contain information about any allergies, conditions, current medications and treatments, pathology test results, and diagnostic images. The patient can decide who has access to these records under normal circumstances. In an emergency where the patient is unable to provide the information themselves (i.e. they are unconscious following an accident), then limited-time emergency access can be granted to the responding healthcare providers so that the patient can receive the best possible treatment rapidly [125].

The benefits of cloud technologies for big data management are clear. It allows for virtually unlimited storage space, the provision of many useful services, and enables accessibility for patients and doctors. This gives patients more control over their own healthcare, and simultaneously enables doctors to provide more suitable treatments without having to even meet with their patient in person. Additionally, big data management schemes that are designed to meet all 5 characteristics of big data will enable data mining, machine learning, and other forms of detailed analysis. This could lead to new medical discoveries by identifying previously unknown trends in patient progression through an illness, finding new links between symptoms and conditions, determining new treatments that may be suitable for various conditions, and much more. Big data management is essential for the IoT healthcare system of the future.

2) DATA PROCESSING AND ANALYTICS

There are several types of data processing that can be performed using cloud technologies, but the most relevant are computational offloading and machine learning. Computational offloading involves using the cloud to perform complex data processing beyond the capabilities of low-resource wearable devices. By sending raw or partially processed sensor data to the cloud, the computing resources of many machines can be utilized for processing. Using this high-powered computing environment over processing on the standalone mobile device offers many advantages; more complex algorithms can be executed, results can be obtained significantly faster, and battery life will be extended in mobile devices due to less processing occurring internally.

Complicated sensor nodes such as those measuring ECG data, blood pressure, or accelerometers for fall detection would benefit greatly from computational offloading. For example, ECGs have a standard shape, and different deviations from this shape can indicate several different heart problems including arrhythmia, heart inflammation, and even cardiac arrest. A small, low-powered sensor node could not analyze ECG readings rapidly using machine learning algorithms to determine the patient's state of health. However, if the raw data was offloaded to cloud, high-power processing could be performed to determine the shape of the ECG before machine learning algorithms compare it to the characteristic shape, identify any serious differences between the shapes, and determine what condition is causing them.

Machine learning can also be applied to large datasets so as to obtain meaningful information from them, including identifying previously unknown links between symptoms and diseases, determining possible diagnoses based on those given to previous patients, developing suitable treatment plans for individual patients based on what has worked for similar patients in the past, and much more. Each of these applications reduces human uncertainty and thus would help patients receive the most suitable care, as soon as possible. Cloud storage enables machine learning to perform rapidly and effectively by providing large databases and high computational power. Standalone mobile devices would not have the storage capacity or computational resources to analyze data through machine learning, and thus it is essential that data is sent to the cloud. Information that could be obtained through machine learning includes disease trends, connections between symptoms, and the development of suitable treatment plans for individual patients.

Several researchers have identified the usefulness of computational offloading in healthcare environments. In [120], readings from WBAN sensors are transmitted to a mobile phone, where some basic processing occurs. The information is then transmitted forward from smartphone to cloud, where advanced processing occurs using feature selection and classification techniques. The meaningful information generated can then be stored or forwarded to healthcare practitioners. The primary weakness of this is that it is reliant on a smartphone, which would run out of battery within days at best. It would be preferable for raw data to be transmitted straight to the cloud for complete processing, using a low-power communications standard such as the previously discussed NB-IoT. Additionally, the information obtained through processing is not analyzed further; instead, it is passed directly to a doctor who manually observes the result. In many cases, it would be possible to implement classification algorithms that alert the doctor when an abnormal reading is detected in a patient's physiological signs.

In [121], cloud computing is used to process the complex raw data and send the meaningful results back to the patient through their sensing system. This is a strong concept, as it allows for the processing power of cloud to be utilized by complex sensors, whilst also enabling the patient to rapidly access their results and share them with a doctor as needed.

Computational offloading for data processing is used in [123] to determine shapes of ECGs and evaluate whether the shape is consistent with congestive heart failure. This evaluation would be far too complicated to perform on a wearable device, and thus is a perfect example of the usefulness of cloud technologies in data processing. The obtained ECG information is stored after processing in the patient's health record, enabling them to view their results and share them with their doctor. Additionally, an alert can be triggered to emergency services workers if the ECG shows heart rhythm consistent with congestive heart failure.

Some research comparing machine learning algorithms has also been conducted. In [126], deep neural networks (DNNs) are compared with gradient boosting decision tree (GBDT), logistic regression (LR), and support vector machine (SVM) algorithms for predicting stroke. In this context, DNNs performed the best with 87.3% accuracy, while the GBDT and LR algorithms were similar in performance at 86.8% and 86.6% accuracy respectively. SVMs performed the worst, with only 83.9% accuracy. This suggests that DNNs are well suited to prediction tasks, but due to the complexity of the algorithm they would need to run on cloud storage frameworks.

Meanwhile, in [127], multi-layer perceptron (MLP), SVMs for regression (SVR), generalized regression neural networks (GRNN), and k-nearest neighbour (kNN) regression approaches were compared for determining a person's psychological wellness index based on five key parameters of psychological health. In contrast to the previous work, in this case the SVM-based algorithm performed the best, while the neural network approach performed second-worst. These two comparison articles highlight the fact that the best machine learning algorithm for healthcare does not exist; rather, there are algorithms that may be suitable for one context but completely unsuitable for another. As such, future system designers should compare machine learning algorithms that may work for their purpose and determine which algorithm has the most desirable characteristics for the system they are designing.

Evidently, there are limited works that investigate computational offloading for IoT healthcare specifically. However, it has been studied extensively for mobile devices such as smartphones. The aforementioned surveys in [116] and [117] present comprehensive overviews of the works in this field, and demonstrate that energy efficiency and higher processing capabilities can be readily achieved when utilized computational offloading to the cloud. The interested reader is referred to these surveys for an overview of the related field of mobile cloud computing.

Overall, using computational offloading for data processing is invaluable in healthcare systems, particularly when analyzing complicated physiological parameters and conditions. Data processing techniques may also aid in the organized storage of health data, as it can generate meaningful information such as a standard ECG from many different types of ECG sensors. This is extremely useful in standardizing health records, and would enable machine learning techniques to be applied to a big data set with more ease. Due to these benefits, computational offloading is vital for IoT healthcare systems to ensure that even the most complicated physiological parameters can be monitored, enabling the highest possible standard of healthcare for the patient.

B. SECURITY AND PRIVACY IN THE CLOUD

Security remains a key issue in cloud-based systems. In a healthcare environment, it is essential that a patient's health information is readily accessible to authorized parties including doctors, nurses, specialists, and emergency services. It is also essential that the patient's sensitive health data is kept private. If malicious attacks revealed the patient's health data, it could have many negative ramifications for the patient, including exposing them to identity theft or making it difficult for them to obtain insurance. Worse still, if the malicious attacker altered a patient's health record, it could have detrimental effects on the patient's health.

Access control policies and data encryption are two means of securing cloud-centric healthcare systems. An access control policy specifies who is authorized access to the patient's health data, and how much access they are allowed. It would also implement an authentication mechanism (e.g. password, facial recognition, etc.) that verifies the identity of the party attempting to access the data. Meanwhile, data encryption provides security for the data whilst in data storage. Strong data encryption would prevent an attacker from reading sensitive health information, even if they did gain access to the database.

Some research has been conducted into developing security mechanisms robust enough for healthcare applications. In [128], a sophisticated access control scheme named ''SafeProtect'' is proposed, focusing on giving patients control over their information. The patient creates a policy that allows specific healthcare providers to access their health record, and can enforce limitations. The patients data is encrypted and stored in cloud storage. If a healthcare provider wants to access the patient's health record, they must enter their credentials. Credentials are checked for validity before data is decrypted for the authorized healthcare provider. If the healthcare provider has been assigned limited access by the patient, then the policy control application will monitor their behavior. If illegal actions are performed, such as the user pressing the Ctrl + C shortcut for a party that is not allowed to copy, then the action will be blocked and the patient will be notified that the healthcare provider tried to perform an illegal action. This is an intelligent mechanism to and could easily be expanded to look for attempts to print or other copy-based actions such as taking a screenshot using the ''Prt Scr'' button. A significant advantage of the SafeProtect scheme is that if the policy changes, keys do not need to be regenerated; healthcare providers' credentials can simply be added to or removed from the policy. The authors identify that they have not protected against all possible means of copying and distributing healthcare information, making this the main area in which future improvement can be made. Additional monitoring of keyboard shortcuts and ports for illegal actions would help increase security. Another potential improvement is immediately revoking access to the patient's data if the healthcare provider performs an illegal action. However, these improvements are minor and relatively easy to make. Overall, SafeProtect is a sophisticated scheme that adequately protects patients data from being accessed or used in an unauthorized manner, and the mechanisms implemented could easily be expanded to protect against more actions.

In [129], a secure cloud scheme is proposed for ''enhanced living environments'', which are generally comprised of both wearable devices worn by the patient and smart home devices, with the aim of supporting independent living for elderly or disabled persons. Access control is policy-based, where access is given to authorized people. To ensure that only authorized people can access health records, biometrics are used to ensure that the person is who they claim to be. Users are asked to provide a fingerprint, and facial recognition software calculates certain distances and angles on the face. The user is also asked to blink a random number of times, so that a photograph cannot be used to "trick" the system. Security of the data stored in the cloud is implemented by attempting to conceal possible weaknesses of the accessing applications. This is achieved by creating several applications with the same functionality but varying implementations, and dynamically swapping them in and out of execution. While this system appears to be a strong solution, it would likely benefit from encryption of patient data in the cloud. Additionally, the identity management server adds another vulnerability to the system, as information about many users' identities could be revealed if an attacker gained access to this server. Ensuring that this server is secure is almost as important as securing patient's healthcare data, as it is still sensitive information pertaining to the users of the system.

Signal scrambling is considered as a means for encryption in [130]. In this application-layer scheme, a small portion of the data - termed "tiny data" - is used as the scrambling key, and is shared between authorized parties. To reduce the risk that a brute force attack could be used to determine what the tiny data used is, algorithms are in place to prevent the tiny data from containing statistically significant characteristics, thus lowering the probability that such an attack would be successful. This scheme would be suitable in addition to other security mechanisms, especially considering its position in the application layer allows for it to be built on top of existing communications standards. Further work could be done regarding securing the exchange of tiny data, as this process could currently be susceptible to man-in-the-middle attacks if the communications standard used is not secure. Additionally, it may be useful to occasionally generate new tiny data to use for scrambling and unscrambling. This would likely decrease the likelihood of a brute force attack succeeding.

A steganography-based approach to access control is presented in [131]. In addition to protecting electronic health records with encryption techniques, this scheme also conceals the data within an ECG signal. This means that if the data was intercepted by an attacker, they would likely assume that it was simply a standard ECG signal, and would not even discover the hidden, encrypted message that is the health record. After encrypting and concealing the health record, the health authority stores several parameters that are required to reconstruct the data at their local servers. If the data is requested, authorization is performed using facial recognition and the location of person making the request. If the user is authorized, then the health authorization recovers the data and provides it to them. While this appears to be a very secure system, it is limiting. Firstly, the use of location as a means for authentication limits flexibility. For example, a paramedic would likely not be able to access a patient's health data whilst travelling to their location. Additionally, the fact that the health authority stores the decryption parameters on their local server means that the health data cannot be easily shared with another health authority. This could be problematic if a patient was travelling overseas and was hospitalized, as the healthcare providers would not be able to readily access the required health data. It would be valuable to make this system more accessible to authorized users, without compromising the high level of security that it clearly provides.

In [132], fully homomorphic encryption (FHE) is considered as a scheme for protecting the security of the data. FHE allows for public-key encryption to be implemented before being sent to the cloud. It also allows mathematic functions to be performed over on the data whilst it is encrypted, enabling basic machine learning without decrypting data in the cloud. If data is requested by an authorized user, the key authority system can use a secure channel to provide them with the secret key required to decrypt the data. This is a promising approach to combining security with machine learning, but it is not yet ready to be implemented into IoT-based healthcare systems. In this work, it is shown that significant computational resources are required for FHE to be successful. Additionally, only limited arithmetic can be performed on the encrypted data. Whilst this work shows improvement on previous FHE schemes, improving the speed and computational capabilities of FHE schemes remains an active field of research.

FHE was also compared to traditional Advanced Encryption Standard (AES) and emerging Attribute-Based Encryption (ABE) in [133]. AES is a 128-bit block cypher, and the scheme has already been optimized to run on small, lower-power devices. It is an accepted industry standard. ABE focuses on allowing access to multiple authorized parties, much like the other schemes discussed in this section. The three types of encryption were compared in depth, and it was found that there is no perfect solution for encryption. AES is the only scheme that is simple and low-latency enough for wearable devices, but ABE is the best scheme for enabling multiple parties to access private data. FHE is the only one that can provide computation and thus enable machine learning, but it is the slowest and requires the highest amount of storage.

Kocabas *et al.* [133] suggest that a scheme that uses AES during acquisition, and then converts to FHE using an AES-to-FHE conversion scheme would be a suitable solution. One advanced AES-to-FHE conversion scheme was proposed in [134], whereby the conversion can be performed iteratively without decrypting the data at any stage. This conversion process requires significant computational power and time, but would be achievable within a cloud storage framework.

We agree that this type of AES-to-FHE scheme is a reasonable means for securing patient data. However, with the clear advantages of ABE for cloud security in healthcare, we believe that it would be beneficial to use it for acquisition and provision of health data. It is therefore suggested that an optimized ABE-to-FHE conversion scheme that at no point decrypts and re-encrypts the data would be extremely valuable for securing patient data.

Overall, there is still significant research opportunity in developing a completely suitable encryption scheme for healthcare systems that rely on both low-power wearables and big data cloud storage. Increasing speed, decreasing computational requirements, and enabling high-level machine learning are all areas for improvement that should be investigated further.

VI. FINDINGS AND RECOMMENDATIONS

Upon completion of this thorough survey of existing technologies, several lessons have been learned. In this section, we will present a summary of these lessons, followed by providing recommendations for future work with the aim of directing researchers to areas that would fill the most significant gaps in the literature.

A. LESSONS LEARNED

In terms of the key sensor types, it was found that there are several options for suitable pulse sensors, while researchers agree that thermistor-type temperature sensors are already suitable for use in measuring human body temperature. The photoplethysmographic method for implementing blood oxygen level monitoring is also widely agreed upon. The issues that remain with these devices are primarily making them robust against motion and ensuring energy efficiency without compromising accuracy. Meanwhile, there is little consensus regarding the most suitable respiratory rate sensor for general-purpose use, and there remains much work to be done on blood pressure sensors in order to achieve an accurate and truly wearable sensor that could be deployed on a wide scale.

The progress made towards suitable solutions largely reflects the frequency with which each topic has been considered in the literature. There are many papers that exist on pulse, body temperature, and blood oxygen monitoring, both current and classical. On the other hand, respiratory rate monitoring with wearable sensors is a newer concept in the literature, and is further divided into subsections for varying sensor types (nasal, stretch, pressure, and so on). Meanwhile, research on blood pressure sensors within the literature is minimal, and is very much still in its infancy when compared to research on other sensor types.

In terms of short-range communications standards, it was learned that Bluetooth Low Energy has the highest suitability for healthcare, and can be immediately implemented into healthcare systems being designed now and in the future. As discussed in Section IV.A., BLE has already been implemented by systems discussed in a reasonable number of papers. Meanwhile, it was found that NB-IoT has the highest suitability for low-power, long-range communications in healthcare, and will likely be deployed rapidly once the standard is finalized, due to the ability to re-use existing cellular station hardware for this purpose.

From our research, it is found that the problem of cloud storage has largely been solved. Additionally, extensive research has been conducted into improving security mechanisms within the cloud. Several works have focused more specifically on the need for privacy and security in healthcare applications. All of these works have made significant improvements on previous methods, but there is still no perfect solution for security within the cloud.

Finally, several works have identified that machine learning is extremely important in healthcare applications. Machine learning as a whole is a topic that has been widely considered by previous researchers. However, minimal works exist on implementing machine learning specifically for diagnostics or other health-related purposes.

B. RECOMMENDATIONS FOR FUTURE WORKS

The lessons learned through conducting this survey highlight several areas for further research. In terms of sensors, much progress has been made but there are still no available devices that match the accuracy of hospital-grade devices without compromising energy efficiency or wearability. This is especially true of complex devices such as blood pressure and respiratory rate sensors, both of which would be invaluable to the field of medicine. As such, further research efforts should be made towards improving the quality of these sensors until they are highly accurate, reliable, and comfortably wearable. In our own future works, we will be placing particular focus on developing a blood pressure monitor that is more wearable than the works presented in this paper, without compromising accuracy. We will also look at reducing the impact of motion on sensors, particularly for respiratory rate and pulse sensors.

In terms of communications standards, it would be worthwhile to develop wearable healthcare systems that are reliant on the emerging NB-IoT standard. As this is an extremely new standard, no known work has implemented it into a healthcare environment despite its obvious advantages for this field. In our own future works, we will be implementing NB-IoT into healthcare devices to confirm its suitability, before using it as the foundation communications standard for a healthcare system that is being developed in accordance with the model proposed by this paper.

Data storage using cloud technologies has been extensively considered, but data processing is an area in which further research should be conducted. The development of cloud-based algorithms that are capable of processing raw data from complex sensors and extract meaningful information about a person's health should be continued.

Machine learning is another branch of data processing that would be extremely valuable in healthcare scenarios. If applied in the high-power computing environment of the cloud, machine learning could provide diagnostics for patients, make new discoveries about disease trends, and aid in the development of treatment plans. Despite these clear advantages, machine learning has not yet been widely explored for healthcare applications, providing a significant research opportunity. This opportunity should be seized by researchers aiming to make notable improvements to the field of IoT-based healthcare. In our own future work, we will be investigating clustering and logistic regression algorithms as a means for providing diagnostics based on vital and other sign information.

There is still much room for improvement in security and privacy for cloud-based healthcare. No known encryption scheme is ideal for protecting data whilst providing accessibility for authorized parties and enabling machine learning. ABE and FHE are schemes that provide appealing characteristics, but are not lightweight enough for implementation into wearable devices. Improving these schemes is the first active area of research. Upon improving the schemes individually, a lightweight ABE-FHE hybrid scheme should be considered, as it could potentially provide all the desirable characteristics for cloud-based healthcare security.

Overall, there is no known end-to-end system for general or specific purposes that contains all components in our proposed model; wearable sensors, short- and long-range communications, cloud-based storage, and machine learning. Developing such a system would be a significant achievement in the field of IoT-based healthcare, and should be considered as the ultimate goal for researchers in this area. In our own future works, we will be striving to reach this goal through the development of a wearable, IoT-based system for the provision of emergency healthcare that incorporates health sign monitoring, machine learning for diagnostics, and long-range communications via LPWANs to notify emergency service providers when a patient needs urgent help.

VII. CONCLUSION

In this work, we have proposed a unique model for future IoT-based healthcare systems, which can be applied to both general systems and systems that monitor specific conditions. We then presented a thorough and systematic overview of the state-of-the-art works relating to each component of the proposed model. Several wearable, non-intrusive sensors were presented and analyzed, with particular focus on those monitoring vital signs, blood pressure, and blood oxygen levels. Short-range and long-range communications standards were then compared in terms of suitability for healthcare applications. BLE and NB-IoT emerged as the most suitable standards for short-range and long-range communications in healthcare respectively.

Recent works utilizing cloud technologies for data storage were presented, and showed that cloud is the best means for storing and organizing big data in healthcare. It is also shown by several works that significantly better data processing can be performed in the cloud than can be performed by wearable devices with their limited resources. The most significant drawback of using cloud is that it introduces security risks, and as such we presented several works focused on improving security in the cloud. It was found that access control policies and encryption can significantly enhance security, but that no known standard is suitable for immediate application into a wearable, IoT-based healthcare system.

Based on our analysis of state-of-the-art technologies in the fields of wearable sensors, communications standards, and cloud technology, we identified several significant areas for future research. Machine learning and the development of a secure yet lightweight encryption scheme for cloud storage were the two areas that provide the most opportunity for researchers seeking to make significant improvements in the field of IoT-based healthcare.

REFERENCES

[1] Australian Institute of Health and Welfare. (2014). *Australia's Health*. [Online]. Available: http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx-?id=60129548150

[2] E. Perrier, *Positive Disruption: Healthcare, Ageing and Participation in the Age of Technology*. Sydney, NSW, Australia: The McKell Institute, 2015.

[3] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[4] N. Zhu *et al.*, "Bridging e-health and the Internet of Things: The SPHERE project," *IEEE Intell. Syst.*, vol. 30, no. 4, pp. 39–46, Jul./Aug. 2015.

[5] S.-H. Chang, R.-D. Chiang, S.-J. Wu, and W.-T. Chang, "A context-aware, interactive M-health system for diabetics," *IT Prof.*, vol. 18, no. 3, pp. 14–22, May/Jun. 2016.

[6] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An emerging era in the management of Parkinson's disease: Wearable technologies and the Internet of Things," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 6, pp. 1873–1881, Nov. 2015.

[7] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1568–1577, May 2014.

[8] S. Sarkar and S. Misra, "From micro to nano: The evolution of wireless sensor-based health care," *IEEE Pulse*, vol. 7, no. 1, pp. 21–25, Jan./Feb. 2016.

[9] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2452414X16000066

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

[11] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," *Healthcare Inform. Res.*, vol. 22, no. 3, pp. 156–163, Jul. 2016. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4981575/

[12] C. C. Y. Poon, B. P. L. Lo, M. R. Yuce, A. Alomainy, and Y. Hao, "Body sensor networks: In the era of big data and beyond," *IEEE Rev. Biomed. Eng.*, vol. 8, pp. 4–16, 2015.

[13] P. K. Schwab, *The Fourth Industrial Revolution: What it Means, and How to Respond*. Cologny, Switzerland: World Economic Forum, 2016.

[14] Smart Parking. (2017). *SmartEye, SmartRep, and RFID Technology—Westminster City Council—London*. [Online]. Available: http://www.smartparking.com/keep-up-to-date/case-studies/3-500-vehicle-detection-sensors-and-epermit-technology-in-the-city-of-westminster-london

[15] University of New England. (2017). *SMART Farm*. [Online]. Available: http://www.une.edu.au/research/research-centres-institutes/smart-farm

[16] Sensus. (2017). *Smart Water—Smarter at Every Point*. [Online]. Available: www.sensus.com/internet-of-things/smart-water

[17] H. El-Sayed and G. Thandavarayan, "Congestion detection and propagation in urban areas using histogram models," *IEEE Internet Things J.*, to be published.

[18] C. A. Tokognon, B. Gao, G. Tian, and Y. Yan, "Structural health monitoring framework based on Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 619–635, Jun. 2017.

[19] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social Internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, Mar. 2015.

[20] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 397–422, 1st Quart., 2017.

[21] R. C. A. Alves, L. B. Gabriel, B. T. D. Oliveira, C. B. Margi, and F. C. L. D. Santos, "Assisting physical (hydro)therapy with wireless sensors networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 113–120, Apr. 2015.

[22] G. Wolgast, C. Ehrenborg, A. Israelsson, J. Helander, E. Johansson, and H. Manefjord, "Wireless body area network for heart attack detection [education corner]," *IEEE Antennas Propag. Mag.*, vol. 58, no. 5, pp. 84–92, Oct. 2016.
[23] M. A. Cretikos, R. Bellomo, K. Hillman, J. Chen, S. Finfer, and A. Flabouris, "Respiratory rate: The neglected vital sign," *Med. J. Austral.*, vol. 188, no. 11, pp. 657–659, 2008.
[24] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586, May 2014.
[25] I. Olaronke and O. Oluwaseun, "Big data in healthcare: Prospects, challenges and resolutions," in *Proc. Future Technol. Conf. (FTC)*, Dec. 2016, pp. 1152–1157.
[26] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.
[27] Shake It Up Australia Foundation. (2017). *Symptoms of Parkinson's*. [Online]. Available: https://shakeitup.org.au/understanding-parkinsons/symptoms-of-parkinsons/
[28] J. Ženko, M. Kos, and I. Kramberger, "Pulse rate variability and blood oxidation content identification using miniature wearable wrist device," in *Proc. Int. Conf. Syst., Signals Image Process. (IWSSIP)*, May 2016, pp. 1–4.
[29] Garmin. (2017). *HSM-Tri*. [Online]. Available: https://buy.garmin.com/en-AU/AU/p/136403
[30] Polar. (2017). *H7 Heart Rate Sensor*. [Online]. Available: https://www.polar.com/au-en/products/accessories/H7_heart_rate_sensor
[31] FitBit. (2017). *FitBit PurePulse*. [Online]. Available: https://www.fitbit.com/au/purepulse
[32] TomTom. (2017). *TomTom Spark Cardio*. [Online]. Available: https://www.tomtom.com/en_au/sports/fitness-watches/gps-watch-cardio-spark/black-large/
[33] H. Lee, H. Ko, C. Jeong, and J. Lee, "Wearable photoplethysmographic sensor based on different LED light intensities," *IEEE Sensors J.*, vol. 17, no. 3, pp. 587–588, Feb. 2017.
[34] Y. Shu, C. Li, Z. Wang, W. Mi, Y. Li, and T.-L. Ren, "A pressure sensing system for heart rate monitoring with polymer-based pressure sensors and an anti-interference post processing circuit," *Sensors*, vol. 15, no. 2, pp. 3224–3235, 2015.
[35] D. Wang, D. Zhang, and G. Lu, "A novel multichannel wrist pulse system with different sensor arrays," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 7, pp. 2020–2034, Jul. 2015.
[36] D. Wang, D. Zhang, and G. Lu, "An optimal pulse system design by multichannel sensors fusion," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 2, pp. 450–459, Mar. 2016.
[37] W. Zuo, P. Wang, and D. Zhang, "Comparison of three different types of wrist pulse signals by their physical meanings and diagnosis performance," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 1, pp. 119–127, Jan. 2016.
[38] Y.-J. An, B.-H. Kim, G.-H. Yun, S.-W. Kim, S.-B. Hong, and J.-G. Yook, "Flexible non-constrained RF wrist pulse detection sensor based on array resonators," *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 2, pp. 300–308, Apr. 2016.
[39] S. Milici, J. Lorenzo, A. Lázaro, R. Villarino, and D. Girbau, "Wireless breathing sensor based on wearable modulated frequency selective surface," *IEEE Sensors J.*, vol. 17, no. 5, pp. 1285–1292, Mar. 2017.
[40] C. Varon, A. Caicedo, D. Testelmans, B. Buyse, and S. van Huffel, "A novel algorithm for the automatic detection of sleep apnea from single-lead ECG," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 9, pp. 2269–2278, Sep. 2015.
[41] D. Oletic and V. Bilas, "Energy-efficient respiratory sounds sensing for personal mobile asthma monitoring," *IEEE Sensors J.*, vol. 16, no. 23, pp. 8295–8303, Dec. 2016.
[42] X. Yang *et al.*, "Textile fiber optic microbend sensor used for heartbeat and respiration monitoring," *IEEE Sensors J.*, vol. 15, no. 2, pp. 757–761, Feb. 2015.
[43] S. D. Min, Y. Yun, and H. Shin, "Simplified structural textile respiration sensor based on capacitive pressure sensing method," *IEEE Sensors J.*, vol. 14, no. 9, pp. 3245–3251, Sep. 2014.
[44] I. Mahbub *et al.*, "A low-power wireless piezoelectric sensor-based respiration monitoring system realized in CMOS process," *IEEE Sensors J.*, vol. 17, no. 6, pp. 1858–1864, Mar. 2017.
[45] O. Atalay, W. R. Kennon, and E. Demirok, "Weft-knitted strain sensor for monitoring respiratory rate and its electro-mechanical modeling," *IEEE Sensors J.*, vol. 15, no. 1, pp. 110–122, Jan. 2015.
[46] P. Aqueveque, C. Gutiérrez, F. S. Rodríguez, E. J. Pino, A. Morales, and E. P. Wiechmann, "Monitoring physiological variables of mining workers at high altitude," *IEEE Trans. Ind. Appl.*, vol. 53, no. 3, pp. 2628–2634, May/Jun. 2017.
[47] P. Narczyk, K. Siwiec, and W. A. Pleskacz, "Precision human body temperature measurement based on thermistor sensor," in *Proc. IEEE 19th Int. Symp. Design Diagnostics Electron. Circuits Syst. (DDECS)*, Apr. 2016, pp. 1–5.
[48] T. Nakamura *et al.*, "Development of flexible and wide-range polymer-based temperature sensor for human bodies," in *Proc. IEEE-EMBS Int. Conf. Biomed. Health Inform. (BHI)*, Feb. 2016, pp. 485–488.
[49] A. Eshkeiti *et al.*, "A novel self-supported printed flexible strain sensor for monitoring body movement and temperature," in *Proc. IEEE SENSORS*, Nov. 2014, pp. 1615–1618.
[50] Heart Foundation. (2017). *High Blood Pressure Statistics*. [Online]. Available: www.heartfoundation.org.au/about-us/what-we-do/heart-disease-in-australia/high-blood-pressure-statistics
[51] S. S. Thomas, V. Nathan, C. Zong, K. Soundarapandian, X. Shi, and R. Jafari, "BioWatch: A noninvasive wrist-based blood pressure monitor that incorporates training techniques for posture and subject variability," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 5, pp. 1291–1300, Sep. 2016.
[52] H. Lin, W. Xu, N. Guan, D. Ji, Y. Wei, and W. Yi, "Noninvasive and continuous blood pressure monitoring using wearable body sensor networks," *IEEE Intell. Syst.*, vol. 30, no. 6, pp. 38–48, Nov./Dec. 2015.
[53] Y.-L. Zheng, B. P. Yan, Y.-T. Zhang, and C. C. Y. Poon, "An armband wearable device for overnight and cuff-less blood pressure measurement," *IEEE Trans. Biomed. Eng.*, vol. 61, no. 7, pp. 2179–2186, Jul. 2014.
[54] D. Griggs *et al.*, "Design and development of continuous cuff-less blood pressure monitoring devices," in *Proc. IEEE SENSORS*, Oct./Nov. 2016, pp. 1–3.
[55] Y. Zhang, M. Berthelot, and B. P. Lo, "Wireless wearable photoplethysmography sensors for continuous blood pressure monitoring," in *Proc. IEEE Wireless Health (WH)*, Oct. 2016, pp. 1–8.
[56] J. Wannenburg and R. Malekian, "Body sensor network for mobile health monitoring, a diagnosis and anticipating system," *IEEE Sensors J.*, vol. 15, no. 12, pp. 6839–6852, Dec. 2015.
[57] S. V. Gubbi and B. Amrutur, "Adaptive pulse width control and sampling for low power pulse oximetry," *IEEE Trans. Biomed. Circuits Syst.*, vol. 9, no. 2, pp. 272–283, Apr. 2015.
[58] B. Venema, H. Gehring, I. Michelsen, N. Blanik, V. Blazek, and S. Leonhardt, "Robustness, specificity, and reliability of an in-ear pulse oximetric sensor in surgical patients," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1178–1185, Jul. 2014.
[59] G. Pang and C. Ma, "A neo-reflective wrist pulse oximeter," *IEEE Access*, vol. 2, pp. 1562–1567, 2014.
[60] V. P. Rachim and W.-Y. Chung, "Wearable noncontact armband for mobile ECG monitoring system," *IEEE Trans. Biomed. Circuits Syst.*, vol. 10, no. 6, pp. 1112–1118, Dec. 2016.
[61] W. Von Rosenberg, T. Chanwimalueang, V. Goverdovsky, D. Looney, D. Sharp, and D. P. Mandic, "Smart helmet: Wearable multichannel ECG and EEG," *IEEE J. Transl. Eng. Health Med.*, vol. 4, 2016, Art. no. 2700111.
[62] E. Spanò, S. D. Pascoli, and G. Iannaccone, "Low-power wearable ECG monitoring system for multiple-patient remote monitoring," *IEEE Sensors J.*, vol. 16, no. 13, pp. 5452–5462, May 2016.
[63] G. Li, B.-L. Lee, and W.-Y. Chung, "Smartwatch-based wearable EEG system for driver drowsiness detection," *IEEE Sensors J.*, vol. 15, no. 12, pp. 7169–7180, Dec. 2015.
[64] U. Ha *et al.*, "A wearable EEG-HEG-HRV multimodal system with simultaneous monitoring of tES for mental health management," *IEEE Trans. Biomed. Circuits Syst.*, vol. 9, no. 6, pp. 758–766, Dec. 2015.
[65] J. Wannenburg and R. Malekian, "Physical activity recognition from smartphone accelerometer data for user context awareness sensing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 12, pp. 3142–3149, Dec. 2017.
[66] P. Vallabh, R. Malekian, N. Ye, and D. C. Bogatinoska, "Fall detection using machine learning algorithms," in *Proc. 24th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2016, pp. 1–9.

[67] K. Ozcan, S. Velipasalar, and P. K. Varshney, "Autonomous fall detection with wearable cameras by using relative entropy distance measure," *IEEE Trans. Human–Mach. Syst.*, vol. 47, no. 1, pp. 31–39, Feb. 2017.

[68] K. Ozcan and S. Velipasalar, "Wearable camera- and accelerometer-based fall detection on portable devices," *IEEE Embedded Syst. Lett.*, vol. 8, no. 1, pp. 6–9, Mar. 2016.

[69] P. Pierleoni, A. Belli, L. Palma, M. Pellegrini, L. Pernini, and S. Valenti, "A high reliability wearable device for elderly fall detection," *IEEE Sensors J.*, vol. 15, no. 8, pp. 4544–4553, Aug. 2015.

[70] P. Pierleoni *et al.*, "A wearable fall detector for elderly people based on AHRS and barometric sensor," *IEEE Sensors J.*, vol. 16, no. 17, pp. 6733–6744, Sep. 2016.

[71] H.-C. Chang, Y.-L. Hsu, S.-C. Yang, J.-C. Lin, and Z.-H. Wu, "A wearable inertial measurement system with complementary filter for gait analysis of patients with stroke or Parkinson's disease," *IEEE Access*, vol. 4, pp. 8442–8453, 2016.

[72] H. F. Maqbool, M. A. B. Husman, M. I. Awad, A. Abouhossein, N. Iqbal, and A. A. Dehghani-Sanij, "A real-time gait event detection for lower limb prosthesis control and evaluation," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 9, pp. 1500–1509, Sep. 2017.

[73] T. T. Pham *et al.*, "Freezing of gait detection in Parkinson's disease: A subject-independent detector using anomaly scores," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 11, pp. 2719–2728, Nov. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7845616/

[74] G. Cola, M. Avvenuti, A. Vecchio, G.-Z. Yang, and B. Lo, "An on-node processing approach for anomaly detection in gait," *IEEE Sensors J.*, vol. 15, no. 11, pp. 6640–6649, Nov. 2015.

[75] S. Haxha and J. Jhoja, "Optical based noninvasive glucose monitoring sensor prototype," *IEEE Photon. J.*, vol. 8, no. 6, Dec. 2016, Art. no. 6805911.

[76] X. Xiao and Q. Li, "A noninvasive measurement of blood glucose concentration by UWB microwave spectrum," *IEEE Antennas Wireless Propag. Lett.*, vol. 16, pp. 1040–1043, 2016.

[77] K.-H. Chang, "Bluetooth: A viable solution for IoT? [Industry Perspectives]," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 6–7, Dec. 2014.

[78] Bluetooth. (2009). *SIG Introduces Bluetooth Low Energy Wireless Technology, the Next Generation Bluetooth Wireless Technology*. [Online]. Available: https://www.bluetooth.com/news/pressreleases/2009/-12/17/sig-introduces-bluetooth-low-energy-wireless-technologythe-next-generation-of-bluetooth-wireless-technology

[79] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[80] *Security, Bluetooth Low Energy*, 1st ed., Bluetooth, Kirkland, WA, USA, 2017, pp. 1–5. [Online]. Available: https://www.bluetooth.com/~/media/files/specification/bluetooth-low-energy-security.ashx

[81] M. Singh and N. Jain, "Performance and evaluation of smartphone based wireless blood pressure monitoring system using Bluetooth," *IEEE Sensors J.*, vol. 16, no. 23, pp. 8322–8328, Dec. 2016.

[82] H. T. Cheng and W. Zhuang, "Bluetooth-enabled in-home patient monitoring system: Early detection of Alzheimer's disease," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 74–79, Feb. 2010.

[83] Digi. (2017). *ZigBee Wireless Standard*. [Online]. Available: https://www.digi.com/resources/standards-and-technologies/rfmodems/zigbee-wireless-standard

[84] Digi. (2009). *XBee/XBee-Pro RF Modules (Datasheet)*. [Online]. Available: https://www.sparkfun.com/datasheets/Wireless/Zigbee/-XBee-Datasheet.pdf

[85] *XBee-PRO 900HP/XBee-PRO XSC RF Modules*, Digi, Shah Alam, Malaysia, 2014.

[86] ZigBee Alliance. (2017). *ZigBee IP and 910IP*. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/

[87] Daintree Networks. (2017). *ZigBee Security*. [Online]. Available: http://www.daintree.net/resources/zigbee-security/

[88] T. Zillner, *ZigBee Exploited*, 1st ed. Vienna, Austria: Cognosec, 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[89] D. M. Taub, S. B. Leeb, E. C. Lupton, R. T. Hinman, J. Ziesel, and S. Blackler, "The escort system: A safety monitor for people living with Alzheimer's disease," *IEEE Pervasive Comput.*, vol. 10, no. 2, pp. 68–77, Apr./Jun. 2011.

[90] J. Gil *et al.*, "A fully integrated low-power high-coexistence 2.4-GHz ZigBee transceiver for biomedical and healthcare applications," *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 9, pp. 1879–1889, Sep. 2014.

[91] Sigfox. (2017). *Getting Started*. [Online]. Available: http://makers.sigfox.com/getting-started/

[92] WAVIoT. (2016). *Comparison of LPWAN Technologies*. [Online]. Available: http://dgmatics.com/technology/waviot-lpwan-technology-comparison

[93] VT Networks. (2016). *Sigfox Network Overview for Technical Professionals*. [Online]. Available: http://vtnetworks.ie/wp-content/uploads/2016/12/Sigfox-Network-Overview.pdf

[94] Thinxtra. (2017). *Empowering Internet of Things in Australia, New Zealand and Hong Kong*. [Online]. Available: https://www.thinxtra.com/

[95] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–5.

[96] Burdekin Shire Council. (2017). *Population of the Burdekin Shire*. [Online]. Available: http://www.burdekin.qld.gov.au/council/business/-population-of-the-burdekin-shire/

[97] *National Regional Profile: Burdekin (Statistical Area Level 2)—Environment/Energy*, Austral. Bureau Statist., Canberra, Australia, 2013.

[98] *LoRaWAN: What is it? A Technical Overview of LoRa and LoRaWAN*, 1st ed., LoRa Alliance, Beaverton, OR, USA, 2015. [Online]. Available: https://www.lora-alliance.org/lorawan-white-papers and https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

[99] R. Miller, *LoRa security: Building a Secure LoRa Solution*, 1st ed., Basingstoke, UK: MWR InfoSecurity, 2016. [Online]. Available: https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf

[100] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "NB-IoT deployment study for low power wide area cellular IoT," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[101] *NB-IoT*, 1st ed., Huawei Technologies Co. Ltd., Shenzhen, China, 2017. [Online]. Available: http://www.huawei.com/minisite/iot/img/nb_iot_whitepaper_en.pdf

[102] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J.-P. Koskinen, "Overview of narrowband IoT in LTE Rel-13," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2016, pp. 1–7.

[103] *LTE Evolution for IoT Connectivity*, 1st ed., Nokia, Espoo, Finland, 2017. [Online]. Available: https://resources.ext.nokia.com/asset/200178

[104] *2011 Census Snapshot: Households Families*, Census Inf. Scheme, London, U.K., 2012.

[105] *3GPP Low Power Wide Area Technologies*, 1st ed., GSMA, London, U.K., 2016. Available: https://www.gsma.com/iot/3gpp-low-power-wide-area-technologies-white-paper/

[106] *Symphony Link vs. LoRaWAN*, 1st ed., Link Labs, Annapolis, MD, USA, 2017. [Online]. Available: https://www.link-labs.com/whitepaper-symphony-link-vs-lorawan

[107] *A Comprehensive Look at Low Power, Wide Area Networks for 'Internet of Things' Engineers and Decision Makers*, Link Labs, Annapolis, MD, USA, 2016.

[108] *nWave Network*, nWave, Brussels, Belgium, 2017.

[109] *Which Weightless Standard?*, Weightless, Cambridge, U.K., 2017.

[110] *Weightless-N Standard Accelerates*, Weightless, Cambridge, U.K., 2014.

[111] *What is NB-Fi Protocol*, WAVIoT, Houston, TX, USA, 2017.

[112] *Frequently Asked Questions*, WAVIoT, Houston, TX, USA, 2017.

[113] *How RPMA Works: An Educational Guide*, 1st ed., Ingenu, San Diego, CA, USA, 2017. [Online]. Available: https://www.ingenu.com/portfolio/how-rpma-works-white-paper/

[114] *Cellular Networks for Massive IoT*, 1st ed., Ericsson, Stockholm, Sweden, 2016. [Online]. Available: https://www.ericsson.com/assets/local/publications/white-papers/wp_iot.pdf

[115] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[116] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[117] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 393–413, Feb. 2014.

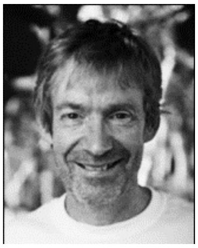
[118] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," *Int. J. Inf. Manage.*, vol. 34, no. 2, pp. 177–184, Apr. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0268401213001680
[119] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile cloud computing model and big data analysis for healthcare applications," *IEEE Access*, vol. 4, pp. 6171–6180, 2016.
[120] S. Ghanavati, J. Abawajy, and D. Izadi, "An alternative sensor cloud architecture for vital signs monitoring," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 2827–2833.
[121] K. Lin, F. Xia, W. Wang, D. Tian, and J. Song, "System design for big data application in emotion-aware healthcare," *IEEE Access*, vol. 4, pp. 6901–6909, 2016.
[122] P. K. Sahoo, S. K. Mohapatra, and S.-L. Wu, "Analyzing healthcare big data with prediction for future health condition," *IEEE Access*, vol. 4, pp. 9786–9799, 2016.
[123] J. H. Abawajy and M. M. Hassan, "Federated Internet of Things and cloud computing pervasive patient health monitoring system," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017.
[124] Australian Government. (2017). *What is My Health Record?* [Online]. Available: http://myhealthrecord.gov.au/internet/mhr/publishing.nsf/-Content/find-out
[125] *Managing Access, Privacy and Security*, Australian Government, Sydney, NSW, Australia, 2017.
[126] C.-Y. Hung, W.-C. Chen, P.-T. Lai, C.-H. Lin, and C.-C. Lee, "Comparing deep neural network and other machine learning algorithms for stroke prediction in a large-scale population-based electronic medical claims database," in *Proc. 39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2017, pp. 3110–3113.
[127] J. Park, K.-Y. Kim, and O. Kwon, "Comparison of machine learning algorithms to predict psychological wellness indices for ubiquitous healthcare system design," in *Proc. Int. Conf. Innov. Design Manuf. (ICIDM)*, Aug. 2014, pp. 263–269.
[128] D. Thilakanathan, S. Chen, S. Nepal, and R. Calvo, "SafeProtect: Controlled data sharing with user-defined policies in cloud-based collaborative environment," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 2, pp. 301–315, Apr./Jun. 2016.
[129] J. Pacheco, C. Tunc, P. Satam, and S. Hariri, "Secure and resilient cloud services for enhanced living environments," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 44–52, Nov./Dec. 2016.
[130] S.-D. Bao, M. Chen, and G.-Z. Yang, "A method of signal scrambling to secure data storage for healthcare applications," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 6, pp. 1487–1494, Nov. 2017.
[131] U. Premarathne *et al.*, "Hybrid cryptographic access control for cloud-based EHR systems," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 58–64, Jul./Aug. 2016.
[132] A. Khedr and G. Gulak, "SecureMed: Secure medical computation using GPU-accelerated homomorphic encryption scheme," *IEEE J. Biomed. Health Informat.*, to be published.
[133] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging security mechanisms for medical cyber physical systems," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 13, no. 3, pp. 401–416, May/Jun. 2016.
[134] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic evaluation of the AES circuit," in *Proc. 32nd Annu. Cryptol. Conf.*, Santa Barbara, CA, USA, 2012, pp. 850–867.

STEPHANIE B. BAKER received the B.Eng. degree (Hons.) in computer systems engineering from James Cook University, Townsville, QLD, Australia, in 2016, where she is currently pursuing the Ph.D. degree in engineering and related technologies.

Previously, she was a summer intern with Cochlear Ltd., where she was involved in an individual research project in biomedical field. Her research interests include developing accurate biomedical sensors, wireless body area networks, machine learning for medical diagnostics, and the use of Internet of Things technology for the provision of rural and emergency healthcare.

WEI XIANG (S'00–M'04–SM'10) received the B.Eng. and M.Eng. degrees in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1997 and 2000, respectively, and the Ph.D. degree in telecommunications engineering from the University of South Australia, Adelaide, Australia, in 2004.

During 2004 and 2015, he was with the School of Mechanical and Electrical Engineering, University of Southern Queensland, Toowoomba, Australia. He is currently a Foundation Professor and the Head of Discipline Internet of Things Engineering with the College of Science and Engineering, James Cook University, Cairns, Australia. He has published over 200 papers in peer-reviewed journal and conference papers. His research interests are in the broad area of communications and information theory, particularly coding, and signal processing for multimedia communications systems. He is a Fellow of the IET and an elected Fellow of Engineers Australia. He received the TNQ Innovation Award in 2016. He was a co-recipient of the three Best Paper Awards at the 2015 WCSP, the 2011 IEEE WCNC, and the 2009 ICWMC. He has been awarded several prestigious fellowship titles. He was named a Queensland International Fellow by the Queensland Government of Australia from 2010 to 2011, an Endeavour Research Fellow by the Commonwealth Government of Australia from 2012 to 2013, a Smart Futures Fellow by the Queensland Government of Australia from 2012 to 2015, and a JSPS Invitational Fellow jointly by the Australian Academy of Science and Japanese Society for Promotion of Science from 2014 to 2015. He is the Vice Chair of the IEEE Northern Australia Section. He is an Editor for the IEEE COMMUNICATIONS LETTERS, and an Associate Editor for the *Telecommunications Systems* (Springer).



IAN ATKINSON is a Professor and the Director of the eResearch Centre, James Cook University. His research interests include environmental monitoring, sensors, data management, and supramolecular chemistry. He has involved in various professional/corporate IT roles and is a recipient of several major research grants.