Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Best Practices for Heterogenous Health IoT Integration into Electronic Health Records

CAPSTONE REPORT

Jeffrey K. DeWitt
Sr. Systems Administrator
Kaiser Permanente

University of Oregon
Applied Information
Management
Program

Spring 2019

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-271

Approved by

Dr. Kara McFall
Director, AIM Program

Best Practices for Heterogenous Health IoT Integration into Electronic Health Records

Jeffrey K. DeWitt

Kaiser Permanente

Abstract

Health IoT represents an agglomeration of medically-based devices that automate collection, communication, and processing of health data (Da Costa, Pasluosta, Eskofier, Da Silva, & Da Rosa Righi, 2018). This study examines how healthcare institutions can integrate heterogenous data into electronic health records. Key potential benefits are within precision medicine (Prosperi, Min, Bian, & Modave, 2018), patient chronic illnesses (Peng & Goswami, 2018), and advanced patient monitoring inside and outside of hospitals (Rodrigues et al., 2017).

Keywords: Health IoT, wearables, Big Data, Cloud computing, electronic health record, smart healthcare, semantic ontology, autonomic computing, cognitive computing, machine learning, and artificial intelligence.

Table of Contents

Introduction to the Annotated Bibliography

Problem

The Internet of Things. The Internet of Things (IoT) refers to "network-enabled technologies, including mobile and wearable devices, which are capable of sensing and actuation as well as interaction and communication with other similar devices over the Internet" (Sheth, Jaimini, & Yip, 2018, p. 89). The Internet of Things includes common physical objects that are embedded with computing devices that can send and receive data (Laplante & Laplante, 2016). Hu, Chen, Fan, and Wang (2017) note recent advancements towards the ability to connect IoT devices to large data pools, such as those stored within Cloud environments. Cloud technologies offer greater flexibility, unlimited resources, immense processing power, and the ability for quick response to the user (Hu et al., 2017). When combined with IoT, Cloud technologies offer a gateway for medical data processing and storage that facilitates remote health monitoring technologies in real-time, reducing clinician time and hospital costs and improving the quality of care (Rodrigues et al., 2017).

In conjunction with advancements to the core facilitating technologies of IoT, there has been a rapid increase in the quantity of available physiological sensors, low-power integrated circuits, and wireless communications to enable an entirely new generation of wireless sensor networks (Hu et al., 2017). Accompanied by advancements in network connectivity, Cloud technologies, and sensors, *wearables* have developed greatly and are considered reliable tools for long-term health monitoring systems (Haghi, Thurow, Habil, Stoll, & Habil, 2017). There are a wide range of wearable health monitoring systems with a common definition of "devices that can be worn or mated with human skin to continuously and closely monitor an individual's activities, without interrupting or limiting the user's motions" (Haghi et al., 2017, p.5). Laplante and

Laplante (2016) note that IoT wearables technology “can deliver comprehensive patient care in various settings, such as acute (in-hospital), long-term (nursing homes), and community-based (typically, in home)” (p.2).

Health Internet of Things. Iqbal et al. (2018) coined the term *health Internet of Things (health IoT)* and defined it as a critical component of “the health information system development, in which IoT concepts are applied to the health field” (p. 1). Other terms from the literature for this specific application of IoT are *Internet of Health Things* (Rodrigues et al., 2017) and *medical-IoT* (Dimitrov, 2016). This study will use the term *health IoT* in reference to these technologies.

Heterogeneous health IoT data and platforms create a unique opportunity for healthcare institutions (Mezghani, Exposito, & Drira, 2017). Health IoT-based systems possess the ability to capture real-time data and offer benefits beyond connecting *things*, namely the transformation of collected data into insights and the ability for patients to interact with health practitioners for better health decision-making (Mezghani, et al., 2017). Health IoT data can provide a rich source of patient health data delivered through physiological IoT devices that is inexpensive, continuous, and delivered in real-time (Hu et al., 2017).

The National Institutes of Health (NIH) defines precision medicine as the “approach for disease treatment and prevention that takes into account individual variability in genes, environment, and lifestyle for each person” (Prosperi, Min, Bian, & Modave, 2018). A common understanding of precision medicine is the customization of disease treatment for a single individual (Prosperi et al., 2018). In the common within the present paradigm is a one-size-fits-all medical approach or treatment known to benefit the majority of the target population, captured in a term of *number needed to treat (NNT);* a measure indicating the average number of people who need to be treated to avert one additional bad outcome (Prosperi et al., 2018). As this is commonly resulting in populations of patients not receiving positive health outcomes, Prosperi et al. (2018) argue that "this exemplifies the need for customized treatment based on variables such as genetics, ethnicity or lifestyle. The underlying assumption is that precision medicine will provide tailored healthcare to patients and will yield lower rates of associated outcomes" furthermore, "given detailed patient characteristics, it is possible to more accurately predict the expected effect of each treatment option and, thus, to optimize care" (p. 2). Dimitrov (2016) identifies the benefits of medically-based IoT within the scope of precision medicine, allowing for multiscale data for analysis and interpretation at the individual patient level rather than more generic assessments.

An application of health IoT that shows promise is better management of patient chronic illnesses (Peng & Goswami, 2018). As chronic diseases have become one of the dominant threats to the health of patients and a substantial management challenge for healthcare systems all over the world, the strategy towards long-term and periodic management of these diseases must evolve with methodologies that allow patients to perform self-management within their homes as a means to mitigate the high costs and inconvenience of acute care that becomes necessary in response to insufficient maintenance of chronic diseases (Peng & Goswami, 2019). Health IoT shows promise in assisting in this shift towards patient self-management within the home for chronic diseases by combining and collaborating data from personal health management to provide a comprehensive overview and increased understanding of a patient's health (Peng & Goswami, 2019). Sheth, Jaimini, and Yip (2018) describe stages of technology-enabled health augmentation; health IoT allows patients to graduate from paradigms of self-monitoring, self-appraisal, and self-management where there is little expertise and data to support care decisions, to more mature levels of intervention along with disease progression tracking and prediction that ultimately deliver better care outcomes.

In addition, Health IoT encourages better self-care facilitated through health data gathered by tracking devices that provide actionable information and knowledge of one's health, ultimately enabling the identification of focused behavioral changes (Peng & Goswami, 2019). This use of health IoT fits with the shifting market demands healthcare institutions are experiencing from patients towards a *customer-oriented delivery of care* where traditional access points of care such as outpatient primary care offices and emergency departments must also be matched with strong investments in consumer-oriented access points such as virtual visits, retail clinics, and urgent care centers (Anton & Caldararo, 2018).

The American population is also skewing towards an aging population, with long-term care requirements that conflict with the limited supply of medical and financial resources and hospitals (Hu et al., 2017). Health IoT data and insights gained through tracking devices can enable the facilitation of at-home, self-managed care for elderly patients (Hu et al., 2017). For example, tracking devices on elderly patients can provide fall risk assessment and monitoring (Haghi, Thurow, Habil, Stoll, & Habil, 2017), supervision of fitness activities within the home environment (Rodrigues et al., 2017), continuous monitoring of vital signs (Hu et al., 2016), as well as monitoring of recovery from an injury or surgery (Dimitrov, 2016).

Health IoT biomedical sensors present the ability for monitoring of electroencephalogram (brain activity), electrocardiography and heart rate (heart monitoring), metabolic disorder and blood glucose (diabetes monitoring), among other vital signs; doing so through various sensors that include the measurement of pulse, oxygen-in-blood (SpO2), airflow, body temperature, glucometer, galvanic skin response, blood pressure, patient position, and electromyography (Rodrigues et al., 2017).

Patients with Alzheimer’s disease may benefit from the adoption of geolocation health IoT wearables to prevent wandering or other unwanted mobility behaviors (Laplante & Laplante, 2016). Patients with bulimia or related eating disorders can benefit from detection of increased body temperature and blood pressure, exercise abuse, or even vomiting, allowing for better diagnosis and management of the illness (Laplante & Laplante, 2016).

Health IoT Integration with Electronic Health Records (EHRs). Medical informatics is the intersection of information science, computer science, and healthcare; it involves the disciplines of resource and device management required to optimize the acquisition, storage, retrieval, and use of information in health and biomedicine (Michigan Technology University, 2019). Medical informatics improve patient care by improving the ability of patients to self-manage illness and maintaining and optimizing EHRs, reducing costs and errors, which further results in less trial and error (University of Illinois at Chicago, n.d.).

Dimitrov (2016) notes that the convergence of medicine and information technologies will ultimately transform healthcare by reducing costs and inefficiencies while improving patient lives. Health IoT’s estimated $117 billion market value is expected to further transform medicine by creating a more personal effect with patients. Peng and Goswami (2019) note that these improvements have implications for healthcare institutions’ electronic health record (EHR) systems; capitalizing on the improvements established by medical informatics. As healthcare organizations adopt IoT to reduce costs and improve patient monitoring (Mezghani et al., 2017), the role of medical informatics will expand as institutions will be required to develop an internal strategy to meaningfully integrate data from heterogeneous health IoT sources into their EHR systems (Peng & Goswami, 2019). According to the United States Department of Health and Human Services, electronic health records (EHR) systems are defined as:

> A digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care (DHS, n.d.).

Alamri (2018) asserts that because healthcare IoT sensor technology contains health-related data, health-based IoT data must be integrated into EHRs, which are meant to comprise a complete health record for the patient and enable health providers to monitor their patients outside of the traditional clinic setting (p. 1). Moreover, IoT integration into EHRs can capture data on a patient's activities and vital signs and add this valuable data to the patient's medical record (Dimitrov, 2016).

Challenges Posed With Integrating Health IoT Data. Alamri (2018) notes however that while configuring IoT into EHRs can enhance patient healthcare by enabling health providers to monitor their patients external to the clinical setting, most EHRs have been designed to be patient-centric management systems that are not oriented to IoT integration (2018). Many EHRs do not yet possess the inherent information architecture to integrate health IoT data without additional tools or enhancements (Alamri, 2018). Healthcare institutions attempting to develop comprehensive overviews of patient health both internal and external to the clinical setting by adopting value-adding health IoT data within their EHRs will face challenges (Peng & Goswami, 2019).

The transmission of health IoT data to EHR systems and the storage of this data within these systems poses security challenges (Strielkina, Illiashenkoi, Zhydenko, & Uzun, 2018). “Information that is being delivered from sensors might appear to be correct, but could be corrupted somehow at the origin or during transmission, or deliberately altered by malware that can gain unwanted access to the IoT via the Internet” (Laplante & Laplante, 2016, p. 3). Within the realm of cybersecurity, Hu et al. (2017) note the requirement to mitigate security threats to health IoT data so that patient records are not negatively impacted and recommend doing so through the design and integration of security measures such as authentication to maintain the confidentiality of health IoT data. Strielkina et al. (2018) note that “dealing with patients' medical data, confidentiality and security and privacy are prevalent for a good health-related product. During transferring and syncing information between networked and connected healthcare devices, data should be encrypted from endpoint to endpoint” (p. 67).

Mezghani et al. (2017) note that IoT produces a complex *System of Systems* (SoS) that outputs a myriad of heterogeneous data; given the dynamic evolution of system requirements within EHRs, the addition of this heterogeneous data to electronic health records poses increasingly greater challenges within the arenas of big data and scalability management. As noted by Bresnick (2016), “standardizing and normalizing that data, especially when it comes from consumer devices that are not necessarily concerned with the ability to interoperate with electronic health records, is one of the biggest obstacles in the way of creating a meaningful IoT for healthcare” (p. 1). Thus, the challenge is that health IoT data is easy to collect, but difficult to manage and secure (Mezghani et al., 2017; Strielkina et al., 2018).

Dimitrov (2016) states that a key fundamental challenge of IoT is communication; many devices collect data through sensors but then interface to proprietary servers using their own computer languages, making interoperability between heterogeneous devices difficult. Reda, Piccinini, and Carbonaro (2018) elaborate that due to the high heterogeneity of data representation formats in IoT, the overall IoT healthcare landscape is characterized by a “ubiquitous presence of data silos which prevents users and clinicians from obtaining a consistent representation of the whole knowledge” (p. 5) of the patient data due to gaps between silos.

Sheth, Jaimini, and Yip (2018) note that health IoT data and insight-producing information are inadequate to fully understand an individual’s health and associated aspects of well-being and overall fitness; at current and likely into the future, health data generated by IoT will be used as supplemental information to an individual's clinical record and behavioral information. Despite this shortcoming, Dimitrov (2016) contends that health IoT technology will enable patients and healthcare providers to use medicines with advanced sensor hardware that provides key physiological data and enables the creation of personalized care services and processes (p. 158). In addition to providing real health benefits for patients, this particular use of IoT will lead to a significant opportunity for innovation and competitive advantage for healthcare institutions that are successful in integrating the emergence of new kinds of service platforms and business models with their currently existing EHR systems (Dimitrov, 2016).

Purpose

The purpose of this annotated bibliography is to present literature that addresses the challenge of integrating heterogenous IoT data and devices into electronic health records. The focus will be to examine the current theoretical, experimental, and applied methodologies to securely integrate health IoT data and information into EHRs. This annotated bibliography will identify current literature that examines the best practices available to integrate IoT data within an EHR. The scope will include the domains of cybersecurity pertaining to IoT patient data, the management of large scales of data, and the relationship between vendor public Cloud storage and interfaces into private institutional networks hosting EHRs.

As heterogeneous IoT devices commonly create heterogeneous data (Reda, Piccinini, & Carbonaro, 2018), the challenge is to utilize the data to create a comprehensive overview and an increased understanding of patient behaviors and health, with the goal of leading to better health outcomes for the patient (Peng & Goswami, 2019) and increased efficiency and competitive advantage for healthcare organizations (Dimitrov, 2016). The focus of this review is to provide technical overviews and best practices in the application of health IoT data into EHRs.

Research Questions

Main question. What are best practices and technologies for healthcare institutions to successfully integrate patient health IoT data from heterogenous sources into their electronic health records?

Sub-questions.

- What technology platforms, infrastructure, and methodologies are required to integrate health IoT into an EHR?
- How do healthcare institutions leverage and maximize the value of heterogenous health IoT data?
- How do healthcare institutions manage large scales of health IoT data through the *3Vs of big data*: velocity, volume, and variety (Mezghani, et al., 2017)?

Audience

The intended audience and stakeholders for this study are primarily composed of those within the healthcare industry and technology fields related to IoT such as data management and analysis, networking, and Cloud-computing. Within the healthcare industry, the audience will include clinical leadership and those responsible for the senior management of information technology.

As stakeholders, healthcare and medical leaders will benefit from this study as it serves to provide a basis for how the rapidly developing health IoT marketplace can integrate into their existing EHR systems and provide clinical as well as patient value. Currently health IoT represents over 40% of all IoT devices, the largest proportion of any industry, and is valued in surplus of $117 billion (Dimitrov, 2016). Artiga and Hinton (2018) cite Schroeder (2007) in identifying that social determinants of total health extend beyond care within a clinical health care setting (10%) to matters such as social environmental factors (20%), genetics (30%), and individual behavior (40%). A *whole-person approach* to healthcare as described by Christensen, Waldeck, and Fogg (2017), where a patient sees a physician for an acute issue and then is encouraged to adopt new health habits by using telehealth technologies such as IoT and health coach assistance, can significantly reduce costs and improve health outcomes. As the number of use cases of health IoT and patient demand increase, hospital and medical groups will need to increase their capability of supplying an integration between the health IoT devices and their EHRs (Rodrigues et al., 2017). Clinical professionals, including physicians and clinicians, will be vital stakeholders in determining the data and presentations of such data that will be most beneficial to the healthcare of their patients within their specific institutions.

Technology professionals who will benefit from this study include those within the facets of data sciences, network services, cybersecurity, and EHR developers. Data scientists and analysts will benefit from models such as “Intelligent Building” as noted by Rathmore, Ahmad, Paul, Wan, and Zhang, (2016) that propose a layered architecture and implementation model that promotes analysis and decision-making using Big Data collected from health IoT devices. Network and cybersecurity professionals will gain value from this study through the presentation of literature that explains the need for those who transmit, store, and use patient health IoT data to adopt confidentiality, security, and privacy measures throughout the processes of transferring, syncing, and the storing health IoT data (Strielkina, et al., 2018). Furthermore, Strielkina et al. (2018) identify issues within health IoT data's landscape that pertain to network cybersecurity; this study presents potential mitigations of these concerns when integrating health IoT data into EHRs. Infrastructure support professionals who interface private and public Cloud data will be interested in strategies that allow for flexibility, scalability, and interoperability of heterogeneous information services and architecture (Hu et al., 2017).

The direct intended benefit to this audience is the ability to assess the latest methodologies and applicability of health IoT within their specific EHRs and institutions. The intent is not to provide findings that are specific to a single organization, but rather to outline best practices for applicability across all healthcare institutions developing IoT processes.

Search Report

Search strategy. I embarked on a three-tier search strategy for this annotated bibliography. The first tier focused on using standard searches online to develop a better grasp of the concepts I was exploring and to obtain keywords for searches in academic library settings. To obtain terminologies within the industry, I used Google Scholar and standard Google searches.

Some of the terms I encountered included certain computer science terms with which I was less familiar, such as *ontology* and *autonomic computing*. By learning about these subjects, I became more aware of the meanings and keywords related to my topic within academic databases.

An additional tier of research was my use of reference sections of the academic journals I read. As these fields are interconnected, I identified many additional and useful sources by leveraging these sections. Finally, I ensured that these resources were peer-reviewed and did not show evidence of biases.

Key Terms. I gathered the following terms from extensive searches and from scholarly articles, books, published white papers, and similar sources.

- Health IoT,
- Heterogenous IoT,
- Electronic Health Record,
- EHR,
- Autonomic computing,
- Big Data,
- Cloud computing,
- Wearables,
- Smart healthcare,
- Cognitive computing, and
- Semantic web technologies and data models.

Search engines and databases. In addition to Google Scholar, I used the UO online library resources and databases as an additional tier of focus. The databases I queried were:

- IEEE Xplore,
- IEEE Access,
- Academic OneFile,
- ACM Digital Library,

- PubMed - U.S. National Library of Medicine National Institutes of Health, and
- Elsevier.

I selected databases that pertain to Computer Science and Healthcare/Medicine. I was able to identify a plethora of resources concerning IoT. I encountered additional terminology such as “mIoT” for *medical* IoT and “health IoT” as I reviewed materials. Because this study is less concerned with the specifics of medical/health IoT and instead focuses on the ability of this technology to integrate into an EHR, I carefully reviewed abstracts to ensure applicability and relevancy. I discarded articles that were returned from searches that did not maintain applicability. As I reviewed the applicable literature, I further filtered my sources based on the reference valuation criteria as described in the subsequent section.

A significant amount of content related to the research topic of technical models of health IoT, applied and theoretical. I discovered that the terminology can vary across the academic articles; some use “mIoT” and others use “health IoT.” I did not find an official definition that claimed differences between these two terms, but observed “medical IoT” was more commonly used in sources focusing on the medical applicability of IoT and less on its technical uses. Overall, sources were plentiful and allowed me to include ample academic and professional sources in my annotated bibliography.

Documentation approach. I documented and captured all references and citations within this study using a single categorized note-taking document within Google Docs. I stored all academic studies and other digital media in Adobe portable documents format (PDF) and categorized sources based on their focuses. I classified each document with an applied coding methodology, which used a coding system of an applied three-digit number correlating the study to corresponding notes stored within the Google Docs document. I stored all relevant information pertaining to searches, citations, and other vital information within this centralized document, which allowed me to make comments on content, searchable keywords, and indexing based on relevancy. I reviewed studies within an iOS and MacOS application called Notability and applied annotations, comments, and other notes within this application.

Reference evaluation criteria. I evaluated potential references for the Annotated Bibliography section of this paper for their authority, currency, quality, relevancy, and potential bias. I developed these evaluations with the use of the criteria from the Center for Public Issues Education *Evaluating Information Sources* model (Center for Public Issues Education, n.d.)

Authority. I applied a strong emphasis and focus to the author(s)' credentials, professional experience, and credibility. I evaluated the authors based on their academic backgrounds, contributions, and related work in the area of IoT. Many, if not all, of the authors cited in this study received their Ph.D and M.S. degrees in the arena of IoT or medical studies. In addition, a few of the authors I identified as active professors focusing in the research of IoT platforms.

I also prioritized articles that I confirmed as peer-reviewed. I ranked academic articles that were peer-reviewed higher, along with those that included an extensive references section. Furthermore, each academic article that I selected for this study was published in a university press, professional society, or scholarly journal, all of which apply a strict editing and review process.

Timeliness. I reviewed all resources for their currency. I prioritized resources published within five years of this study's writing due to the rapid developments in health IoT. I reviewed articles with a publishing date surpassing this time period for additional contextual understanding, but did not utilize these sources for information about current affairs pertaining to health IoT. I also reviewed established technical theories and facets as a means to elaborate on the core foundational technologies supporting health IoT.

Quality. All resources cited within this study were published in academic journals and therefore have undergone the rigorous reviews associated with scholarly publications.

Relevancy. References cited within this study are relevant to the central research question and subsequent sub-questions. To qualify for citation, a reference needed to pertain to one of the categories in the annotated bibliography and address at least one of the research questions posed for this study.

Bias. I evaluated all resources for their merits and objective status. I included no sources that endorsed products, services, or non-academic purposes. I evaluated authors for their academic merit and purpose. I reviewed the author's section of each article as well as any sections within the article that identified funding sources or potential conflicts of interest. I scrutinized and commonly discarded any sources that demonstrated clear conflict of interest or non-academic funding sources.

Annotated Bibliography

Introduction to the Annotated Bibliography

The following references are exhibited to elucidate and summarize their content and applicability towards this study. Each annotation includes: (a) a complete APA formatted bibliographic citation, (b) the published abstract provided by the author(s), in full or in essential constituency, and (c) a key point summary that addresses the relevancy and applicability towards this study; for example, how the reference addresses the problem posed, provides potential solutions or alternatives, and benefits the designated audience.

Category 1: Healthcare Applicability of IoT

Baker, S., Xiang, W., & Atkinson, I. (2017). Internet of Things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, 5, 26521-26544. doi:10.1109/ACCESS.2017.2775180

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.

Summary. This article presents a universal and generic model that identifies all key components of an end-to-end IoT healthcare system. The authors suggest health IoT is of use with critical patients within a hospital system as well non-critical patients within a home setting to allow for a reduction in strain on hospital resources, including physicians. Health IoT may also serve as a benefit to those living in rural areas and geriatric patients living independently at home.

The authors further identify significant disadvantages of health IoT, such as the security risk of centralizing large amounts of sensitive data within a single database; the possible need to recalibrate sensors; and possible network connectivity disconnections from healthcare services, including cellular connections; the authors suggest that all of the challenges are mitigatable. The authors' recommended mitigations include: (1) wearable sensor and central nodes where data is received from sensor nodes (health IoT devices) and information is processed to a decision-making outcome prior to being transferred to an external location (Cloud), (2) Short-range communications protocols for sensor-to-central nodes with consideration for the effects to the human body, cybersecurity, and latency of these communications, (3) Long-range communications where data is obtained by the health IoT device and then forwarded to a database where relevant parties can securely access it, and (4) Secure Cloud storage architecture and machine learning where the large data sets are stored and machine learning is used to identify trends that would potentially remain unknown otherwise, providing treatment plans and recommendations based on the specific individual patient.

Based on their review of existing IoT research, the authors recommend effective IoT devices, including non-invasive and non-intrusive external *wearables,* along with scenario-based environmental or vision-based sensors within a home setting. Communication between these devices, such as Bluetooth transferring of sensor data to a smartphone and then middleware to transfer data to the Cloud, is essential. A limitation of smartphones is the internal batteries must be recharged and the risk posed by a medical event occurring when the device is either de-energized or disconnected from a network or data transfer protocol. Due to the large volumes of data created by Health IoT devices, machine learning algorithms are necessary within the Cloud architecture to identify previously unknown disease trends and provide diagnostics and treatment plans. The authors present a framework consisting of: (a) wearable sensors and dedicated central nodes that includes IoT devices and a smartphone, (b) short-range communications, such as low-power wide area network (LPWAN) and Bluetooth, (c) long-range communications, transferring data at low-latency to a destination (Cloud), and (d) secure Cloud storage architecture that is machine learning enabled. The machine learning enabled Cloud environment is capable of reducing large volumes of data into higher value insights that can be further integrated into external sources, such as an EHR.

The value of this study is that it provides a logical framework that encompasses heterogenous IoT sensor data and a centralized node unit at the patient level that further creates the opportunity for high-value insights using a Cloud-based machine learning platform that reduces data streams to manageable levels within an interface to EHRs.

Dimitrov, D. (2016). Medical Internet of Things and Big Data in healthcare. *Healthcare Informatics Research, 22*(3), 156-163. http://dx.doi.org/10.4258/hir.2016.22.3.156

Abstract. A number of technologies can reduce overall costs for the prevention or management of chronic illnesses. These include devices that constantly monitor health indicators, devices that auto-administer therapies, or devices that track real-time health data when a patient self-administers a therapy. Because they have increased access to high-speed Internet and smartphones, many patients have started to use mobile applications (apps) to manage various health needs. These devices and mobile apps are now increasingly used and integrated with telemedicine and telehealth via the medical Internet of Things (mIoT). This paper reviews mIoT and big data in healthcare fields.

Methods mIoT is a critical piece of the digital transformation of healthcare, as it allows new business models to emerge and enables changes in work processes, productivity improvements, cost containment and enhanced customer experiences.

Results Wearables and mobile apps today support fitness, health education, symptom tracking, and collaborative disease management and care coordination. All those platform analytics can raise the relevancy of data interpretations, reducing the amount of time that end users spend piecing together data outputs. Insights gained from big data analysis will drive the digital disruption of the healthcare world, business processes and real-time decision-making.

Conclusions A new category of "personalized preventative health coaches" (Digital Health Advisors) will emerge. These workers will possess the skills and the ability to interpret and understand health and well-being data. They will help their clients avoid chronic and diet-related illness, improve cognitive function, achieve improved mental health and achieve improved lifestyles overall. As the global population ages, such roles will become increasingly important.

Summary. The author of this article identifies the challenges, benefits, and potential capabilities of health IoT technologies. The author notes that one of the major challenges in implementing IoT is with communication; many of the health IoT devices currently on the market are heterogeneous and communicate to host servers within their own proprietary computer languages. This fragmentation is coupled with privacy concerns and bureaucratic tendencies to hoard all collected information within vendor platforms, creating what is referred to as *data islands.* Additional challenges include resolving legacy fragmentation within EHR and IoT data. As increasingly standardized vocabularies and formats become more common, the problem of data fragmentation and a lack of normalization of data into consistent structures around a unique patient identifier is exacerbated with the use of legacy EHR and IoT data structures.

Dimitrov asserts that to become successful in adopting IoT devices and data within an EHR system, firms must achieve five key capabilities: (a) simple connectivity, where IoT devices are easily connected to Cloud-based services, (b) easy device management, where assets are maintained with minimal outages, (c) information digestion, where diverse IoT data is transformed to essential values, (d) informative analytics, where insights and better decision-making is facilitated, and (e) reduced patient risk, where notifications of incidents allow quick resolution. Dimitrov also notes that healthcare organizations adopting health IoT devices and data will need to account for the *three V's of Big Data*: volume, variety, and velocity.

The author also notes potential benefits of using health IoT data. By leveraging health IoT data, healthcare providers can test hypotheses for better understanding on nutrition, fitness, disease progression, and treatment success, as well as provide a continuously updated view of patients. In addition, health insurers and hospitals can reduce re-admission rates by "targeting patients where predictive artificial intelligence (AI) algorithms indicate people who may be at highest risk based on an analysis of available data collected from existing patient records" (p. 5).

The value of this article is that it presents the challenges and possible mitigations of health IoT integration within EHRs from both a medical and value standpoint. The audience most benefiting from this article will be medical professionals and leadership along with data management teams.

Laplante, P., & Laplante, N. (2016). The Internet of Things in healthcare: Potential applications and challenges. *IT Professional, 18*(3), 2-4. doi:10.1109/MITP.2016.42

Introduction. The Internet of Things (IoT) is a collective term for any one of the many networks of sensors, actuators, processors, and computers connected to the Internet. Healthcare applications for the IoT can potentially deliver comprehensive patient care in various settings, including acute (in-hospital), long-term (nursing homes), and community-based (typically, in-home).

An IoT has the potential to accurately track people, equipment, specimens, supplies, or even service animals and analyze the data captured. With patients attached to sensors to measure vital signs and other biometric information, problems could be more rapidly diagnosed, a better quality of care given, and resources used more efficiently.

Summary. In this article, the authors discuss the potential applications and challenges of health IoT. Applications of health IoT include utilizing sensors to detect: (a) exercise abuse, (b) decreased body temperature, (c) decreased blood pressure, (d) odors from vomit in patients with bulimia, (e) hypertension, (f) macular degeneration, (g) diabetes, (h) mobility and falls among elderly patients, and (i) geolocations of patients with Alzheimer's disease. At the hospital-level, health IoT that uses low-cost RFID tags can track and inventory many supplies. The authors state that health IoT "could substantially improve patient care, optimize resource utilization, and save vast amounts of money, [but only] if the systems could be built" (p.3). Along this note, the authors present challenges, including *security* of the health IoT devices; the *loss of privacy* due to the tradeoff between security, functionality, and privacy; along with *trust* that information that is being delivered from sensors is correct, not corrupted, and not subject to forms of malware. Ultimately, if health IoT can mitigate these challenges and becomes scalable, it will improve workflow, optimize scarce resources, and provide the potential for cost savings.

Rodrigues, J., Segundo, D., Junqueira, H., Sabino, M., Prince, R., Al-Muhtadi, J., & Albuquerque, V. (2017). Enabling technologies for the Internet of Health Things. *IEEE Access*, *6*, 13129-13141. doi:10.1109/ACCESS.2017.2789329

Abstract. The Internet of Things (IoT) is one of the most promising technologies for the near future. Healthcare and well-being will receive great benefits with the evolution of this technology. This paper presents a review of techniques based on IoT for healthcare and ambient-assisted living, defined as the Internet of Health Things (IoHT), based on the most recent publications and products available in the market from industry for this segment. Also, this paper identifies the technological advances made so far, analyzing the challenges to be overcome and provides an approach of future trends. Through selected works, it is possible to notice that further studies are important to improve current techniques and that novel concept and technologies of IoHT are needed to overcome the identified challenges. The presented results aim to serve as a source of information for healthcare providers, researchers, technology specialists, and the general population to improve the IoHT.

Summary. The authors discuss applications of health IoT devices in collaboration with EHR deployments; namely, health IoT devices can provide data on electrocardiography; heart rate; electroencephalogram, electromyography; diabetes; and other body vital signs such as pulse, oxygen in blood (SPO2), airflow, body temperature, blood glucose, galvanic skin response, blood pressure, and patient position. Tangible examples of health IoT and EHR integrations include monitoring patients in rural or low density populations through the aggregation of body vital signs that may not be collected as regularly without heath IoT devices, as well as measuring and transmitting blood pressure during cardiac rehabilitation and pregnancy, measuring and transmitting knee flexion range of motion post total knee arthroplasty, Parkinson disease monitoring, bipolar disorder episode detection, automatic detection of chronic wounds based on color and size features, skin monitoring for early detection of melanoma, medical check reminders, as well as interconnected sensors for elderly patients that detect falls and episodes of Alzheimer's related activities. Health IoT presents a potential for cost savings for patients and hospital systems, quality of life improvements for patients with chronic disease, needed health monitoring, and the prevention of disease complications.

Remote health monitoring technologies are adopted by homecare, clinicians, and hospital environments to remotely monitor the vital signs of patients in real-time, particularly when looking for abnormalities from standard patient health. The authors conclude that there are many potential opportunities of services and applications created by health IoT; however, many of the options are currently becoming more isolated. The authors recommend that vendor firms and developers build solutions that embrace interoperability.

The value of this article is that it presents opportunities of leveraging health IoT technology within an integrated EHR system and options for how health IoT devices can better enhance patient outcomes while integrating with currently existing medical records stored in an EHR system. The audience most benefiting from this article will be medical professionals and leadership implementing health IoT.

Sheth, A., Jaimini, U., & Hong, Y. (2018). How will the Internet of Things enable augmented personalized health? *IEEE Intelligent Systems, 33*(1), 89-97. doi:10.1109/MIS.2018.012001556

Abstract. The Internet of Things refers to network-enabled technologies, including mobile and wearable devices, which are capable of sensing and actuation as well as interaction and communication with other similar devices over the Internet. The IoT is profoundly redefining the way we create, consume, and share information. Ordinary citizens increasingly use these technologies to track their sleep, food intake, activity, vital signs, and other physiological statuses. This activity is complemented by IoT systems that continuously collect and process environment-related data that has a bearing on human health. This synergy has created an opportunity for a new generation of healthcare solutions.

Summary. The authors discuss the ability of health IoT to augment personalized health through monitoring of sleep, food intake, activity, vital signs, and other physiological data. The authors assert that health IoT presents a “paradigm shift from reactive medicine to proactive and preventative medicine [that] is primarily motivated by economic imperatives such as the rising cost of healthcare, as well as continued improvements on quality of life and longevity” (p. 1). The authors also note that “health IoT data alone is not adequate to fully understand an individual's health and associated aspects of well-being and fitness; it is necessary to look at that individual's clinical record and behavioral information, as well as social and environmental information affecting that individual" (p. 2). The authors thus present the need to integrate health IoT data into EHR systems to augment personalized healthcare. The authors define augmentation as "aggregating this data and converting into actionable information that can improve health-related outcomes through better and more timely decisions" (p. 2). The authors propose that augmenting is accomplished through (a) aggregation of data, (b) conversion of data, and (c) creation of actionable data.

The authors further identify stages of health IoT enabled, augmented care as: (a) self-monitoring, (b) self-appraisal, (c) self-management, (d) intervention, and (e) disease progression tracking and prediction. To achieve these stages, contextual or condition-specific annotation, integration, and interpretation of sensor data using *Semantic Sensor Network (SSN) ontology* is required. They note that SSN ontology will need to incorporate contextualization, abstraction, and personalization to allow for the accurate understanding and use of health IoT data. This method employs machine learning algorithms and data analytics with reasoning engines and knowledge bases to support augmented personalized healthcare. The principle goal of this effort is to achieve actionable information that is based on meaningful information that supports decision making towards the improvement of patient health. The authors conclude that while a transition from cohort-based treatment, where a larger population is considered, to more personalized treatment is necessary to improve patient outcomes.

The value of this article is that it presents a paradigm and framework to create meaningful and actionable data from health IoT that can be integrated into an EHR system. The audience most benefiting from this article will be medical professionals and technologists within data management.

Category 2: IoT Integration with Electronic Health Records

Alamri, A. (2018). Ontology middleware for integration of IoT healthcare information systems in EHR systems. *Computers, 7*(4), 1-15. doi:10.3390/computers7040051

Abstract. Healthcare sectors have been at the forefront of the adoption and use of IoT technologies for efficient healthcare diagnosis and treatment. Because healthcare IoT sensor technology obtains health-related data from patients, it needs to be integrated with the electronic healthcare records (EHR) system. Most EHR systems have not been designed for integration with IoT technology; they have been designed to be more *patient-centric management systems*. The use of the IoT in EHR remains a long-term goal. Configuring IoT in EHR can enhance patient healthcare, enabling health providers to monitor their patients outside of the clinic. To assist physicians to access data resources efficiently, a data model that is semantic and flexible is needed to connect EHR data and IoT data that may help to provide true interoperability and integration. This research proposes a semantic middleware that exploits ontology to support the semantic integration and functional collaborations between IoT healthcare Information Systems and EHR systems.

Summary. In this article, the author asserts that "because healthcare IoT sensor technology obtains health-related data from patients, it needs to be integrated with electronic health records (EHR) systems" (p. 1). Despite this need, EHR integration of

IoT data remains a long-term goal because the design architecture of EHRs are more *patient-centric management systems;* current EHR designs focus on facilitating the management of health information and records related to medications, diagnoses, hospital admissions, operations, imaging, laboratory tests, and pathology data. Future EHR designs and versions are needed to integrate IoT technology, which will allow a health provider to monitor a patient's health status related to chronic and acute conditions.

A prevalent challenge within health IoT is that many devices have sensors that collect data, but use data formats that are typically "locked into uni-modal closed systems" (p. 2). To mitigate this challenge, the author identifies *Semantic Web Technologies* that can be used to define the data collected from health IoT devices and normalize the structures and relationships of the complex and unstructured health data contained within EHRs. Furthermore, the Semantic Web provides a basis of well-defined information framework and interoperation middleware for IoT and EHR data that will "facilitate data interoperability, integration, information search and retrieval, and automatic inference" (p. 2). The semantic web ontology needed to do so consists of an EHR and IoT *triplestore*, or purpose-built database for each, and semantic integration process. The core goal of the semantic web ontology is to improve care by configuring IoT within an EHR to "collect actionable data that can be used for treatment or other interventions" (p. 7). Measures of success for healthcare organizations implementing this strategy will be: (a) the ability to share data with health information systems (EHR systems) and (b) scalability in order to handle the increasing amount of data stored.

The value of this article is that it creates a theory of semantic web ontologies between IoT and EHR data and frameworks to allow interoperability. The audience valuing this material will be data management and Cloud operations teams.

Da Costa, C., Pasluosta, C., Eskofier, B., Da Silva, D., & Da Rosa Righi, R. (2018). Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. *Artificial Intelligence In Medicine, 89*, 61-69. doi:10.1016/j.artmed.2018.05.005

Abstract. *Background:* Large amounts of patient data are routinely manually collected in hospitals by using standalone medical devices, including vital signs. Such data is sometimes stored in spreadsheets, not forming part of patients' electronic health records, and is therefore difficult for caregivers to combine and analyze. One possible solution to overcome these limitations is the interconnection of medical devices via the Internet using a distributed platform, namely the Internet of Things. This approach allows data from different sources to be combined in order to better diagnose patient health status and identify possible anticipatory actions.

Methods: This work introduces the concept of the Internet of Health Things (IoHT), focusing on surveying the different approaches that could be applied to gather and combine data on vital signs in hospitals. Common heuristic approaches are considered, such as weighted early warning scoring systems, and the possibility of employing intelligent algorithms is analyzed.

Results: As a result, this article proposes possible directions for combining patient data in hospital wards to improve efficiency, allow the optimization of resources, and minimize patient health deterioration.

Conclusion: It is concluded that a patient-centered approach is critical, and that the IoHT paradigm will continue to provide more optimal solutions for patient management in hospital wards.

Summary. This article addresses the possibilities of health IoT within the scope of monitoring vital signs in hospital wards. Patients are routinely assessed during hospitalizations by measuring vital signs and these observations are crucial to preventing health deterioration, potentially minimizing morbidity and mortality, abridging hospitalization time, and reducing costs. Currently, many of these assessments are conducted manually and stored in sub-optimal locations, as well as discarded after the patient is discharged. Health IoT creates an opportunity for partially or fully automatized collection of vital signs, diminishing the burden imposed on nurses and allowing for more comprehensive data collection. A distributed platform of health IoT to process and store data can be merged with machine learning algorithms to "infer the risk of patient health deterioration, and to optimize resources in hospitals by predicting future patient requirements" (p. 1).

A core required integration involves EHR systems that act as data repositories of information regarding patient health statuses, which creates a need for heath IoT data within a hospital ward setting to be interfaced with EHR systems. To successfully integrate, the authors propose four distinct layers with a patient centric view: (a) acquisition, (b) storage, (c) processing, and (d) presentation. This layered approach corresponds to the general view of health IoT structures through smart health objects acquiring data, personal health records storing the information, intelligent algorithms processing the data, and medical results presenting the data. Each of these layers interfaces within a framework designed to collect data from health IoT devices, route the data to the patient's personal health record (PHR) within the EHR system, and process the data through intelligent algorithms to display actionable results for medical providers. The authors conclude that current health IoT technologies can capture patient data on blood pressure, body temperature, heart rate, respiratory rate, oxygen saturation, level of pain, level of consciousness, and urine output. They note that these measurements mainly focus on heuristics based on predefined thresholds rather than fully incorporating artificial intelligence. The authors suggest a shift from reactive approaches to symptoms and pathologies to more proactive and personalized approaches based on the incorporation of health IoT data into EHRs. The audience most benefiting from this article will be medical professionals and leadership implementing health IoT and those in the data management arena.

Ganzha, M., Paprzycki, M., Pawlowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications, 81*, 111-124. doi:10.1016/j.jnca.2016.08.007

Abstract. The Internet of Things (IoT) idea, explored across the globe, brings about an important issue: how to achieve interoperability among multiple existing (and constantly created) IoT platforms. In this context, in January 2016, the European Commission has funded seven projects that are to deal with various aspects of interoperability in the Internet of Things. Among them, the INTER-IoT project is aiming at the design and implementation of, and experimentation with, an open cross-layer framework and associated methodology to provide voluntary interoperability among heterogeneous IoT platforms. While the project considers interoperability across all layers of the software stack, we are particularly interested in answering the question: how ontologies and semantic data processing can be harnessed to facilitate interoperability across the IoT landscape. Henceforth, we have engaged in a "fact finding mission" to establish what is currently at our disposal when semantic interoperability is concerned. Since the INTER-IoT project is initially driven by two use cases originating from (i) (e/m)Health and (ii) transportation and logistics, these two application domains were used to provide context for our search. The paper summarizes our findings and provides foundation for developing methods and tools for supporting semantic interoperability in the INTER-IoT project (and beyond).

Summary. The authors describe a principal challenge with health IoT is that there are significant varying capabilities of devices on the marketplace and an exploding number of services, culminating in IoT being "among the biggest conceptual and technological challenges of our time" (p. 1). They further note that "every IoT domain and every IoT vendor produces its own IoT platform" (p. 1). To mitigate these interoperability challenges, the authors propose multiple levels of the software stack, allowing for "common description and data representation frameworks, which will characterize things, their capabilities and data they produce, in machine-readable and machine-interpretable forms" (p. 1-2). The authors explore state-of-the-art semantic ontologies to combat challenges such as data collected from different sources, in this case, health IoT devices, which describe the same medical facts about a patient, such as blood pressure. The context and accuracy of measurements can be different in each case of separate health

IoT devices, thus there is a need for interrelation of such data to describe an accurate assessment of the patient's health.

The authors conclude that interoperability is of great importance, but is plagued with the challenge of achieving across IoT silos due to very strong competition between organizations that are developing and promoting proprietary, individual approaches based on closely guarded intellectual property rights. Despite the challenges, frameworks that achieve semantic interoperability, combined with middleware, agent, and service-oriented techniques, should be considered as potential solutions to establish interoperability between heterogenous IoT platforms.

The value of this article is that it describes the many semantic web ontologies currently present on the market and the challenges they present. It further benefits data management teams as a guide to creating a semantic ontology for an organization level or leveraging an already present option.

Peng, C., & Goswami, P. (2019). Meaningful integration of data from heterogeneous health services and home environment based on ontology. *Journal of Sensors, 19*(4), 1-19. doi:10.3390/s19081747

Abstract. The development of electronic health records, wearable devices, health applications and Internet of Things (IoT)-empowered smart homes is promoting various applications. It also makes health self-management much more feasible, which can partially mitigate one of the challenges that the current healthcare system is facing. Effective and convenient self-management of health requires the collaborative use of health data and home environment data from different services, devices, and even open data on the Web. Although health data interoperability standards including HL7 Fast

Healthcare Interoperability Resources (FHIR) and IoT ontology including Semantic Sensor Network (SSN) have been developed and promoted, it is impossible for all the different categories of services to adopt the same standard in the near future. This study presents a method that applies Semantic Web technologies to integrate the health data and home environment data from heterogeneously built services and devices. We propose a Web Ontology Language (OWL)-based integration ontology that models health data from HL7 FHIR standard implemented services, normal Web services and Web of Things (WoT) services and Linked Data together with home environment data from formal ontology-described WoT services. It works on the resource integration layer of the layered integration architecture. An example use case with a prototype implementation shows that the proposed method successfully integrates the health data and home environment data into a resource graph. The integrated data are annotated with semantics and ontological links, which make them machine-understandable and cross-system reusable.

Summary. This article describes a health IoT architecture that models the aggregation and integration of both EHR and health IoT data. Health IoT's health data interoperability standards and IoT ontology have been developed and promoted, but it remains nearly impossible for all services to adopt a similar standard in the near future due to a lack of consensus on a single interoperability standard such as HL7 or Healthcare Interoperability Resources (FHIR). The authors propose the use of a solution by using *Web Ontology Language (OWL)-based integration ontology* through *HL7 Fast Healthcare Interoperability Resources (FHIR)* along with normal web services that incorporate the Web of Things (WoT) to achieve a layered integration architecture.

Combining these elements, the authors further propose *Linked Health Resources (LHR)* ontology as “a consolidated framework that aggregates health and home environment data from different sources and integrates them as a data resource graph” (pp. 2-3); the goal is to employ the output “for upper-level collaborative use” (p. 3). Data integrated through this method is annotated with semantics and ontological links, which allows for machine-understandable reuse across various systems.

The authors propose a model of three core levels: (a) health data service sources (EHR and health IoT devices) funneling data through (b) integration layers such as a data API layer, data aggregation layer, and resource integration layer into which the data is processed, and (c) utility applications that produce virtualizations, analytics, diagnoses, and alerts. Obstacles still exist within this model, such as a lack of standardized data models with legacy health IoT devices as they pre-date recent progress in interoperability standards, making a full realization of the model not yet possible for real-world use.

The value of this article is that it describes a theoretical semantic web ontology utilizing HL7 FHIR, a very common language among EHRs that is currently present on the market, and the challenges associated with this potential solution. The main audience of this study will be those developing information architectures of EHRs, data managers, and IoT integration teams.

Prosperi, M., Min, J., Bian, J., & Modave, F. (2018). Big data hurdles in precision medicine and precision public health. *BMC Medical Informatics and Decision Making*, *18,* 1-15. doi:10.1186/s12911-018-0719-2

Abstract. Nowadays, trendy research in biomedical sciences juxtaposes the term ‘precision’ to medicine and public health with companion words like big data, data science, and deep learning. Technological advancements permit the collection and merging of large heterogeneous datasets from different sources, from genome sequences to social media posts or from electronic health records to wearables. Additionally, complex algorithms supported by high-performance computing allow one to transform these large datasets into knowledge. Despite such progress, many barriers still exist against achieving precision medicine and precision public health interventions for the benefit of the individual and the population.

Main body The present work focuses on analyzing both the technical and societal hurdles related to the development of prediction models of health risks, diagnoses and outcomes from integrated biomedical databases. Methodological challenges that need to be addressed include improving semantics of study designs: medical record data are inherently biased, and even the most advanced deep learning's denoising autoencoders cannot overcome the bias if not handled a priori by design. Societal challenges to face include evaluation of ethically actionable risk factors at the individual and population level; for instance, usage of gender, race, or ethnicity as risk modifiers, not as biological variables, could be replaced by modifiable environmental proxies such as lifestyle and dietary habits, household income, or access to educational resources.

Conclusions Data science for precision medicine and public health warrants an informatics-oriented formalization of the study design and interoperability throughout all levels of the knowledge inference process, from the research semantics, to model development, and ultimately to implementation.

Summary. This article discusses the relationship of Health IoT and Big Data to precision medicine. Precision medicine presents an ability for customized disease treatment and presents a significant paradigm shift from current notions of *number needed to treat* (NNT) target population medical treatment practices. Clinical trials to date have been limited in population and often are cost-prohibitive. The authors argue that “medicine must revolve around data, especially in generating, linking, and learning from a variety of sources” (p. 2). They further propose that a “plethora of markers can be used to predict future health status with high precision” (p. 2) and note that employing these markers can become cost-effective while reducing burdens on the medical system.

The authors propose that the incorporation of health IoT into electronic health records that also account for social, behavioral, environmental, genomics, metabolomics, and transcriptomics attributes and medications can help health care professionals to with early risk prediction, differential diagnosis, and treatment optimizations, all in reduced timeframes. To achieve these outcomes, “multi-domain studies need to extend beyond the ‘omics’ data and consider other domains in a person’s life” (p. 5); with the ubiquitous nature of internet access, smartphone technologies, and health IoT wearable devices, key patient-generated data can be seamlessly collected.

Despite these tremendous potential health improvements, the authors caution that there are many barriers to linking and efficiently exploiting health information across different sites. However, data integrations through EHRs, while requiring enormous efforts and resources, offer the most successful outcomes due to rigorous governance standards and solid infrastructure. When designing system integrations to achieve interoperability, the authors caution that “increasing model complexity can lead to better approximation of functions and enhance prediction performance, but can lead to a decrease in interpretability of the model" (p. 10), indicating an inverse relationship between human interpretability and model complexity.

A model that has successfully achieved interoperability between a health IoT device and EHR is exemplified by the integration of Apple Inc.'s HealthKit into Epic Systems' EHR. Epic's Orchard app enables the collection of wearable technology data and the transmission of the data into the EHR, where the data is stored and can be displayed. Despite these successes, the authors caution that are a number of hurdles remain, such as: (a) prediction models of future health statuses are not yet accurate and (b) the actionability of these models is not yet accounted for; that is, it remains to be seen if the identification of a disease will occur or be mitigated solely through IoT related tracking. The value of this study is that it provides a comprehensive overview of the multiple domains that are functionally possible to be integrated, how might they be integrated, and what hurdles remain. The audience members of this study are healthcare leadership and physicians as well as those working in the EHR technology space.

Category 3: Health IoT Infrastructure Requirements

Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., . . . Rana, O. (2018). The Internet of Things, fog and cloud continuum: Integration and challenges. *Internet of Things,* 3-4, 134-155. doi:10.1016/j.iot.2018.09.005

Abstract. The Internet of Things needs for computing power and storage are expected to remain on the rise in the next decade. Consequently, the amount of data generated by devices at the edge of the network will also grow. While cloud computing has been an established and effective way of acquiring computation and storage as a service to many applications, it may not be suitable to handle the myriad of data from IoT devices and fulfill largely heterogeneous application requirements. Fog computing has been developed to lie between IoT and the cloud, providing a hierarchy of computing power that can collect, aggregate, and process data from/to IoT devices. Combining fog and cloud may reduce data transfers and communication bottlenecks to the cloud and also contribute to reduced latencies, as fog computing resources exist closer to the edge. This paper examines this IoT-Fog-Cloud ecosystem and provides a literature review from different facets of it: how it can be organized, how management is being addressed, and how applications can benefit from it. Lastly, we present challenging issues yet to be addressed in IoT-Fog-Cloud infrastructures.

Summary. This study describes how there is a significant trend in connecting nearly everything to the internet and the accompanying need to review strategies on transferring, storing, and processing unprecedented amounts of data. IoT devices typically generate raw data that may not be useful as a whole, creating an extraordinary challenge of data processing that can lead to knowledge extraction and the delivery of insightful information knowledge. Most IoT devices commonly communicate through a network connection to a centralized Cloud data center, implying that "communication and data transfers traverse multiple hops, which introduces delays and consumes network bandwidth of edge and core networks" (p. 135). With the widespread adoption of Cloud computing combined with the increasing ability of edge devices to run heterogenous applications, there is a significantly higher amount of data being generated, which will require new computing infrastructures and network designs to cope. This situation is exacerbated by the increase in data transfer quantity, volume, and speed that accompanies 5G network support.

The authors discuss *fog computing*, which brings together edge devices and the Cloud to introduce a hierarchy of computing capacity for uses at the edge of the network. The authors' fog computing infrastructure model enables edge devices in the context of health IoT to handle applications within a hierarchy to provide adequate processing capacity and resolve latency challenges through network connections. The proposed fog computing model improves upon resource allocation and optimization, introduces potential of serverless computing, improvements in energy consumption, federation of IoT devices, and better data management based on locality. A high-level hierarchy within the model includes: (a) infrastructure for computing and networking, (b) management of services, energy, device federation, resources, data locality, and orchestration, and (c) applications where IoT is performing a task. The hierarchy is designed to limit the network hops required between the health IoT device and the *fog nodes*, and the higher in the hierarchy the node is, the more processing/storage capacity it has. This distributed approach is meant to process data faster and limit latency. The authors conclude that the use of *fog-Cloud computing* is a promising way of providing full capabilities to support health IoT with low-latency/real-time processing.

The value of this contribution is that it identifies a fog-Cloud computing architecture to allow for the integration, storage, and use of massive amounts of heterogenous health IoT data. Leveraging this model, particularly within the health IoT space, can limit the latency and slow processing of critical patient information. The core audience who will be interested in this technology include technology teams within network operations, data management, and Cloud operations.

Hu, J., Chen, C., Fan, C., & Wang, K. (2017). An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. *Journal of Sensors, 2017*, 1-12. doi:10.1155/2017/3734764

Abstract. Internet of Things (IoT) is the network of physical objects where information and communication technology connect multiple embedded devices to the Internet for collecting and exchanging data. An important advancement is the ability to connect such devices to large resource pools such as cloud. The integration of embedded devices and cloud servers offers wide applicability of IoT to many areas of our life. With the aging population increasing every day, embedded devices with cloud server can provide the elderly with more flexible service without the need to visit hospitals. Despite the advantages of the sensor-cloud model, it still has various security threats. Therefore, the design and integration of security issues, like authentication and data confidentiality for ensuring the elderly's privacy, need to be taken into consideration. In this paper, an intelligent and secure health monitoring scheme using IoT sensor based on cloud computing and cryptography is proposed. The proposed scheme achieves authentication and provides essential security requirements.

Summary. Within this article, the authors discuss the increasing care needs of a rapidly increasing quantity of elderly patients, particularly those with chronic diseases, who require long-term-care (LTC), as well as those who desire to remain independent in their own homes. The authors cite a current lack of medical resources that prevents full treatment of chronic diseases, hospital constraints due to high demand, and the need for continuous monitoring of critical vital signs as key challenges. In conjunction with these challenges, health IoT has seen a rapid increase in capabilities as physiological sensors.

Using health IoT devices based on a Cloud computing platform as a plausible solution, the authors develop a scheme that identifies stages of: a *digital envelope,* a secure electronic data container used to protect a message through encryption and data authentication; *digital container,* metadata coexisting with the file; and a *digital signature* and *timestamp,* authentication and validation.

This methodology is intended to protect elderly patients from cybersecurity threats and enable them to receive available medical services conveniently. The methodology successfully reduced patient travel to hospitals to seek care, resulted in more patient engagement with their own health information, and enabled the fast dispatch of emergency services if needed.

The value of this article is that it provides a technical overview and schema to develop secure and rapid interactions between a healthcare institution and provider with the specific focus of elderly patients, a unique class of patients. The larger value is the provision of a means to leverage health IoT data and devices to reduce the hospital impact of an increasing population of elderly patients, as well as the introduction of a means to facilitate senior living in an independent home setting. The core audience who will be interested in this schema will be teams within network operations, data management, cybersecurity, and Cloud operations.

Mezghani, E., Exposito, E., & Drira, K. (2017). A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence, 1*(3), 224-234. doi:10.1109/TETCI.2017.2699218

Abstract. Due to its abilities to capture real-time data concerning the physical world, the Internet of Things (IoT) phenomenon is fast gaining momentum in different applicative domains. Its benefits are not limited to connecting things, but lean on how the collected data are transformed into insights and interact with domain experts for better decisions. Nonetheless, a set of challenges including the complexity of IoT-based systems and the management of the ensuing big and heterogeneous data and as well as the system scalability need to be addressed for the development of flexible smart IoT-based systems that drive the business decision-making. Consequently, inspired from the human nervous system and cognitive abilities, we have proposed a set of autonomic cognitive design patterns that alleviate the design complexity of smart IoT-based systems, while taking into consideration big data and scalability management. The ultimate goal of these patterns is providing generic and reusable solutions for elaborating flexible smart IoT-based systems able to perceive the collected data and provide decisions. These patterns are articulated within a model-driven methodology that we have proposed to incrementally refine the system functional and nonfunctional requirements. Following the proposed methodology, we have combined and instantiated a set of patterns for developing a flexible cognitive monitoring system to manage patients' health based on heterogeneous wearable devices. We have highlighted the gained flexibility and demonstrated the ability of our system to integrate and process heterogeneous large-scale data streams. Finally, we have evaluated the system performance in terms of response time and scalability management.

Summary. The authors assert that health IoT has benefits beyond connecting "things" and identify how collected data is transformed into insights through interaction with domain experts (medical providers) who can then make better decisions. However, the authors note current challenges with the complexity of health IoT-based systems, the management of heterogenous big data sets, as well as system scalability. The authors assert that solutions to both scalability and heterogeneity within the data are required in order to achieve smart health IoT systems that drive business decision-making and value. The authors note the increasing number of health IoT sensors that monitor and collect ever-increasing quantities of data and state there may be impacts to "execution of components implementing computational intelligence to learn from this data and generate hidden information, due to their heterogeneity and the non-understanding of the meaning of the received data" (p. 224). To mitigate these issues and achieve advancements in scalability and heterogenous data sets, the authors propose an integration of health IoT and autonomic cognitive design patterns to "alleviate the design complexity of smart IoT-based systems, while taking into consideration big data and scalability management" (p. 224). Autonomic computing in this context is defined as "designing self-managed systems that automatically adapt their structure based on context changes" (p. 224). An advantage to leveraging autonomic computing within health IoT, thus referred to as "cognitive IoT," is that it attempts to become a solution for the dynamic evolution of system requirements, variability in new health IoT devices, and challenges posed within managing big data and scalability.

The methodology identifies two initial phases of what is referred to as a *management processes' coordination*: (a) *requirements identification* and (b) *requirements formalization.* Within the requirements identification phase, health IoT engineering teams are encouraged to have detailed discussions with domain experts (medical providers) in order to identify the system functions and identify non-functional requirements. This iterative process is meant to elucidate use cases of health IoT data from the perspective of those administering care and interpreting the data into information. During the phase of requirements formalization, there is a focus on "formalizing and structuring the identified requirements into concrete models describing the system processes' interactions" (p. 227). The central aim of these management phases is to develop solid management processes which can facilitate monitoring, analysis, planning, and execution processes, as well as their combination. The process management stage is also where cognitive, predictive, prescriptive, and autonomic management patterns are established.

Once the knowledge formalization stage is accomplished, the next phases approach *semantic integration, "*where the information about the system and its environment as well as procedural knowledge (know-how) for decision-making are formalized in order to be automatically reused by the management process" (p. 227). This establishes a re-usable basis to be replicated onto other use-cases, creating efficiencies in scaling. A *semantic knowledge mediator* pattern is also developed at the semantic management level that guarantees interoperability and integration for the overall system. Overall, having combined the initial steps of management coordination with semantic integration and mediation, the output becomes a semantic model of *the sensory, the context* and *the procedural knowledge* of health IoT data. This foundation is then paired with the last level of *Big Data & Scalability Management,* where big data challenges such as volume, variety, and velocity are addressed, along with scalability in system performance. Within this level are stream detection patterning, analytic predictive patterning, as well as multi-tenant management process patterning, all of which are digitally cognitive and autonomic; thus, self-learning and self-correcting. This levels-based structure thus addresses how and why the health IoT data is used, what semantic structure it will undertake, and finally what infrastructure is needed to address the data at a scalable level. What it is meant to achieve is a flexible and evolving system to accommodate heterogenous devices and intake heterogeneous data such that computational and engineering frameworks are built-into the overall system, rather than by constant human-based interaction.

The value of this article is that it demonstrates a methodology of advanced computer and machine learning that adjusts and thus adapts to an evolving landscape of heterogenous health IoT. Once developed, the core architecture is able to onboard additional data and devices, without needing to be fully re-architected based on new structures. The core audience for this article will be teams within network operations, data management, cybersecurity, and Cloud operations.

Rathore, M., Ahmad, A., Paul, A., Wan, J., & Zhang, D. (2016). Real-time medical emergency response system: Exploiting IoT and Big Data for public health. *Journal of Medical Systems, 40*(12), doi:10.1007/s10916-016-0647-6

Abstract. Healthy people are important for any nation's development. Use of the Internet of Things (IoT)-based body area networks (BANs) is increasing for continuous monitoring and medical healthcare in order to perform real-time actions in case of emergencies. However, in the case of monitoring the health of all citizens or people in a country, the millions of sensors attached to human bodies generate massive volume of heterogeneous data, called "Big Data." Processing Big Data and performing real-time actions in critical situations is a challenging task. Therefore, in order to address such issues, we propose a Real-time Medical Emergency Response System that involves IoT-based medical sensors deployed on the human body. Moreover, the proposed system consists of the data analysis building, called "Intelligent Building," depicted by the proposed layered architecture and implementation model, and it is responsible for analysis and decision-making. The data collected from millions of body-attached sensors is forwarded to Intelligent Building for processing and for performing necessary actions using various units such as collection, Hadoop Processing (HPU), and analysis and decision. The feasibility and efficiency of the proposed system are evaluated by implementing the system on Hadoop using an UBUNTU 14.04 LTS coreTMi5 machine. Various medical sensory datasets and real-time network traffic are considered for evaluating the efficiency of the system. The results show that the proposed system has the capability of efficiently processing WBAN sensory data from millions of users in order to perform real-time responses in case of emergencies.

Summary. Within this article, the authors assert that “the main requirement of any IoT-based healthcare system is that uses should benefit in real-time anytime and everywhere, which requires continuous network connectivity, data generation, and results in the production of a substantial volume of data” (p. 283). This forms the basis for the authors’ proposal of the creation of a system architecture that processes, analyzes, and produces actionable medical data for all patients in a healthcare system in real-time, allowing for emergency response to critical events. In order to continuously monitor patient health data such as physical activities, medical measurements, and disease monitoring efficiently in high-speed, the authors discuss a proposed *real-time medical emergency response system,* a layered system architecture and smart solution prototype of a wireless sensor network (WSN). Their prototype consisted of five key layers: (1) data collection, (2) communication, (3) processing, (4) management, and (5) service. The data collection layer is meant to provide the necessary functionality to the entire system, consisting of data sensing, acquisition, buffering, and processing. The communication layer introduces the use of Apache Spark and provides functionalities for end-to-end connectivity to various devices involved with a network concept called *wireless body area network (WBAN)*. The processing layer maintains the use of Apache Spark and is a core unit of intelligence building that receives aggregated data in the form of sequenced files from the communication layer, processes the data and further performs necessary pre-determined calculations and statistical measures based on the nature of the data. The management layer enables intelligent management of various types of processes such that medical experts can analyze the results generated. Finally, the service layer routes the actionable outcomes to necessary parties, such as hospitals, emergency services, and remote physician support to ensure that the data obtained from wearable devices is successfully transmitted to necessary hospital EHRs and emergency services to expediently address the medical event.

The value of this article is to present an architecture for medical emergency response that enables necessary services to be engaged, including care providers, hospitals, and emergency services. The health IoT devices described can be leveraged to ensure expedient response and improved patient outcomes. The prototype is particularly useful for aggregating data in an automated and rapid manner during critical medical events, providing a point of leverage for hospital emergency departments. The audience members of this article are hospital leadership, emergency care providers, emergency services, and

health technologists within network operations, data management, cybersecurity, and Cloud operations.

Sharma, S., & Wang, X. (2017). Live data analytics with collaborative edge and cloud processing in wireless IoT networks. IEEE*, 5*, 2017th ser., 4621-4635. doi:10.1109/ACCESS.2017.2682640

Abstract. Recently, big data analytics has received important attention in a variety of application domains including business, finance, space science, healthcare, telecommunication and Internet of Things (IoT). Among these areas, IoT is considered as an important platform in bringing people, processes, data and things/objects together in order to enhance the quality of our everyday lives. However, the key challenges are how to effectively extract useful features from the massive amount of heterogeneous data generated by resource-constrained IoT devices in order to provide real-time information and feedback to the end- users, and how to utilize this data-aware intelligence in enhancing the performance of wireless IoT networks. Although there are parallel advances in cloud computing and edge computing for addressing some issues in data analytics, they have their own benefits and limitations. The convergence of these two computing paradigms, i.e., massive virtually shared pool of computing and storage resources from the cloud and real- time data processing by edge computing, could effectively enable live data analytics in wireless IoT networks. In this regard, we propose a novel framework for coordinated processing between edge and cloud computing/processing by integrating advantages from both the platforms. The proposed framework can exploit the network-wide knowledge and historical information available at the cloud center to guide edge computing units towards satisfying various performance

requirements of heterogeneous wireless IoT networks. Starting with the main features, key enablers and the challenges of big data analytics, we provide various synergies and distinctions between cloud and edge processing. More importantly, we identify and describe the potential key enablers for the proposed edge-cloud collaborative framework, the associated key challenges and some interesting future research directions.

Summary. The authors of this article describe the main challenge of IoT as how to handle the real-time processing of huge amounts of data/information, identified as Big Data, that is generated from heterogenous wireless IoT environments. Big Data in this context refers to “larger, heterogenous and complex (semi-structured and unstructured) data-sets, which cannot be handled by the conventional data processing and storage tools/applications such as Relational Database Management Systems (RDBMS)” (p. 4623). This core issue presents downstream challenges as well, such as computational capability, processing ability, facilitation of real-time delivery at the edge-side, and storage/caching constraints. The overall complexity of Big Data generated from IoT is not dependent on the size of the data, but instead depends on the computational cost to process the data. “Besides, this massive amount of data needs to be transferred from the edge nodes to the cloud, leading to the need of enormous communication bandwidth which is precious and expensive natural resource” (p. 4621).

Specific to IoT data, primary concerns include the question of how to effectively extract useful features from the massive amount of heterogeneous data and provide real-time information and feedback to end-users, along with how to utilize data-aware intelligence in enhancing the performance of wireless IoT networks. Combining the challenges posed by Big Data and IoT, the authors note four other specific features that present challenges:

(1) distributed and heterogenous data structure, (2) real-time requirements, (3) weak data semantics, and (4) data inaccuracy. These challenges present real impacts to the use of Big Data and IoT in the form of creating burdens of handling the data over networks that may result in the wrong or incomplete data sets being transferred; in the context of health IoT, this poses serious the problem of presenting false conclusions.

While these issues may be resolved in part by probability-based confidence levels to offer the safe operation of devices, the authors argue that this is not enough to fully resolve the issues presented. The authors propose a solution of mitigating these challenges by combining the benefits of Cloud and fog/edge computing architectures. The authors identify the key benefits of a Cloud computing platform in wireless IoT networks as "massive storage, very high computational efficiency, wide-area coverage" (p. 4626) and the key advantages of edge computing as "real-time data handling, edge resource pooling, user-centric process, the support for high mobility, and high Quality of Service (QoS)" (p. 4626).

IoT devices, within this proposed schema, will connect through gateways equipped with cache memory and capable of performing edge-caching to deliver popular content local to the end-user. These edge gateways can include any device capable of computing, storing, and network communication, such as a router, switch, or similar device within a home or office setting. The processing of much more demanding tasks can be offloaded and stored on Cloud systems. This solution presents a pivotal balance between centralized Cloud computing that is more suited towards storage and computational tasks and distributed edge devices that are advantageous in handling delay-sensitive tasks.

This paper presents key fundamentals in architecting a strategic network deployment and utilization of IoT devices. It presents the possibilities of utilizing network connected equipment at the edge level as well as Cloud to optimize network traffic and processing distribution. The fundamentals the authors present are very useful for network deployment teams, data management teams, and those in Cloud computing teams.

Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Fratu, O. (2015). Big Data, Internet of Things and Cloud convergence - an architecture for secure E-Health applications. *Journal of Medical Systems, 39*(11), 1-8. doi:10.1007/s10916-015-0327-y

Abstract. Big data storage and processing are considered as one of the main applications for cloud computing systems. Furthermore, the development of the Internet of Things (IoT) paradigm has advanced the research on Machine to Machine (M2M) communications and enabled novel tele-monitoring architectures for E-Health applications. However, there is a need for converging current decentralized cloud systems, general software for processing big data and IoT systems. The purpose of this paper is to analyze existing components and methods of securely integrating big data processing with cloud M2M systems based on Remote Telemetry Units (RTUs) and to propose a converged E-Health architecture built on Exalead CloudView, a search based application. Finally, we discuss the main findings of the proposed implementation and future directions.

Summary. This article addresses the convergence of IoT, Big Data, and Cloud computing and their combined abilities in developing the next generation of eHealth systems. The convergence of Big Data produced by large volumes of heterogenous IoT medical data can be combined with a Cloud computing infrastructure to allow for search-based applications to provide remote diagnostics, better understanding of diseases and the development of innovative solutions for therapeutics. The authors note that heterogenous and geographically distributed sensors require immense distributed storage capacities on Cloud computing platforms that are capable of intaking and processing thousands of simultaneous sensor streams (IoT devices). The data types and formats consist of: (a) structured, (b) unstructured, (c) semi-structured, and (d) multi-structured, all of which originate from a diverse assortment of sources within the greater umbrella of IoT, such as sensors, devices, social networks, web content, and mobile phones, among others.

The authors propose an architecture of an IoT device interfacing with a remote telemetry unit (RTU) and through a gateway through the internet to a Cloud infrastructure designed to process Big Data. Within the Cloud infrastructure are a *Presentation Service (PS),* a software package focused on data presentation, and an *Application Service* focused on special tasks at the command of the end-user. By processing all data and extracting all relevant metadata within the Cloud, the Cloud middleware layer enables the heterogenous devices to act as data sources and integrate data from other healthcare platforms such as an EHR. The local cloud enables interconnection with various different devices through a standardized network protocol and interfaces, allowing more seamless communication to additional downstream destinations (EHRs). The authors' principle conclusions are: (a) that storage and data processing must remain as close as possible in space and time to where the data is generated (edge devices/IoT devices), (b) security and reliability are supported by a tight integration of high-level services at the IoT and gateway levels, (c) energy efficiency and scalability of the systems are achieved through the distribution of inferred content rather than raw data, and (d) cross-domain applications using real-time data from multiple sources can be seamlessly implemented.

The value of this study is that it provides a model architecture that addresses the convergence of IoT, Big Data, and Cloud computing and a methodology that synthesizes data in a manner that allows integration into EHRs.

Strielkina, A., Illiashenkoi, O., Zhydenko, M., & Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. *IEEE Intelligent Systems,* 67-73. doi:10.1109/DESSERT.2018.8409101

Abstract. The paper deals with exponentially growing technology - Internet of Things (IoT) in the field of healthcare. It is spoken about the networked healthcare and medical architecture. The attention is given to the analysis of the international regulations on medical and healthcare cybersecurity. For building a trustworthy healthcare IoT solution, a developed normative hierarchical model of the international cybersecurity standards is provided. For cybersecurity assessment of such systems the case-oriented technique, which includes Advanced Security Assurance Case (ASAC) and an example on a wireless insulin pump of its application are provided.

Summary. The authors of this article describe how hardware and software solutions within healthcare have grown in significant complexity and observe that medical decisions regarding patient care have become entangled in multiple competing goals from various vendors within the marketplace. To mitigate these challenges, the authors note that many healthcare organizations have shifted priorities to focus more on individual patient-level objectives. One of the corresponding technologies of this shift in priority is IoT. However, IoT, among other network-connected medical devices, raises four main concerns: (1) random failures, (2) privacy, (3) deliberate disruption, and (4) malware disruption. The authors thus assert the need to develop an approach "that takes into account all aspects of development processes, regulatory and standardization, different methodologies for security, risk, and hazard assessment" (p. 67) such that health IoT environments remain secure at all levels.

Health IoT sensor security is a highly discussed topic within healthcare and past literature. There are many discussions of specifications and design spaces that include interoperability, security of network infrastructures, and the deployment model of the wireless sensors themselves. However, the authors assert that trust verifications must be applied to a layered architecture for the IoT infrastructure, rather than at a specific interface. In other words, there is a need to evaluate the entire infrastructure from end-to-end and develop "a unified methodology [that] allows obtaining the verifiable, traceable, justifiable results" for data creators and users. This architecture is designed in part to decrease the inherent vulnerabilities and threats posed. The authors identify a layered structure consisting of: (a) sensing layer (IoT devices), (b) network layer, (c) service layer, (d) information security management, (e) risk assessment, and (f) PHI data security, including HIPAA Privacy and Security Rules. The authors assert that looking at cybersecurity through this lens will help system architects identify the methods, processes, and cybersecurity tools necessary for complete security. In addition, by looking at the end-to-end system rather than at individual parts, cybersecurity teams can create a holistic solution that mitigates potential gaps that present vulnerabilities.

The value of this article is that it provides an assessment methodology for creating a holistic cybersecurity strategy for IoT infrastructure. The authors also present the notion that the infrastructure must be thought of as a layered structure, rather than an individual and isolated structure. The main audience of this article will be cybersecurity professionals working within the IoT field.

Conclusion

Health IoT presents many opportunities for cost savings for patients and healthcare organizations as well as improvements in the quality of life for patients, including management of chronic diseases, health monitoring, and prevention of disease complications (Rodrigues et al., 2017). By year-end 2019, health IoT is projected to be adopted by up to 87% of U.S. healthcare organizations; adoption will be driven primarily by cost reductions and improved patient care motivations (Sheth et al., 2018). A core challenge for healthcare organizations will be the integration of a plethora of heterogenous health IoT devices along with the subsequent enormous quantities of data they create into their existing EHRs (Dimitrov, 2016).

This annotated bibliography summarizes literature that addresses the best practices and technologies for healthcare institutions to successfully integrate heterogenous patient health IoT devices and data within their EHRs. Sources have been selected based on the healthcare applicability of IoT, the integration of IoT with EHRs, and the infrastructure requirements to achieve integration.

The Evolving Landscape of Health IoT

In recent years, there has been a convergence of IoT, Big Data, and Cloud computing, leading to the development of the next generation of healthcare and related technologies (Suciu et al., 2015). It is becoming more feasible, necessary, and even cost-effective to perform medical diagnoses without visiting a hospital or ambulatory care setting (Hu et al., 2017). A paradigm shift is also occurring within healthcare that encourages the transition from a primarily reactionary system to a more preventative and proactive care model (Sheth et al., 2018). Prosperi et al. (2018) note that “medicine must revolve around data, especially in generating, linking, and learning from a variety of sources” (p. 2) and that data from health IoT can cost-effectively help predict future health status with high precision. A consistent theme within the literature is that health IoT presents unique abilities and capabilities to improve care and achieve a more proactive model (Alamri, 2018; Dimitrov, 2016; Peng & Goswami, 2019, Prosperi et al., 2018). Mainly, health IoT expands the potential for precision medicine to customize disease prevention, monitoring of health, and treatment at the individual patient level (Prosperi et al., 2018).

An additional theme within the literature is that health IoT also presents several challenges (Dimitrov, 2016; Ganzha et al., 2017; Laplante & Laplante, 2016; Peng & Goswami, 2019; Sharma & Wang, 2017). Examples of such challenges are the real-time processing of enormous amounts of data and information, commonly referred to as *Big Data*, that are generated from heterogeneous wireless IoT environment (Sharma & Wang, 2017; Sheth et al., 2018); security risks of centralizing large amounts of sensitive patient data (Baker, Xiang, & Atkinson, 2017); the possible need to recalibrate sensors (Baker et al., 2017); network connectivity issues (Baker et al., 2017); as well as making the data meaningful, interpretable, and actionable (Sheth et al., 2018). Ganzha, Paprzycki, Pawlowski, Szmeja, and Wasielewska (2017) suggest the significant heterogeneity of the varying capabilities of health IoT devices on the marketplace and number of corresponding services culminates in health IoT being "among the biggest conceptual and technological challenges of our time" (p. 1).

Dimitrov (2016) summarizes the core challenge of health IoT as related to *communication*: between the devices themselves; their heterogeneity in manufacturing, models, and the protocols used to communicate to host servers using proprietary computer languages; and the creation of *data islands* based on vendor hoarding of data from their IoT products' proprietary sensors. Interoperability presents a challenge and goal among IoT devices; health IoT devices are seen to have a need for shared data and the ability to communicate across shared ontologies to allow EHR integration, but achieving interoperability is plagued by data silos, closely guarded proprietary computer languages, and intellectual property rights of vendors (Ganzha et al., 2017). Despite many potential benefits and successes, health IoT currently does not provide prediction models for future health statuses that are completely accurate, and health IoT data is not yet able to provide early identification of disease along with mitigation of the disease (Prosperi et al., 2018).

This annotated bibliography seeks to identify the challenges and currently proposed mitigations in integrating health IoT into EHRs.

Healthcare Applicability of IoT

Sheth et al. (2018) identify a vision for *augmented personalized healthcare* where continuous monitoring, engagement, and health management based upon health IoT are able to aid in the prevention, intervention, mitigation, or elimination of disease. This vision extends itself to many areas of health IoT applicability (Sheth et al., 2018). A key callout is within the continuous monitoring of chronic diseases and patient well-being through the tracking of sleep, food and nutrition intake, activity and fitness, vital signs, and other physiological statuses (Dimitrov, 2018; Sheth et al., 2018). Specifically, health IoT can provide data from electrocardiography on heart rate, electroencephalography on brain activity, and electromyography on muscle activities (Rodrigues et al., 2017). Health IoT can also provide data on other body vital signs such as pulse, oxygen in blood (SPO2), airflow, body temperature, blood glucose, galvanic skin response, blood pressure, and patient position (Rodrigues et al., 2017). Utilizing the data, health IoT has been shown to provide patient benefits by: (a) measuring and transmitting blood pressure during cardiac rehabilitation and pregnancy, (b) measuring and transmitting knee flexion range of motion post total knee arthroplasty, (c) monitoring Parkinson disease, (d) detecting bipolar disorder episodes, (e) automatically detecting chronic wounds based on color and size features, (f) monitoring skin for early detection of melanoma, (g) providing medical check-up reminders, and (h) detecting falls and episodes of Alzheimer's-related activities for elderly patients (Rodrigues et al., 2017).

The health IoT devices that gather this data can go beyond health indicators to devices that also auto-administer therapies and treatments based upon the medical need (Dimitrov, 2016). Through participatory and personalized treatments of diseases, health IoT devices can administer therapy, such as an automatic insulin pen injection in conjunction with a glucose monitor (Dimitrov, 2016). Health IoT also goes beyond merely connecting devices to facilitating the collection of data that is transformed into key health insights based upon analysis from technological sources such as artificial intelligence and machine learning, as well as physicians who are domain experts within the medical data that is gathered (Mezghami et al., 2017). Medical specialties and departments also benefit from health IoT (source). Hu et al. (2017) identify the usage of health IoT to facilitate geriatric patients in remaining active and independent within their own home settings for as long as possible, doing so through active monitoring as well as delivery of emergency procedures during a detected medical emergency.

Da Costa, Pasluosta, Eskofier, Da Silva, and Da Rosa Righi (2018) identify an additional application of health IoT through the automation of data collection within emergency departments to improve efficiency, allowing the optimization of key medical personnel and resources while minimalizing patient health deterioration. Dimitrov (2016) also shares the ability for health IoT to reduce readmission rates among patients by using predictive artificial intelligence algorithms to identify those with higher risk from existing patient information from the EHR. The consistent finding from the evidence provided is that health IoT presents many applicable and beneficial capabilities within the healthcare space.

Health IoT Infrastructure Requirements

Heterogenous health IoT devices produce large volumes of medical data that aggregate as Big Data. The convergence of IoT, Big Data, and middleware software running on Cloud and Edge computing infrastructures allows for search-based applications to enable remote diagnostics, better understanding of diseases and the development of innovative solutions for therapeutics (Bittencourt, Immich, Sakellariou, Fonseca, Madeira, Curado, & Rana, 2018; Suciu et al., 2015). A health IoT environment will involve multiple components and levels of infrastructure to become successful (Bittencourt et al., 2018).

Advancements in Cloud computing have provided ubiquitous and on-demand access to virtually-shared pools of configurable computing and storage resources (Sharma & Wang, 2017). Cloud computing has become established as an effective way to acquire large amounts of computational power and storage and is excellent in handling the enormous data generated by a health IoT environment (Bittencourt et al., 2018; Sharma & Wang, 2017). Health IoT devices must transfer the data collected through sensors over an internet-connected network and, in the process, will traverse multiple network hops, introducing delays as well as consumption of valuable network bandwidth (Bittencourt, et al., 2018). To mitigate these issues, Edge computing has been introduced, as it resolves many of the disadvantages posed by Cloud-only environments (Sharma & Wang, 2017). Edge computing occurs closer to the end user and supports applications and services that demand low-latency, location-awareness, high-mobility, and high *Quality of Service (QoS)* (Sharma & Wang, 2017). Edge computing thus can be coalesced to lie in between health IoT devices and Cloud computing, creating a hierarchy that combines data collection, aggregation, processing, storage, and computational power and also reduces network bandwidth and latency concerns (Bittencourt et al., 2018).

A complete infrastructure overview of health IoT can be compiled from descriptions from multiple authors (Baker, Xiang, & Atkinson, 2017; Sharma & Wang, 2017; Suciu et al., 2015). Baker, Xiang, and Atkinson (2017) share that health IoT devices collect data through sensors and transfer the data through short-range communication protocols such as Bluetooth to Edge devices such as smartphones. The data is processed in real-time through the application and/or service running on the Edge device to provide actionable information to the user (Suciu et al., 2015). Data and information are then uploaded through a network connection to a Cloud computing environment, where further processing and storage occurs (Sharma & Wang, 2017). Cloud servers then interface with an EHR, providing specific information as needed by medical professionals (Sharma & Wang, 2017).

Rathore, Ahmad, Paul, Wan, and Zhang (2016) assert that “the main requirement of any IoT-based healthcare system is that users should benefit in real-time anytime and everywhere, which requires continuous network connectivity, data generation, and results in the production of a substantial volume of data” (p. 283). This assertion is commonly shared among the research findings (Baker et. al. 2017; Dimitrov, 2016; Haghi et al., 2017; Suciu et al., 2015) and is an indication of the need for novel and multi-faceted approaches to health IoT integration within EHRs. Integration of health IoT within EHRs is not static and limited to the domains of Big Data and infrastructure such as Cloud or Edge computing; rather it also extends to additional technologies, such as network management, data analytics, software development, cybersecurity, and other information science domains (Baker et. al. 2017; da Costa et al., 2018, Mezghami et al., 2017; Sharma & Wang, 2017; Strielkina et al., 2018).

One key technology for health IoT is semantic web ontologies (Alamri, 2018; Ganzha et al., 2017; Mezghami et al., 2017; Peng & Goswami, 2018; Reda et al., 2018; Prosperi et. al, 2018). The use of semantic web ontologies is a frequently discussed topic within the research as it pertains to health IoT (Alamri, 2018; Costa et al., 2018; Ganzha et al., 2017; Mezghani et al., 2017; Peng & Goswami, 2019; Prosperi et al., 2018; Reda et al., 2018). Semantic web ontologies are ways of defining a common vocabulary and classifying objects in relation to one another within a domain (Noy & McGuinnes, n.d.). Within an ontology, properties and relationships of objects are applied, creating rules that can define classes, roles, facets, and instances that create a knowledge base (Noy & McGuinnes, n.d.). Mezghami et al. (2017) propose that the use of semantic web ontologies can apply to health IoT integration within EHRs and become a mediation towards large volumes of data. The semantic model of *the sensory, the context*, and *procedural knowledge* form a foundation for achieving the challenges of Big Data, namely volume, variety, and velocity (Mezghami et al., 2017). Using common definitions and rules that are shared among health IoT and EHRs, new capabilities are created such as detection patterning, analytic predictive patterning, as well as multi-tenant management process patterning (Mezghami et al., 2017).

Semantic web ontology structures also create a methodology to moderate the heterogeneity of health IoT devices on the marketplace (Mezghami et al., 2017) and a mitigation for interoperability challenges (Ganzha et al., 2017). Utilizing semantic web ontology structures, a common description and data representation framework is established that allows for health IoT data to become machine-readable and interpretable (Ganzha et al., 2017). This approach becomes a pivotal foundation for introducing cognitive systems, artificial intelligence, and machine learning capacities into the health IoT environment (Mezghami et al., 2017) as well as integration into EHRs (Peng & Goswami, 2019).

A semantic web ontology provides the ability for cognitive system monitoring to manage patient health based on data collected from heterogenous health IoT sources (Mezghami et al., 2017). As defined by Sommer (2017), cognitive computing is “systems that learn at scale, reason with purpose and interact with humans naturally” (p. 1) as a mixture of computer and cognitive science. This builds upon artificial intelligence, when machines work intelligently to make decisions to maximize the chances of success, as well as machine learning, a specific type of artificial intelligence where computers have the ability to continually learn without being pre-programmed, allowing algorithms to create foresights and learnings based upon the data (Sommer, 2017). Additional artificial intelligence capacities such as autonomic computing environments allow for self-configuring, self-healing, self-optimizing, and self-protecting by sensing and responding to situations that occur, shifting the burden of managing a computer environment from human administrators to technology (IBM, n.d.). Mezghami et al. (2017) argue that combining a cognitive computing system with autonomic computing that integrates with health IoT systems will “ensure the smart management through enabling the cooperation and interaction between IoT and human” and “lead to unprecedented opportunities for the development of smart IoT-based systems” (p. 225).

Finally, there is a vital need to protect and secure patient health IoT data (Laplante & Laplante, 2016; Strielkina et al., 2018). Strielkina et al. (2018) suggest a layered trust verification platform at every level of the architecture to address the four main concerns: (a) random failures, (b) privacy, (c) deliberate disruption, and (d) malware disruption. Achieving a high level of cybersecurity within a heterogenous health IoT environment as it integrates with EHRs will be a core and evolving challenge for healthcare firms, as they try to increase trust among patients and quell feelings of lost privacy (Laplante & Laplante, 2016).

IoT Integration with EHR

Use of health IoT data within an electronic health record is a long-term goal for many healthcare organizations and will require new innovations and practices to achieve fuller interoperability (Alamri, 2018). As noted by Alamri (2018), part of the challenge resides within the EHR architecture itself, as electronic health records are commonly not designed to integrate health IoT data completely independently, but are meant to integrate with external platforms that facilitate the necessary data interoperability, integration, information search and retrieval, and automatic inference (Alamri, 2018).

Health IoT data alone is insufficient and inadequate to fully understand a patient's total health; it is meant to enhance the understanding of a patient's health in combination with clinical records, behavioral information, and social and environmental information (Sheth et al., 2018). As EHRs house much of the social, behavioral, environmental, genomic, and historical health information of patients, the incorporation of health IoT can add tremendous value to a more complete and real-time health outlook for patients (Prosperi et al., 2018)

Peng and Goswami (2019) identify promising standards related to health IoT, including HL7 Fast Healthcare Interoperability Resources (FHIR), which deals with data interoperability, and IoT standard ontologies such as Semantic Sensor Network (SSN), but note that it remains difficult to impossible to universally adopt full standardization across all heterogeneously created IoT data (p. 1). As direct routing of health IoT is not ideal and in many ways not feasible, alternative platforms built upon the aforementioned infrastructure have been introduced (Prosperi et al., 2018). Examples of such opportunities on the marketplace are Fitbit's platform of activity tracking as well as Apple's Healthkit and ResearchKit (Dimitrov, 2016). Both of these vendor platforms have enabled researchers to access vast stores of health IoT data, where the data can be used to test hypotheses on nutrition, fitness, disease progression, and treatment success (Dimitrov, 2016). Furthermore, partnerships are developing between health IoT middleware vendors and EHR firms (Prosperi et al., 2018). A significant example is exemplified by the integration of Apple Inc.'s HealthKit into Epic Systems' EHR; Epic's Orchard module enables the collection of wearable technology data and the transmission of the data into the EHR, where the data is stored and can be displayed through an interface with Apple's HealthKit product. Key strategic partnerships between EHR vendors and firms that provide middleware that aggregates data from heterogenous IoT devices through Cloud and Edge computing architectures will be central to both the integration capabilities and potentials of health IoT (Dimitrov, 2016; Prosperi et al., 2018).

Going forward, health IoT integration within EHR presents significant opportunities for cost reductions, efficiency gains, and improved patient care (Dimitrov, 2016). To achieve this goal, healthcare institutions will need to incorporate technology platforms that incorporate multi-faceted approaches, novel techniques, as well as partnerships between health IoT vendors and EHR vendors (Baker et al., 2017; Dimitrov, 2016; Mezghami et al., 2017; Sheth et al., 2018).

References

Alamri, A. (2018). Ontology middleware for integration of IoT healthcare information systems in EHR systems. *Computers, 7*(4), 1-15. doi:10.3390/computers7040051

Anton, J., & Caldararo, K. (2018, March). *Millennials: The unforeseen generation that will lead healthcare transformation.* Retrieved April 30, 2019, from https://www.aha.org/sites/default/files/2018-03/180321-workforce-webinar.pdf

Artiga, S., & Hinton, E. (2018, May 10). *Beyond health care: The role of social determinants in promoting health and health equity.* Retrieved May 23, 2019, from https://www.kff.org/disparities-policy/issue-brief/beyond-health-care-the-role-of-social-determinants-in-promoting-health-and-health-equity/

Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., . . . Rana, O. (2018). The Internet of Things, Fog and Cloud continuum: Integration and challenges. *Internet of Things, 3-4*, 134-155. doi:10.1016/j.iot.2018.09.005

Bresnick, J. (2016, March 30). *Can healthcare's Internet of Things move from froth to function?* Retrieved May 15, 2019, from https://healthitanalytics.com/features/can-healthcares-internet-of-things-move-from-froth-to-function

Center for Public Issues Education. (n.d.). *Evaluating information sources.* University of Florida. Retrieved from http://www.piecenter.com/wp-content/uploads/2014/08/evaluateinfo.pdf

Christensen, C., Waldeck, A., & Fogg, R. (2017, November 6). The innovation health care really needs: Help people manage their own health. *Harvard Business Review.* Retrieved from https://hbr.org/2017/10/the-innovation-health-care-really-needs-help-people-manage-their-own-health

Dimitrov, D. (2016). Medical Internet of Things and Big Data in healthcare. *Healthcare Informatics Research, 22*(3), 156-163. http://dx.doi.org/10.4258/hir.2016.22.3.156

Haghi, M., Thurow, K., Habil, I., Stoll, R., & Habil, M. (2017). Wearable devices in Medical Internet of Things: Scientific research and commercially available devices. *Healthcare Informatics Research, 23*(1), 4-15. doi:10.4258/hir.2017.23.1.4

Hu, J., Chen, C., Fan, C., & Wang, K. (2017). An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. *Journal of Sensors, 2017*, 1-12. doi:10.1155/2017/3734764

IBM. (n.d.). *Autonomic computing overview.* Retrieved May 30, 2019, from https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.dbobj.doc/doc/r0051462.html

Iqbal, U., Dagan, A., Syed-Abdul, S., Celi, L., Malwade, S., Min-Huei, H., & Li, Y. (2018). A hackathon promoting Taiwanese health-IoT innovation. *Computer Methods and Programs in Biomedicine, 163*, 29-32. doi:10.1016/j.cmpb.2018.05.020

Karaagac, A., Suanet, P., Joseph, W., Moeman, I., & Hoebeke, J. (2018). Light-weight integration and interoperation of localization systems in IoT. *Journal of Sensors, 18*(7), 1-22. doi:10.3390/s18072142

Kindig, D., & Stoddart, G. (2016). *Understanding population health.* Retrieved May 24, 2019, from http://www.hasc.org/policy-or-politics/understanding-population-health

Laplante, P., & Laplante, N. (2016). The Internet of Things in healthcare: Potential applications and challenges. *IT Professional, 18*(3), 2-4. doi:10.1109/MITP.2016.42

Mezghani, E., Exposito, E., & Drira, K. (2017). A model-driven methodology for the design of autonomic and cognitive IoT-based systems: application to healthcare. *IEEE*

Transactions on Emerging Topics in Computational Intelligence, 1(3), 224-234. doi:10.1109/TETCI.2017.2699218

Michigan Technological University. (2019). *What is medical informatics?* Retrieved May 30, 2019, from https://www.mtu.edu/medical-informatics/what-is/

Noy, N., & McGuinness, D. (n.d.). *Ontology development 101: A guide to creating your first ontology*. Retrieved from https://guides.library.ucla.edu/ld.php?content_id=16693276

Office of the National Coordinator for Health Information Technology. (n.d.). *What is an electronic health record (EHR)?* Retrieved May 16, 2019, from https://www.healthit.gov/faq/what-electronic-health-record-ehr

Peng, C., & Goswami, P. (2019). Meaningful integration of data from heterogeneous health services and home environment based on ontology. *Journal of Sensors, 19*(4), 1-19. doi:10.3390/s19081747

Pham, T., Tran, T., Phung, D., & Venkatesh, S. (2017). Predicting healthcare trajectories from medical records: A deep learning approach. *Journal of Biomedical Informatics, 218*. doi:10.1016/j.jbi.2017.04.001

Prosperi, M., Min, J., Bian, J., & Modave, F. (2018). Big data hurdles in precision medicine and precision public health. *BMC Medical Informatics and Decision Making, 18*, 1-15. doi:10.1186/s12911-018-0719-2

Rathore, M., Ahmad, A., Paul, A., Wan, J., & Zhang, D. (2016). Real-time medical emergency response system: exploiting IoT and Big Data for public health. *Journal of Medical Systems, 40*(12), 283. PMID: 27796839 Version:1

Reda, R., Piccinini, F., & Carbonaro, A. (2018). Towards consistent data representation in the IoT healthcare landscape. In *Proceedings of the 2018 International Digital Health Conference* (pp 5-10). doi:10.1145/3194658.3194668

Rodrigues, J., Segundo, D., Junqueira, H., Sabino, M., Prince, R., Al-Muhtadi, J., & Albuquerque, V. (2017). Enabling technologies for the Internet of Health Things. *IEEE Access,* 6, 13129-13141. doi:10.1109/ACCESS.2017.2789329

Schroeder, S. (2007). We can do better — Improving the health of the American people. *The New England Journal of Medicine, 357*(12), 1221-1228.

Sharma, S., & Wang, X. (2017). Live data analytics with collaborative edge and cloud processing in wireless IoT networks. *IEEE Access, 5,* 4621-4635. doi:10.1109/ACCESS.2017.2682640

Sheth, A., Jaimini, U., & Hong, Y. (2018). How will the Internet of Things enable augmented personalized health? *IEEE Intelligent Systems, 33*(1), 89-97. doi:10.1109/MIS.2018.012001556

Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Fratu, O. (2015). Big Data, Internet of Things and Cloud convergence - An architecture for secure E-Health applications. *Journal of Medical Systems, 39*(11), 1-8. doi:10.1007/s10916-015-0327-y

Strielkina, A., Illiashenkoi, O., Zhydenko, M., & Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. *IEEE Intelligent Systems,* 67-73. doi:10.1109/DESSERT.2018.8409101

University of Illinois at Chicago. (n.d.). *4 ways health informatics improves patient care.* Retrieved May 30, 2019, from https://healthinformatics.uic.edu/blog/4-ways-health-informatics-improves-patient-care/