Communications of the Association for Information Systems

Volume 46 Article 21

4-2020

The Internet of Things: Multi-faceted Research Perspectives

J. P. Shim
Georgia State University, jpshim@gsu.edu

Ramesh Sharda
Oklahoma State University

Aaron M. French
University of New Mexico

Rhonda A. Syler
University of Arkansas

Karen P. Patten
University of South Carolina

Recommended Citation
Shim, J., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of Things: Multi-faceted Research Perspectives. Communications of the Association for Information Systems, 46, pp-pp.
https://doi.org/10.17705/1CAIS.04621

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04621 ISSN: 1529-3181

The Internet of Things: Multi-faceted Research Perspectives

J. P. Shim
Georgia State University
jpshim@gsu.edu

Ramesh Sharda
Oklahoma State University

Aaron M. French
University of New Mexico

Rhonda A. Syler
University of Arkansas

Karen P. Patten
University of South Carolina

Abstract:

Living beyond the hype, the Internet of things (IoT) continues to grow and has clearly emerged as a leading-edge topic in information systems. As the IoT moves beyond novel technologies and exploratory sandbox initiatives to ubiquitous technologies and full production, understanding the phenomenon surrounding IoT challenges and issues has become even more important. In this paper, we explore the critical issues and challenges currently facing IoT adoption and implementation in order to identify areas that require further study. Specifically, we discuss IoT from several key perspectives including IoT connectivity, platforms and 5G, IoT analytics, IoT privacy, security, and litigation risks, IoT business value and monetization, and human interaction with IoT and design considerations Finally, through identifying the current state of IoT and IoT research, we identify potential areas of contribution and future directions for IoT research.

Keywords: Internet of Things (IoT), Connectivity, Fifth Generation (5G), IoT Standards, IoT Platforms, Analytics, Privacy, Security, Compliance, Business Value and Monetization, Human Interaction, IoT Design Considerations, Litigation Risks.

This manuscript underwent peer review. It was received 01/23/2019 and was with the authors for 7 months for 2 revisions. Thomas Case served as Associate Editor.

1 Introduction

According to the Consumer Electronics Show (CES) and various research reports from Gartner, Deloitte, McKinsey, and Info-Tech Research Group, the Internet of things (IoT) will become a multi-trillion-dollar opportunity. Recent reports on the IoT predict that it will grow to contain 64 to 73 billion connected devices by 2025 (Columbus, 2018; Newman, 2019). The IoT connects the physical world to the Internet in contrast to the Internet of people that connects humans to each other through technology. The IoT uses sensors on physical devices connected to the Internet and collects data on their operation, location, and state. Organizations process this data using various analytics techniques for monitoring devices remotely from a central office or for predicting any upcoming faults in them. The autonomous and connected car, which continues to evolve, exemplifies an IoT device. Self-driving automobiles need to have enough sensors that automatically monitor the situation around them and take appropriate actions to adjust to any setting necessary, such as their speed, direction, and so on. Fitness tracker devices, which allow users to track their physical activities such as walking, running, and sleeping, exemplify another IoT device.

The IoT has numerous issues and requirements, such as connectivity, platforms, analytics, gateway and device (including sensors) management, communication services (i.e., networking and software protocols), security, privacy and compliance, and user interactions. In addition, organizations need to consider various perspectives for monetizing the IoT, such as their business model. As a disruptive technology, the IoT represents perhaps one of the most challenging research topics in the information systems (IS) field due to its multifaceted nature and widespread impact. Researchers initially considered the IoT—interconnected devices that use Internet technology—a machine-to-machine (M2M) technology. Yet, IoT technology has rapidly evolved to become a machine-to-person (M2P) technology. Human interaction with IoT will radically change how we live in several ways. User experiences and expectations will change with the development of consumer-oriented IoT applications, which should make life more comfortable and safe (Agarwal & Dey, 2016). “Smart environments” will also be able to automatically adjust people’s surroundings based on their needs.

Due to the IoT ecosystem’s overlapping layers and moving parts, researchers should explore the IoT from a multi-faceted research perspective for a holistic view. Accordingly, in this paper, we disseminate the different perspectives for the IoT, stimulate an engaging conceptual discussion, explore critical IoT issues and challenges, and identify areas for future research.

This paper proceeds as follows: in Section 2, we evaluate the current state and trends of IoT connectivity and platforms and review use cases among key industry sectors in order to lay the technical foundation from which IoT emerges. In Section 3, to bring attention to the interconnectedness of the IoT ecosystem, we explore four additional facets of the IoT. To do so, we describe illustrative examples of IoT analytics and applications and related research opportunities. In Section 4, we discuss IoT privacy, security, and litigation risks and IoT business value and monetization. In Section 6, we discuss human interactions with IoT including human concerns and design considerations. Finally, in Section 7, we conclude the paper by summarizing the current state of the IoT, synthesizing the salient suggestions for research selected from those presented throughout each section of the paper, and providing recommendations for the future of the IoT.

2 IoT Connectivity, Platforms and Use Cases

The IoT platform, also called the “platform of platforms”, enables connectivity among devices (MacGillivray, 2016) and successful IoT deployments. The IoT platform refers to a multi-layer technology that enables one to manage and automate connected devices in the IoT. Figure 1 depicts the IoT platform as IoT middleware. The critical components of platform and mode of connectivity have direct implications on the security, privacy, risk, and human interaction with the system, which makes it worth examining. Additionally, an IoT system must have robust platform and connectivity technology before end users and organizations can realize the IoT’s business value.

As we mention above, connectivity enables any IoT platform, and the emerging fifth generation (5G) connectivity technology is jumpstarting rapid advancements in the IoT. From 2020, commercial deployment of 5G networks will provide additional capabilities that the IoT requires, such as network slicing[1] and the capacity to connect exponentially more devices than one can do today. As the IoT

[1] For a discussion of 5G network slicing, see Appendix B.

proliferates, so does the unprecedented amount of data it generates. To cope with this data, organizations in varying industries and government agencies have either taken initial steps or continue to implement the IoT's component parts such as sensors/controllers (i.e., light, HVAC, thermal, location, identity), devices, software, and connectivity (i.e., Cellular, Wi-Fi, NFC, Zigbee, Bluetooth, RFID, TCP/IP). We also discuss underlying telecommunications technology relevant to the development of IoT low-power wide area network (LPWAN) in Appendix A.

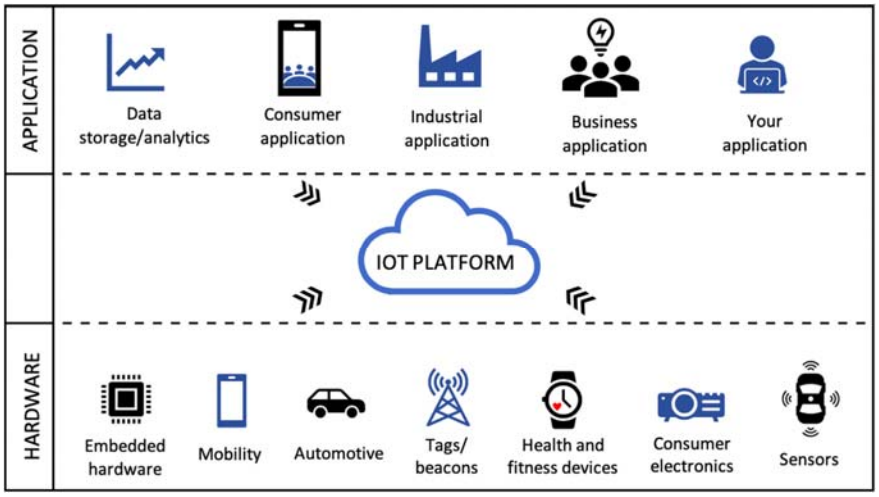

Figure 1. Internet of Things Platform (Adapted from Bondarenko, 2016)

IoT devices need to use radio resources in the most efficient way. Network requirements vary depending on latency, penetration, mobility, voice, battery life, size, and throughput. As the use cases for the IoT grow, the number of IoT platforms available in the market will also increase. Recent reports have stated that more than 500 IoT platforms in the industry exist (Shim, Dam, Coursey, & Barnes, 2017a; Hasan, 2019; Gartner, 2019). Among the key players that provide robust environments for IoT system development and deployment include Amazon AWS IoT, Google Cloud Platform, AT&T IoT, IBM Watson IoT Platform, and Canopy IoT platform. For example, Canopy, an enterprise IoT platform that takes real-time data from a network of devices and centralizes it into a single view, allows users to monitor, manage, control, and update their devices. The platform benefits users by enabling automation, reducing costs, generating revenue, enhancing security, and providing data insights.

2.1 IoT Use Cases

Potential IoT use cases and IoT adoption continues to accelerate as device costs fall, platforms improve, and innovative applications emerge. In Figure 2, we illustrate many connected enterprises, such as open architected common platforms; edge-enabled devices, data, and analytics; global-scale data and analytic services; and common applications and service workflow. These enterprises comprise utilities, supply chains, logistics and transportation, consumer electronics, public sector, smart cities, smart buildings, and industrial automation. As Figure 2 shows, businesses across all industries can use the industrial IoT to improve productivity, reduce operating expenses, and assist with new product development (Eriksson, Rossi, Shim, & Sorensen, 2019). In order for the IoT to be viable, municipalities and organizations must ensure that they use analytics when designing data-gathering systems.

5G speeds and low latencies are essential in order to meet the increasing connectivity requirements for highly reliable and low latency services. These connectivity requirements emanate from applications such as virtual reality, augmented reality, extended reality, autonomous vehicles, drone networks, smart agriculture, smart cities, and numerous use cases. Since the convergence of promising and emerging technologies, such as 5G, artificial intelligence (AI), and IoT, introduces greater efficiency and stand to be the top factors driving the digital economy in various industries, researchers should identify research possibilities for potential market opportunities as to how 5G connectivity will power applications in conjunction with developments in AI. In Section 2.2 we go into more depth on research opportunities through IoT platforms, connectivity, and use cases.

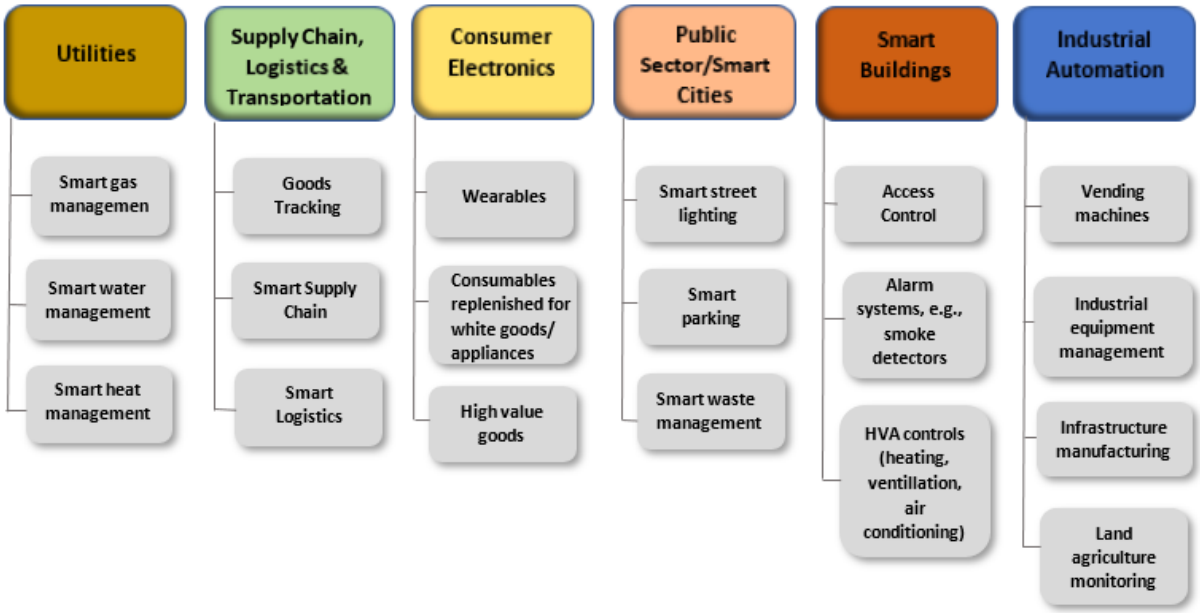

Figure 2. IoT in Various Industries and Use Cases (Adapted from Shim et al., 2017a)

2.2 IoT Platform, Connectivity, and Use Case Research Opportunities

High-speed networks' (e.g., 5G) emergence and integration with IoT platforms provides numerous research opportunities from both a design science and behavioral science perspective. From a design science perspective, researchers should establish new technologies and IT artifacts should to take advantage of these technologies' increased capabilities. Limitations due to network speeds and low latency no longer pose an issue, which opens the door for more organizations to develop and use open source platforms. For example, one could use mesh networks of IoT-enabled GPS systems to manage and direct the flow of traffic based on data collected about the number of cars, wait time, traffic speeds, accidents, and numerous other factors that the systems can record in real time. These mesh networks can analyze traffic conditions in real time and, thus, provide the most efficient route to drivers based on traffic conditions rather than the fastest route or shortest route calculated based on a static map. Further, researchers could investigate and develop drone delivery systems for various items that range from products to food. These new platforms and high-speed connectivity provide a wealth of opportunities to connect more devices, collect more data, and process that data to initiate real-time results using IoT-connected devices. With the increased development, implementation, and use of the IoT, numerous research opportunities also become more prevalent.

As with any new technology, users may use it differently to how its designers originally intended. Such alternative uses have led to numerous advancements that designers did not imagine when initially developing artifacts. We need to understand how users perceive and use new IoT technologies to understand their future directions and what end users find important. Such an understanding could result in new technologies, improvements in existing technologies' usability, or better knowledge about why users do not adopt or discontinue using the IoT. Privacy and security represent other important factors that provide research opportunities. The increase in big data also provides many research opportunities in data analytics, which we discuss in Section 3.

3 IoT Analytics

The IoT infrastructure comprises four components: 1) hardware, 2) connectivity, 3) data management software on the back end, and 4) the analytics applications. The IoT requires these components to interpret collected data and provide useful, actionable information to decision makers or to another device that can take prescribed actions based on the received information (which, of course, analytics focuses on in general). In this section, we review some IoT analytics applications and identify relevant research issues.

3.1 IoT Applications: Illustrative Examples

Siemens, which produces a variety of trains and infrastructure components including control systems and power systems, recently applied the IoT in the industrial sector. The company wanted to move from reactive maintenance (after the incident) and preventive maintenance (with regular inspections) to maintain trains. The company connected sensors to its trains' components to measure their current situation. The company collected the sensor data and analyzed it in near real time. If the company found any anomaly found in the data, then the anomaly indicated a component would likely fail. Thus, the company could take appropriate preventive measures. According to a Teradata blog, Siemens' engineers leveraged data from thousands of sensors. Data from the trains and rails, repair process data, weather data, and data from the supply chain enabled Siemens' data scientists and engineers to quickly identify false positives (predicting a failure that would not occur) and more clearly predict actual part failures (Teradata, 2015). By incorporating weather data, Siemens learned to differentiate what would more likely fail on the high-speed train between Moscow and St. Petersburg in the frigid winter versus the high-speed train traveling in the hot Spain summers.

If the company found abnormal patterns in the sensor data it collected, it dispatched a team to inspect these components and, thus, prevent trains from failing on the tracks. By employing sensors that generated a large amount and variety of data and merging that data with other data sources such as weather, a company can build a better picture of how its products perform in the real environment. Further, analyzing such data can help a customer perform maintenance when actually necessary rather than on a timed schedule. Selling such analytic services has become a major new focus for all leading industrial equipment makers, such as Siemens and General Electric. Selling services to perform analytics on products and predictive maintenance or repairs exemplifies how organizations can create new market opportunities for established products. These two examples show how Siemens has begun to use digital innovation through IoT analytics to both improve its internal processes to provide better services and to develop new digital analytic products to other companies.

Teradata reported a similar application that it provided to the U.S. Navy to analyze data coming from multiple sensors and employ analytics to determine the optimal time to perform maintenance. For example, the U.S. Navy operates a variety of helicopters around the world. Sensors on a helicopter generate over 21,000 8K data blocks. Engineers analyze this data using pattern-recognition techniques to identify the best time to perform maintenance. If such predictive analyses improve capacity by just five percent, one more helicopter out of 20 becomes available in urgent situations (Davis, 2017). Such IoT analytics has caused the term "condition-based maintenance" to become popular. Rather than performing maintenance on equipment at a predefined schedule, in the emerging approach, one monitors equipment's condition using hundreds of sensors and then performs maintenance as the conditions warrant. These applications, which exemplify digital innovation through IoT analytics, truly employ all three types of analytics techniques: 1) descriptive (to understand the past performance), 2) predictive (to determine when the next fault might occur given the state of the equipment), and 3) prescriptive (to optimize the maintenance schedule).

3.2 IoT Analytics Research Opportunities

Through various research projects in IoT industry applications (see, e.g., how many doctors now use the IoT to better coordinate care) (Patten, Regan, & Wu, 2018), many interesting IoT research opportunities arise. Clearly, one needs to predominantly consider many security and privacy issues in implementing the IoT for enterprise and consumer applications to, among other things, ensure that users accept them. In Section 4, we focus on issues and research opportunities related to security and privacy. In this section, we present research implications related to analytics. We can broadly group these research opportunities

into two categories: 1) novel applications and 2) advances in data science algorithms to enable these novel applications.

First, given the IoT's nascence, many interesting applications remain undeveloped. Just as analytics/data science and artificial intelligence work led to many innovative applications and corresponding research opportunities to develop new algorithms and systems, the IoT offers similar possibilities. As we and the many references we cite note, interesting applications of IoT have begun emerging in smart cities, healthcare, smart supply chains, smart grids, smart transportation systems, and more. The three Vs commonly associated with big data (i.e., volume, variety, and velocity) constitute key ingredients for developing these applications. Sensors of all types now generate massive *volumes* of data, creating a *variety* of data streams arriving at a high *velocity* that need to be compiled, analyzed, and acted on. These three Vs each lead to various research opportunities. Marjani et al. (2017) identify some of these issues. To frame the data issues, they divide all IoT applications into several sub-categories: real time, offline, memory level, BI analytics, and massive data. The first subcategory of applications focuses on real-time analytics, which requires low latency response times since data changes rapidly. Autonomous vehicles would fit in this subcategory. "Complex event processing" (CEP) represents an analogy to such IoT analytics applications. With CEP, one analyzes many data streams as they arrive and infers a specific event/opportunity from them to take further action. Researchers have continued to develop complex event processing for some time (Buchmann & Koldehofe, 2009) to analyze a data streams, create an alert, and possibly even initiate an action. Developing such analytics applications requires very efficient storage and modeling responses. Domain needs will also play a role in determining the data and models one chooses. Researchers continue to investigate this area.

Marjani et al. (2017) call the next subcategory of applications offline analytics. In offline applications, one can collect and compile IoT data over time and analyze it to develop the best models. Massive storage needs have led researchers and organizations to develop Hadoop and other related technologies for such analytics. Tools such as Kafka (Kreps, Narkhede, & Rao, 2011) specifically help one analyze data streams. Marjani et al. (2017) label the next subcategory of applications memory-level applications. One can employ the small dataset being generated to build an IoT application. Many research projects may start here as a proof of concept before needing a full cluster of computers for model development and eventual deployment. Marjani et al. (2017) also note another subcategory of applications related to business intelligence Business intelligence (BI) analytics refers to the more traditional analytics architectures for building and deploying IoT models. Given that the BI industry has matured the most, one can employ some BI tools and models in developing IoT applications. Exploring the limits of traditional BI analytics platforms in the IoT space represents another research opportunity.

Marjani et al. (2017) call the last subcategory of applications massive datasets. Overall, data volumes continue to grow, which has led to a continuous need for efficient data-storage and management techniques and hardware for organizing, storing, and curating data and deleting unnecessary data. The data processing step in the data mining process CRISP-DM (Shearer, 2000) will likely be even longer and more iterative when one deals with IoT data. Indeed, integrating the data coming from various sources, initially examining/exploring it, and figuring out what to do with it involves much complexity even in traditional data-mining projects. As such, we can see why CRISP-DM's data processing step can take up to 80 percent of an analytics project's total effort (Sharda, Delen, & Turban, 2019). When data arrives from thousands of sensors at a massive rate, the scale of the problem increases exponentially.

The second major category of research opportunities refers to developing new algorithms and methods for enabling IoT applications. We must recognize that the data that IoT devices collect mostly has little value in and of itself. Only when one derives specific performance measures from recorded data does something valuable emerge from IoT. Thus, one may have to identify new performance metrics or even predictor variables by transforming the data that one collects.

Visualizing data is a key step in data processing and usually one of the first outputs from analytics applications. Visualizing large datasets in analytics projects already involves much difficulty, but the problem grows even more when we consider IoT data with its multiple formats, sheer volume, and varying collection rate. To identify anything interesting from visualizing such data streams, one needs to develop new ways to present the data, to investigate ways to reduce dimensionality, and to identify novel ways to interpret results from visualizations. For example, Automated Insights (Caswell & Dörr, 2018) has developed some pre-formatted ways to interpret Tableau visualizations. As IoT data grows in volume and variety, interpreting data in such automated ways will become even more important and require further research efforts.

Due to the IoT, the predictive analytics modeling step also presents new opportunities for research. For example, the large data volumes associated with the IoT require one to develop parallelized algorithms. Researchers have and continue to develop such parallel algorithms for virtually all classes of data mining models: classification, clustering, association mining, and so on. Wu, Zhu, Wu, and Ding (2014) provide an early summary of these parallelization efforts. Of course, such algorithms also need to evolve as parallel architectures evolve. This area has been and continues to remain an active research area. Due to the sequential nature of IoT data in many settings, a need to develop time-based association mining or other modeling methods also exists. For example, researchers have begun to explore autoregressive moving average methods and other time series approaches for analyzing IoT data (Ryan, 2013).

Besides the above two broad categories of research opportunities related to making the IoT more useful and practical, one can also apply the developed analytics approaches to more efficiently manage data-collection and compilation methods or to build a better predictive model. For example, researchers have explored optimization models to determine where to optimally place sensors to maximize coverage or optimize the cost (e.g., see Faragardi, Vahabi, Fotouhi, Nolte, & Fahringer, 2018; Rullo, Serra, Bertino, & Lobo, 2019). In addition, researchers have also applied analytical models to develop better data-management methods. For example, Kumar and Chaurasiya (2019) propose and compare a data-mining method with other approaches to minimize data redundancy in a sensor network. Many such opportunities for analytical modeling applications in the IoT exist.

Besides all the technical and system approaches that many design science IS researchers know well, opportunities abound for exploring how well IS theories apply to or extending such theories to the IoT. For example, could media richness theory or its variants help one present IoT-based analytics or alerts? Son, Lee, Jin, and Lee (2019) studied how one could apply media synchronicity theory to determine what tweets should optimally contain in emergency alerts. Similarly, would researchers more widely accept the results of such models if technology acceptance model or its variants (Davis, 1989) guided such development?

Thus, the IoT provides a rich playground for researchers in the analytics and design science domains to develop new applications, models, and data methods while also providing significant opportunities for extending IS theory in these domains.

4 IoT Privacy, Security, and Litigation Risks

With 4G already here and 5G[2] on the way, the infrastructure now exists for businesses to capitalize on the hyper-connectivity of the estimated 64 to 73 billion IoT-connected devices by 2025 (Columbus, 2018; Newman, 2019). Although industrial IoT has already been established as a successful business model, the smart home and healthcare markets have the biggest potential for future IoT development (FTC, 2013). While this vast infrastructure of connected devices continues to grow, which creates a wide array of opportunities, we need to address growing concerns about privacy and security.

As a technology, the IoT extends previously built infrastructure, which further adds to security risks that network administrators must address. As Figure 3 shows, the IoT creates multiple connections to networks that only users could previously access through devices they owned. These extensions potentially add connectivity to any device through automated procedures without any human interaction, which would create numerous access points from various devices that must be secured to protect the network. Gartner predicts that more than 25 percent of all cyberattacks on businesses will comprise IoT-based devices (Cook, 2019). Furthermore, the increase in connectivity will cause data's variety, velocity, and volume to exponentially increase, which will further contribute to big data's growth. Such growth will create privacy concerns about the types of data that organizations collect, store, and manage.

[2] See Appendix A and B for information on LPWAN, IoT connectivity, 5G, network slicing, and diverse spectrum.

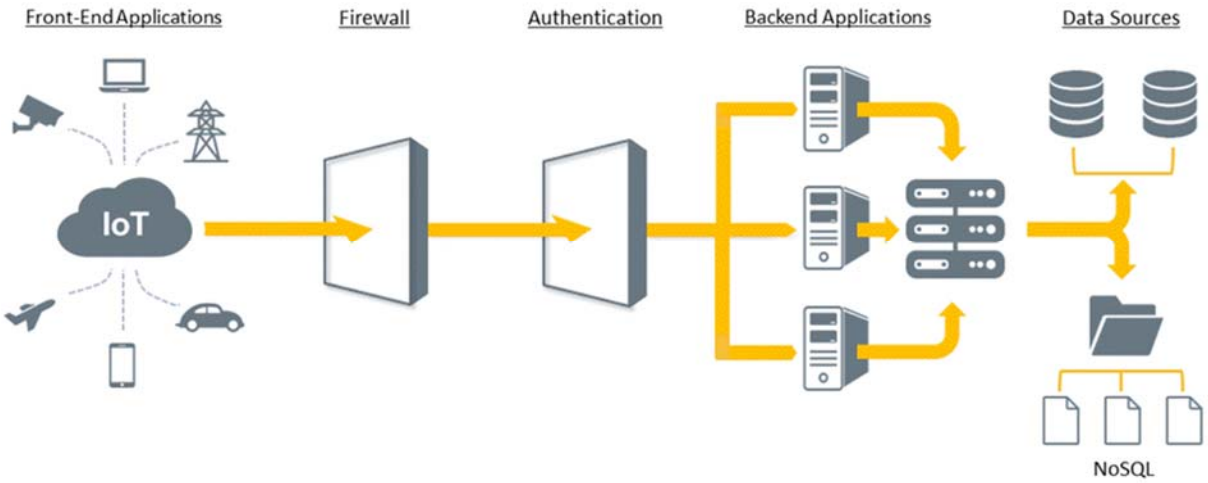

Figure 3. IoT Infrastructure

4.1 Types of Threats

When discussing privacy and security, we must be able to classify the type of concerns and the urgency for addressing them. While data's volume and variety continue to grow, data differs in its sensitivity. We can divide privacy concerns into low to high sensitivity and low to high harm (Smith, Dinev, & Xu, 2011). Security threats can span from inconveniences, such as a denial-of-sleep attacks (Raymond, Marchany, Brownfield, & Midkiff, 2009) that causes one's phone battery to constantly die, to physical threats, such as a hacker compromising one's IoT-enabled car in such a way that it causes an automobile accident (Takefuji, 2018). Figure 4 demonstrates the range of security and privacy threats that businesses must address and relevant examples.

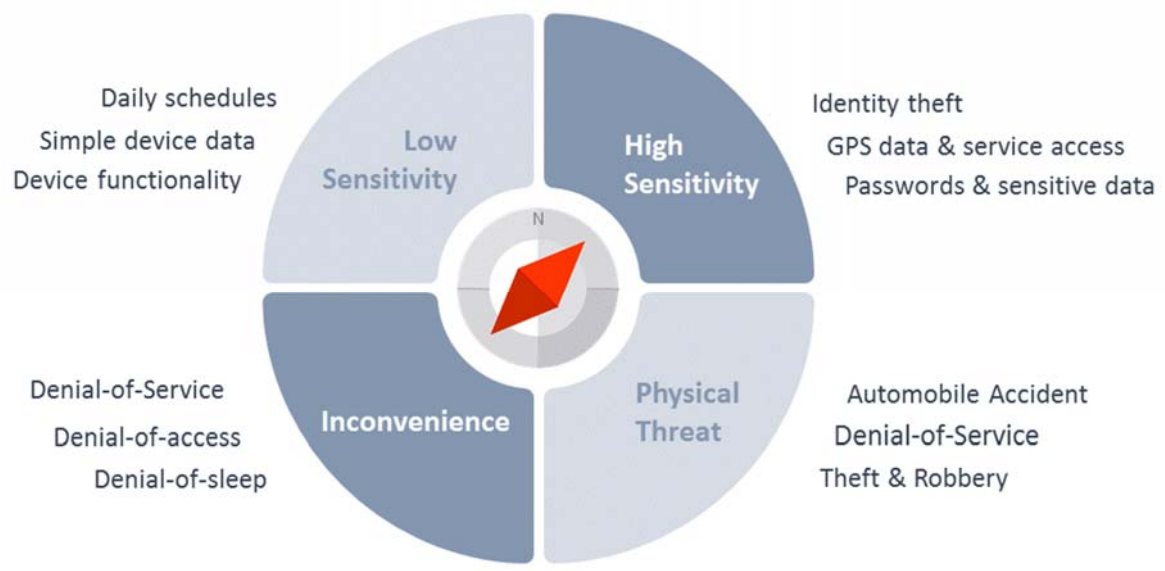

Figure 4. Privacy and Security Concerns

The harm a threat may have and its sensitivity have a subjective nature: they depend on users' perspective about the consequences that may result. For instance, users could consider a denial-of-service attack that results in their inability to access their Fitbit an inconvenience, while they could consider a denial-of-service attack to their IoT pacemaker monitoring service a physical threat since it

could potentially result in their death. However, threats can have consequences for stakeholders other than end users as well, such as IoT device creators, IoT service providers, and third parties. Thus, when considering how to handle privacy and security threats, one must first identify who to protect.

One can easily recognize the threat that privacy and security concerns can have for users since users have direct contact with IoT devices and the user data they provide. Users may be subjected to breaches of their private data or security threats due to using IoT-enabled devices (Hossain, Fotouhi, & Hasan, 2015). Their home security may be compromised or the services they rely on may be lost due to an IoT security breach. The service provider or device creator may also be subject to negative consequences due to IoT privacy and security breaches. Providers have a responsibility to protect users and secure their devices. Security breaches could result in loss of reputation, lawsuits, or even in the company going out of business. They also threaten third parties who do not use IoT devices or did not play a part in creating them. Although manufacturers often put the security burden on users, manufacturers certainly bear a large responsibility to "bake in" the security as much as possible.

Cyber-physical systems and industrial IoT (IIoT) cybersecurity have become buzzwords in today's IT security world (Shim, 2019). IIoT continues to grow from automated manufacturing to IoT-enabled power grids. A breach in IoT manufacturing could cost a company millions of dollars and result in in increased product and service prices for its customers. More severe consequences could include service losses or terminated production, which could limit or eliminate customers' access to the products and services that they need. Security breaches in IoT-enabled power grids could leave customers who rely on electricity from those power grids without power. Despite the infancy of IoT technology and services, several security breaches have already occurred. In 2016, attackers hacked cameras and DVRs to create a massive power outage in the United States (KOS, 2016). Attackers used handheld computing devices to steal cars in Queensland in Australia (Robertson, 2012), and Jonathan Petit of Security Innovations in Massachusetts identified a vulnerability in self-driving cars when he discovered that a laser could disable the vehicle (BBC, 2015).

4.2 Addressing the Threats, Regulations, Privacy, and Compliances

A man-in-the-middle attack—where attackers hacked IoT-enabled devices and used them to carry out the attack—caused many breaches that we discuss above. Organizations face several challenges in securing new IoT-enabled devices, such as the lack of growth in programmers and IT specialists and significant growth in connected devices (Roscher-Nielsen, Ratliff, Rudy, & Petroules, 2017). While the number of programmers has steadily grown since 2005, it has not matched the exponential growth in the number of IoT-enabled devices (Roscher-Nielsen et al., 2017). The number of tools used to create IoT-enabled devices also continues to grow, which poses challenges in keeping up with users' security needs. Given that the Internet remains unsecured, one cannot reasonably expect the IoT to be totally secure. However, we recommend that companies should address the more serious vulnerabilities before a major attack occurs, which could harm the ecosystem of users, services, and equipment providers.

Governments have established several regulations to address the growing threat to privacy and security. Regulations and compliance laws push developers to address the issues with the IoT rather than delegate the responsibility to end users. For example, the European Union (EU) has implemented the General Data Protection Regulation (GDPR) that requires measures to protect user data of all citizens in the EU (Nadeau, 2018). This regulation extends to all non-E.U. companies that manage data of citizens in the EU and, thus, has created a pseudo global regulation for data management and protection. The GDPR applies to any type of data that one could use to identify individuals; thus, it covers what data one can store, how one can store it, for long one can store it, and how one can use it. The GDPR also includes strict rules on how organizations must report data breaches. The EU enforces hefty fines for organizations that fail to comply with the regulations. While the United States (US) does not have uniform regulations addressing data security, individual states have begun to proactively address privacy and security issues. In California, lawmakers passed the California Consumer Privacy Act (CCPA) in June, 2018. It mirrors the GDPR but has less rigid requirements in comparison (AbacusNext, 2018). Like the GDPR, the CCPA focuses on protecting local citizens' data and targets all companies despite location that handle any personally identifiable information of Californian residents.

While government regulations represent a big step forward to address privacy concerns, we still need to do much to prevent IoT-related security threats. Governments may put regulations in place to address responsibility and accountability, but preventative measures would be much more successful than responsive measures. Governments can apply preexisting technical knowledge and training to address

security issues in the IoT arena; however, many organizations do not have sufficient human resources to implement the solutions. Many companies struggle to meet the demands of IoT growth even with their entire programming team focused on new development. Without proper manpower, they lack enough time to focus on non-revenue generating aspects of IoT development related to security. Security represents more of a cost-preventative measure that organizations often defer to future initiatives once a breach takes place, which causes them to act reactively rather than proactively. To address this lack in human resources and match programming developments in industry, organizations need to focus on attracting new talent and increasing the number of programmers they hire.

4.3 IoT Cybersecurity and Litigation Risks

Within the rapidly evolving IoT ecosystem, IoT devices often lack managers or strong security since they prioritize convenience rather than security. An unmanaged IoT device refers to individual devices that individual end users connect to and manage (U.S. Chamber of Commerce, 2017). With the door wide open for attacks, we have seen a tremendous rise in cyberattacks against these unprotected and unmanaged, or unsecured, IoT devices, which leads to a compromise. The list of numerous IoT harms continues to grow daily, such as data breaches, IoT ransomware, distributed denial-of-service (DDoS) attacks, vulnerable and unpatched IoT devices, and potential for cyber-physical systems. Furthermore, these unsecured and unprotected devices have a debilitating effect as they infiltrate every tier and department of and compromise organizations. Given that the supply chain serves as a backbone for most organizations' business operations, defective IoT devices are at even more risk than ever before.

Given that traditional security solutions have shown weaknesses—unprotected storage, hardcoded backdoors, unencrypted communications, and insecure pairing procedures—they cannot reliably protect IoT devices against cybersecurity attacks and risks. Recently, a wave of legal litigation over IoT liability has emerged. The federal class action lawsuit on Jeep Cherokee hacking (Davis, 2018) will serve as a warning to all software, design, and hardware companies that have not properly prepared for IoT cybersecurity threats and risks.

The various cutting-edge issues that organizations face today, such as privacy, data security, data transfer, and other cybersecurity requirements, have entered the forefront more questions now revolve around the complexity of defective IoT devices and how much attention this topic will receive. When it comes to legality and litigation risks, the question then surrounds who will be responsible in these legal issues. This question will be more problematic as organizations face even more inadequate data protection and may not recognize how much information that their networks and nearby IoT devices transmit.

4.4 IoT Security, Privacy, and Litigation Risks Research Opportunities

Researchers have long investigated privacy and security. Contemporary privacy research began in the 1970s and encompasses a variety of levels from individual, group, organizational, and societal (Smith et al., 2011). The history of security spans various areas from intellectual ownership, identity management, communication security, and computer security (Leeuw & Bergstra, 2007). We can subdivide these broad areas into various categories that span many domains and contexts that have specific privacy and security attributes based on the technology and parties involved. Privacy and security constitute two distinct areas that often converge as one affects the other. As new technologies emerge, the privacy and security landscape will continue to evolve. While privacy and security may have a reciprocal relationship depending on the domain, technology, and active parties involved, they also individually provide opportunities that we need to address.

As we demonstrate above, IoT extends existing frameworks in that it provides new access points through which smart devices can connect to a network. As the technology environment continues to change due to the IoT, the tools that organizations use to secure the network also need to change. These new access points have created new opportunities for hackers, which has resulted in new techniques for gaining access to the network as man-in-the-middle attack examples show. Researchers should focus on identifying these new vulnerabilities and new attacks that could adversely affect technology and how individuals perceive security when using it. Organizations continue to put the responsibility of security in users' hands by implementing mobile verification for their services and using biometric authentication software (e.g., software that recognizes fingerprints, eyes, or faces). Researchers should also evaluate these new security techniques to determine their implications and limitations for possible vulnerabilities, assess how end users should use them, and evaluate their social-engineering capabilities. For example, if

an individual uses mobile verification for all their IoT services, then they create a single access point that, if compromised, would leave all the services accessible. To ensure IoT networks remain secure, users need to ensure that they take proper measures to secure their devices. Accordingly, researchers should evaluate the various security options available for mobile devices (e.g., fingerprint scans, iris scans, passcodes, facial recognition, voice recognition, etc.) using a matrix that comprises ease of use and secureness to determine the most secure options and what users consider the easiest to use. Social engineering—another aspect of security—also warrants more research attention as IoT devices not only collect data in real time but also post in real time to various social networking platforms. Historically, social engineering required stronger interpersonal skills to extract private information from individuals that one could use to gain access to certain networks and services. However, since many users publish their private information on social media, social engineering may now only require researchers to connect with individuals on social networking platform(s) and to search for the information they need directly. Information provided on social media could provide many personal details about a person, their friends and family, habits, geological data and daily schedules, and more. Here, privacy and security become integrated the most.

On the privacy side of the equation, the IoT provides vast amounts of data about individuals that ranges from their habits and interests to a complete daily activity schedule. As we note above, the IoT contributes to the big data environment in that smart devices that connect to the Internet continuously collect data. For example, a person using a Fitbit device daily provides information related to their health condition and daily activities. Fitbit tracks and monitors individuals' heart rate and sleep quality, which one could use to extrapolate health conditions they may have. Fitbit also tracks individuals' location, number of steps they make each day, and various other personal metrics. While HIPAA regulations prevent healthcare professionals from disseminating patients' medical information for personal safety, the data that Fitbit collects could give insights to various conditions that laws seek to protect. Here, IoT analytics and privacy research provides analysis of varying levels of privacy controls and ever-changing regulations, especially with the level of exposure of private data collected via privacy tools. Marketing companies can identify various medical conditions, pregnancy, personal interests, and more through analytical tools that organizations use to evaluate purchasing habits. Given how much data organizations could obtain through IoT devices, we need to ask whether governments should extend compliance laws to cover them. Future research should also evaluate privacy's implications for the multitude of IoT devices and vast amounts of data that organizations collect.

5 IoT Business Value and Monetization

In addition to the issues surrounding IoT standardization and platforms, IoT privacy and security, and the IoT analytics landscape, we need to understand the IoT's potential business value and avenues for monetization. Indeed, the continued surge in IoT devices may have significant implications for organizations' bottom line. Indeed, Richard Kelly, Partner of McKinney and Company, has estimated the IoT to economically impact various different domains by as much as €11 trillion (SAP TV, 2016). Given this potential impact and IoT devices' prevalence and ubiquity, we need to understand how to leverage IoT technologies to realize their benefits to derive value from them. From optimizing operations to enhancing customers' service experience, IoT digital innovations have begun to revolutionize the way we do business. As these technologies become ubiquitous and platforms and architecture begin to reach maturity, understanding IoT digital innovations' value proposition becomes increasingly important. The IoT's advantages (e.g., process improvement and optimization, increased organizational efficiency, improved customer experiences, optimized cost structures, and risk mitigation) extend across multiple industries (Omnim2m, 2015).

5.1 Finding the Business Value: Reducing Costs and Increasing Revenue

As with many disruptive technologies, especially in the honeymoon phase, we do not know what impact the IoT will have. As yet, we lack a roadmap for navigating the IoT landscape and the IoT's value. By examining the IoT's cost-saving benefits and IoT technologies' and services' revenue potential, it becomes possible to begin to identify the IoT's value proposition.

5.1.1 The IoT's Cost-control Benefits

From an internal-operational perspective, IoT applications bring value through operational optimization, organizational efficiencies, and cost-control reductions. For example, Trenitalia, the Italian train company,

has reduced its maintenance costs by almost 10 percent and saved itself around €100 million per year using an IoT approach (SAP, 2016). In Section 3, we also note some other cost-saving examples in maintenance or supply chains.

The IoT can help organizations from all industries reduce costs. In another example, a U.S. telecommunications company reduced costs by deploying a tracking system in its residential service vehicle fleet. With this system, it could obtain immediate feedback, analyze efficiencies in route planning, and intervene in real time should a driver leave the route's boundaries, exceed speed limits, or experience unexpected mechanical issues. It also used sensors to provide real-time data on vehicle performance for predicting system issues and mechanical breakdown, which allowed fleet management to intervene early and prevent possible system failure.

5.1.2 Revenue and Monetization Potential of IoT

The IoT can also help organizations increase their revenue. Leveraging IoT product or services to consumers provides value through enhanced customer experiences, value-added services, and subscription revenue models. For example, Burberry has used RFID tags to create a unique customer experience. When a customer has a product in hand or cart and encounters a monitor, the tag launches a video that provides information about the product, which enhances and adds value to the customer experience. As we mention in Section 3, Siemens developed an IoT analytics process to improve its train and track maintenance and now sells the IoT analytics services as a product to other manufacturers—another way to increase revenue that the IoT has created.

5.2 IoT: Shifting Business Models and Shifting Mindsets

Even though the IoT can clearly help organizations reduce their costs and increase their revenue, they need to change their business model and mindset to realize this value.

5.2.1 Value Creation and Value Capture

As a disruptive phenomenon, the IoT shatters paradigms about how organizations produce and deliver products and services and how individuals perceive them. Looking at products and services from a value-creation and -capture lens (see Table 1), one can see the paradigm shift from the traditional product mindset to the IoT environment (Hui, 2014).

Table 1. Value Creation versus Value Capture (Hui, 2014)

		Traditional product mindset	Internet of things mindset
Value creation	Customer needs	Solve for existing needs and lifestyle in a reactive manner	Address real-time and emergent needs in a predictive manner
	Offering	Stand-alone product that becomes obsolete over time	Product refreshes through over-the-air updates
	Role of Data	Single point data for future product requirements	Information convergence creates the experience for current products and enables services
Value capture	Path to profit	Sell the next product or device	Enable recurring revenue
		Potentially includes commodity, advantages, IP ownership and brand	Adds personalization and context; network effects between products
		Leverage core competencies, existing resources and processes	Understand how other ecosystem partners make money

With traditional products, product-development approaches have a reactive nature and focus on meeting customers' pre-existing needs and wants. Also, traditional products are not developed to anticipate product bugs and failure nor are they designed to integrate with the consumer experience for real-time response to product issues. IoT products, on the other hand, can address real-time and emergent consumer needs as they occur and often before they occur through techniques such as predictive analytics to intervene to avoid or mitigate costly repairs or equipment down time Traditional product offerings often constitute standalone products that will eventually become obsolete. Products in the IoT ecosystem shatter that paradigm in that one can update them "over-the-air" in real time and, thus, extend their life and potentially improve the synergistic value between consumers and companies and between

companies and companies. Finally, with traditional products, organizations typically collect data once at the initial transaction with the consumer, but the IoT provides the opportunity to gather data at various touchpoints before, during, and after consumers acquire a product, which allows organizations to develop more robust insights about their consumers and enhance the value of the consumer experience (Laskowski, 2015).

Organizations also need to adopt a different approach to capturing value when developing business models for IoT products compared to traditional products. Indeed, value capture in traditional products has a radically different route to profit compared to value capture in IoT products. With traditional products and services, organizations profit simply by selling the next one (Hui, 2014). However, with the IoT, organizations can profit on a recurring basis via mechanisms such as subscription services. Additionally, traditional products include commodity, IP ownership, and branding advantages, but IoT business models have a multi-dimensional nature, which adds personalization and context layers to the customer experience and helps organizations to lock customers into their products and services, which network effects enhance as they introduce new products.

5.2.2 IoT Requires Shifting Mindsets

Finally, a significant difference in traditional versus IoT product mindset concerns the need to understand how other IoT ecosystem partners generate money. IoT products have a considerably deeper market stack than traditional products (Westerlund, Leminen, & Rajahonka, 2014). Thus, a company must think about how others monetize their products to be able to capitalize on where its business model fits best. A company also needs to understand how its products can help others generate and collect value. Being able to serve as a cog in the wheel of the IoT system can help make a firm viable and sustainable in the IoT marketplace. Figure 5 illustrates how these IoT aspects potentially shatter preexisting paradigms.

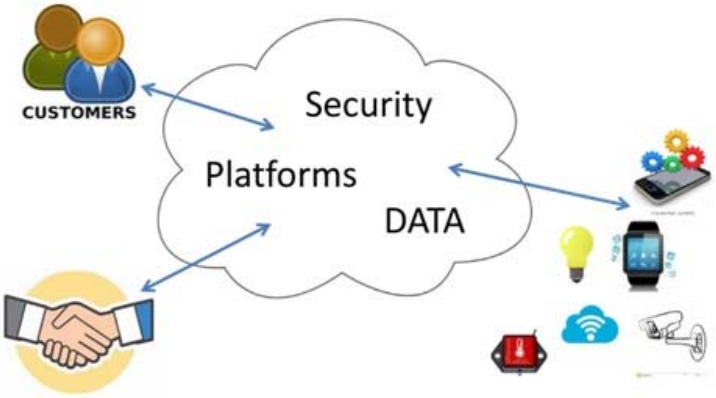

Figure 5. IoT Ecosystem—Paradigm Shifts

5.3 IoT Business Value and Monetization Research Opportunities

As we show above in this paper, the IoT ecosystem has numerous issues that deserve a closer look in order to optimize the potential the IoT affords and understand the drivers that ultimately impact its business value. However, while we cannot overstate the IoT's business value, we need to better understand the phenomenon from all facets to enable organizations to most effectively design IoT systems, reengineer processes accordingly, and reinvent business models to realize its full potential.

Like the IoT ecosystem itself, many research opportunities in the IoT space (including the ones we present in this paper) have an integrative nature. The behavioral factors of human-computer interaction (see Section 6) and security compliance (see Section 4), the IoT's physical and technical security characteristics, the technical infrastructure, and the success of IoT analytics initiatives each separately and together directly impact the value that businesses can realize from the IoT's potential. For example, organizations can improve the value they gain from deploying an IoT via insights from analyzing the massive amount of data they collect when monitoring processes and events in real time. A well-designed IoT that optimizes human-computer interaction and builds trust through proven security protocols theoretically has a better chance to engage consumers and improve customer experiences. Effectively, research on the IoT's business value uses business value as the primary variable of interest as opposed

to an explanatory construct. In particular, the IoT system's various facets (connectivity and platforms, security, and data) and behavioral constructs such as trust hold much potential for examination.

Industrial and business-to-business IoT deployments experience the greatest growth today likely due to these IoT initiatives being the easiest and least risky to initially deploy. Organizations have obtained various benefits such as reduced costs from monitoring critical systems in real time, predicting outages, remotely monitoring field equipment rather than sending technicians to the field, and so on. But can these organizations sustain such benefits? What IoT characteristics lead to or moderate process improvements? What IoT characteristics help organizations mitigate risk? What IoT characteristics make the IoT the proper solution for an industrial or operational efficiency problem overall? What key drivers will maximize quantifiable business value? What implications will emerge from the inevitable shift in the way organizations conduct business operationally? Will such a shift have unintended consequences, such as job losses?

As the IoT further matures and the technical and procedural infrastructure exists from industrial and B2B deployments, business-to-consumer models become less risky and potentially more fruitful. Thus, we will see greater movement in the business-to-consumer IoT domain in the future. From this perspective, several areas of inquiry deserve attention. The relationship between organizations and customers and between customers and products in an IoT economy primarily has a transformative nature, which leads us into unchartered waters. With products that self-diagnose and direct a customer to conduct their own routine maintenance and repair, service models will change. What customer service models will be most successful? What are those models' key drivers? How do we best design these models, especially in terms of communication and engagement with the customer to maintain customer satisfaction, improve the customer experience, and maintain customer loyalty? With products such as smart watches, smart washing machines, smart refrigerators, and more, companies can realize significant cost savings by automating and remotely conducting diagnoses and, in some cases, repairing products. In this way, organizations can save on costs in that technicians need only go on site when they need to conduct physical maintenance or repairs. This lack of human intervention, however, has the potential to negatively affect business-to-consumer relationships. So how do we design user interfaces and other customer touch points to maximize customer satisfaction and increase customer loyalty?

The IoT is and will continue to disrupt business as we know it, and no industry will go untouched. Business models overall are shifting to embrace a world where IoT will become a core element to the way we do business. The nature of the IoT ecosystem and IoT economy itself requires organizations to collaborate, cooperate, and even co-innovate and co-create. But to what degree do they need to? Does a cooperation threshold that begins to be counterproductive or even, perhaps, undermine IoT's potential value exist? Can organizations realize competitive advantage and, if so, in what stages and where? What role will/can other technologies such as blockchain, machine learning, and artificial intelligence play in complementing or disrupting evolving IoT business models? As the IoT continues to mature and many organizations have iterated through a complete IoT system lifecycle, we will need to develop a maturity assessment framework and to conduct studies that evaluate and understand best practices for IoT development and deployment in order to help organizations achieve the greatest business value.

Finally, monetization of the IoT and its outcomes constitutes a key research area with many opportunities. For example, organizations stand to gain significant dividends from monetizing the data that they collect while using the IoT for their daily operational and industrial oversight. We need to understand the degree of monetized value in relation to the tradeoff of customer relationship and proprietary value. Other research opportunities in this area include examining the business value and sustainability of various monetization strategies such as access to analyze usage data through pay-per-use or subscription services. In particular, what drivers lead to a successful IoT monetization strategy? Where in a monetization model's lifecycle can an organization achieve a competitive advantage? And what drivers make it sustainable?

6 Human Interaction with IoT: Human Concerns and Design Considerations

While the IoT and increased connectivity show promise for making our lives more comfortable and safer (Agarwal & Dey, 2016), IoT developers have a mindset focused more on reaching the market first than on improving individuals' quality of life. As we mention in Section 1, although originally considered a machine-to-machine (M2M) technology, IoT technology has also emerged as a machine-to-person (M2P)

technology with many different types of human interactions. Research shows that human interactions with the IoT continue to evolve as different domains adopt and transform due to it. However, Agarwal and Dey (2016) point out that research into the IoT's impact on humans remains in its nascency. In this section, we discuss several human-centered concerns and what we may consider best practices for efficient, effective, and secure IoT design from the user perspective.

6.1 The Human-centered Internet of Things

Researchers generally consider human-centered IoT to have three components: 1) things, 2) the Internet, and 3) semantics (Atzori, Iera, & Morabito, 2010; Koreshoff, Leong, & Robertson, 2013). The best and most effective consumer-related IoT application design will integrate all three components as Figure 6 shows. The shared area between things and semantics reflects a person's "sensemaking" from using IoT smart devices. In Section 3, we describe the need for "sensemaking" or interpreting collected data to provide useful, actionable information for decision makers. The shared area between things and the Internet reflects the connectivity between IoT smart devices and networks through which the devices can transfer/receive data and information. In Sections 2 and 4, we discuss issues and research opportunities concerning the intersection of the Internet and IoT smart devices.

The area between the Internet and semantics reflects people's communications and how they understand the resulting information. Therefore, one must evaluate IoT design considerations at the intersection of all three components for human-centered IoT success. In this section, we focus more on how users use smart devices and what developers need to understand about how different users will use data in different contexts.

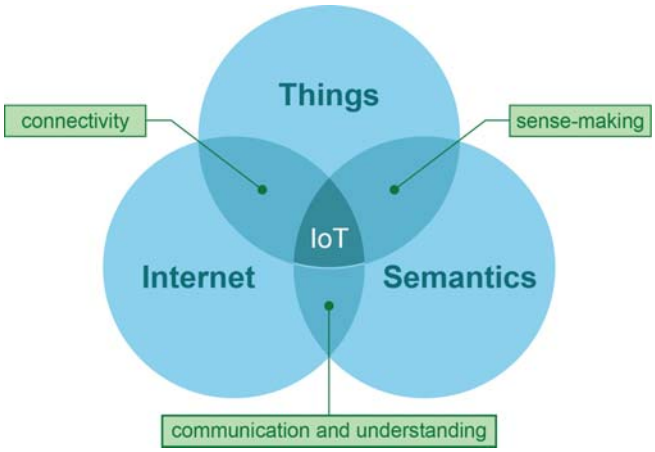

Figure 6. The Human-centered Internet of Things (Adapted from Atzori et al., 2010)

6.2 Human Concerns and Design Considerations

Focusing on human-centered design considerations, we reviewed the literature that focused on the IoT from the human-interaction perspective. For this paper, we identified five specific categories of IoT characteristics and concerns that developers should consider when designing IoT devices and applications for human interaction: 1) types of environmental interactions, 2) semantic data selection, 3) smart device design, 4) smart devices' interaction levels, and 5) application trustworthiness. Trust in IoT applications depends on individuals' expectations, values, and beliefs. We summarize the following significant factors to provide a broader perspective for IoT developers to consider when designing IoT applications for human interaction. These same five categories also provide opportunities for IS research, especially in human-computer interactions (HCI) and human factors. These categories focus on how humans interact with IoT devices, what information humans or devices require to understand situations and take appropriate action, and how humans perceive the trustworthiness of the interactions.

6.2.1 Environmental Interactions

A human interacts with smart devices in different ways depending on the environment and application or the interaction's purpose. Based on the application or use, Nguyen (2015) describes three types of human interactions: 1) person centric (individual), 2) home centric (individual or family), or 3) city centric (group or

community). A person-centric environment has a strictly "tool-based" interaction model in that a smart device assists a user to complete a task (i.e., turning on/off lights, locking/unlocking car doors.) Unlike a person-centric environment, a home-centric environment may have either a tool-based or "automated" interaction model. For example, in a tool-based model, an individual would give instructions to a smart device, which would open or close shutters on command. In the automated model, shutters, which sun sensors control, would automatically sense and react without any human instruction. In the city-centric environment, a small group or even a large community also has two different interaction model choices: automation and proactive. In the automation model, a smart device senses and reacts without any human initialization. However, in the proactive model, data from the environment causes the smart device to make its own decisions. In this case, the users must trust the smart devices to complete tasks (i.e., a trusted robot). Thus, developers should first identify the appropriate environmental interaction for any new application. Then, they can determine the appropriate human interaction. To do so, they need to address several questions, such as:

- When the smart devices require human interaction, how should one instruct or train individuals to use them?
- How do users interact with the smart devices (e.g., with a remote control or via a remote location)?
- If a smart device uses the automatic or proactive model, who programs the devices (e.g., users or manufacturers)?
- Do manufacturers notify users when these actions take place?
- Who is responsible if the action causes problems or impacts others negatively?

6.2.2 Semantic Data Selection

Semantic data refers to a set of information that a smart device senses or collects from the environment and may also analyze to provide insight. How the information is represented, displayed, stored, transmitted, searched, or organized is constrained by the types of devices used, which also should be considered and defined based on the goals for the applications. IoT application developers need to consider all variables to decide what to represent and how to present it. For example, if we examine a human's physical activity, heart rate could be one element. However, how should we measure heart rate: number of beats per minute/hour/day, the strength of the heartbeat, the patterns of the heart pulse, or the variations in heart rate? Therefore, we need to clearly understand how we intend to use collected data before designing smart devices intended for human interaction.

6.2.3 Smart Device Design

Smart devices must have properties for identifying, collecting, and displaying data; for transmitting data over appropriate networks; and for sensing, actuation, decision making. Apart from these properties, smart devices must also possess management features, including permissions, updates, liabilities, and restrictions. One could not upgrade early smart home devices through networks or the Internet. Thus, individuals required a new version of the device when an organization developed new features or capabilities. If users can upgrade newer devices through a network connection, does the device do it automatically or must the user activate it? How will users know when their device needs new features or capabilities to improve its security or to minimize privacy issues?

Generally, humans physically interact with smart devices via 1) sight, 2) audio, and/or 3) touch (Fritzsche, 2015). Simple visual displays include a bar graph with data granularity (from simple to complex), time granularity, or comparisons. Complex visual displays include time series, spatial layouts, and abstract displays such as aquatic ecosystems or rain flow designs (Fritzsche, 2015). Consider the following example of different display types when understanding the ways users will interact with smart devices. Smart phones have small interactive screens that require simple visualization for short interactions. Unlike mobile phones, tablets have larger screens with more visualization and feedback capabilities. Laptops have the strongest usability since they have the largest displays, which allow for complex visualization with complex feedback. In designing an application, one must consider the appropriate smart device. In this case, one IoT app device design does not fit all.

6.2.4 Smart Devices' Interaction Levels

Depending on the IoT application, smart devices may possess up to five interaction levels (see Table 2) (Hernandez & Reiff-Marganiec, 2014). IoT app developers must consider the appropriate interaction levels when creating effective and secure IoT apps again since one IoT app design does not fit all. All smart devices must have at least the first two levels of interaction to be "smart".

Table 2. Five Levels of Interaction for Smart Devices (Hernandez & Reiff-Marganiec, 2014)

	Name	Description / examples
Level 1	Essential	In this level, all smart devices must have essential capabilities including digital identification, communications, retention, and energy harvesting. For example, a smart key always allows a user to track the key's location.
Level 2	Networked	Every smart device must also possess programming, processing, and networking capabilities so that it can collect and share data while one controls it remotely. Smart devices that require networked capabilities include devices that control lighting or doorbell videos via Wi-Fi.
Level 3	Enhanced	In this level, smart devices should be able to sense data, log data, and actuate data changes. For example, a smart plate can sense food and provide critical information on eating behavior.
Level 4	Awareness	More advanced smart devices have self-awareness, environment awareness, and human awareness. For example, smart air conditioning senses the number of people in a room and adjusts the temperature accordingly to provide comfort without any human interaction. A smart vehicle with headlights that turn on based on poor lighting conditions exemplifies a smart device with environment awareness
Level 5	IoT complete	When a smart device includes all five levels, it offers the best human-centered IoT design capabilities. Under this best design, a smart device has social readiness and self-management. A smart refrigerator that inventories all products, orders replacements for expired products, and notifies the owner exemplifies a smart device with all five levels.

6.2.5 IoT Application Trustworthiness

Users develop a level of trust in any computer application based on their perceptions about security and privacy. Therefore, the "trustworthiness" of an IoT application may be the most important user issue (Lindqvist & Newman, 2017). In Section 4, we discuss the technical issues of IoT privacy and security including infrastructure threats, regulations, privacy, and manufacturing compliances. In this section, we focus on IoT trustworthiness from the user perspective.

According to Dhillon, Carter, Abed, and Sandhu (2016), studies on IoT security and privacy focus mainly on security's technical aspects but not on the human perspective. Dhillon and Torkzadeh (2006) explain that designers should first understand users' expectations, values, and beliefs before developing the technical requirements to ensure product acceptance. As designers develop smart devices, they must identify and mitigate security and privacy risks based on the different characteristics of the human interactions with the IoT applications and how they expect people to use smart devices. If users do not recognize issues such as their responsibilities, smart device management and maintenance, and who does updates, installs security patches, or replaces faulty devices, they will become uncertain and dissatisfied.

In their study, Dhillon et al. (2016) identified mechanisms to ensure IoT trust, which developers have a fundamental and moral obligation to provide. An example includes "ensure security of personal data on public databases and also maximize IoT data integrity" (p. 9). To ensure that users use IoT apps properly, designers must design technologies to encourage trustworthiness. Developers will need to increase IoT consumer trust to ensure they trust in and use IoT products in the future. As we mention above, Agarwal and Dey (2016) point out that, since research into the IoT's impact on humans remains its in nascency, we need much more research in this area.

6.3 Human Interaction and IoT Research Opportunities

In this section, we highlight five specific categories on how humans interact with the IoT devices and applications, which developers should consider during design. These same five categories also provide opportunities for IS research, especially in human-computer interaction (HCI) and human factors.

Research should identify how person-centric, home-centric, or city-centric environmental interactions differ and ways to improve the tool-based, automatic, and proactive interaction models. As we mention above, research should help developers, researchers, and users to clearly understand how they intend to use the data they collect before designing the smart devices intended for human interaction. Researchers should conduct experiments on the pros and cons of the three ways humans physically interact with smart devices (i.e., via sight, audio, and touch) to create a best-case scenario for different application types. Researchers could map applications and different types of smart devices against the five levels of IoT device interaction, which could become a standardized guide for developers. One would need to classify any new IoT application and then design it based on its appropriate level of human interaction. And, finally, as Dhillon et al. (2016) clarified, we need more research to understand the different characteristics of human interactions before designers make technical design decisions.

Some other research opportunities exist as well. One interesting research area involves the human interaction with IoT sensemaking. Jennex (2017) has proposed a revised "knowledge pyramid" to include the IoT and big data analytics. The original knowledge pyramid described relationships among data, information, knowledge, and wisdom. Jennex found that IoT sensors result in two separate layers of data: 1) traditional operational or transactional data and 2) new massive sets of data from multiple environments. This research will have a strong impact on knowledge management (KM) research. Another interesting research area in the health IoT domain involves using different types of sensors that patients use and that reside in them to provide immediate feedback to doctors and other healthcare specialists concerning patient behavior. A recent example includes a "digital drug", which the U. S. Food and Drug Administration approved in 2017, that lets doctors know if patients have taken their prescribed medicines. The medicine has an embedded sensor that reacts with stomach fluid and sends an electrical signal to a wearable patch on the patient's body. The patch then sends the signal to the patient's smartphone, which notifies their doctor (Ozdemir & Hekim, 2017).

User awareness issues probably represent the most critical issues that researchers need to investigate and address. To solve these issues, we need to determine the social, cultural, and behavioral impacts of IoT development and use. Shin (2014) used a socio-technical framework in a case study to predict how IoT would develop in Korea. His promising research represents a good start to research human issues, clearly a critical component of successful human-centered IoT. By using a socio-technical perspective, researchers can both uncover new issues while providing design approaches that solve them.

7 Conclusion and Future Directions

The IoT has exploded, and its landscape is vast and complex. Implementing IoT has many challenges. In addition to navigating the security, platform, and data challenges in the IoT space, organizations also need to understand and leverage the ecosystem mindset inherent to its functionality to monetize the IoT. Organizations need to develop IoT platforms and adopting standards, mitigating security and privacy issues surrounding IoT, and understanding the role of data analytics and human interaction with the technology in the IoT space to realize the IoT's full potential and business value. Researchers have begun to develop solutions to solve these challenges and mitigate risks (Lindqvist & Neuman, 2017). We have little doubt that the IoT will only continue to grow in ubiquity, especially as IoT standards organizations and industry groups develop protocols and standards to address security, privacy, architectural, and interoperability challenges. Hence, such protocols and standards will have a ripple effect that will eventually impact all industries and how they manage their communication networks.

In this paper, we highlight different facets and applications of the IoT. In doing so, we also highlight many research issues. Some pivotal research opportunities encompass design science and behavioral science research and span various domains such as people, technology, and organizations evaluating development, implementation, effectiveness, use, analytics, privacy, and security across many different industries. Design science recommendations include designing and developing new artifacts, networks, and capabilities using the IoT such as mesh networks for GPS systems and drone delivery systems. Here, we also make several recommendations for researchers to create new algorithms and data models to handle the increasing data flow with real-time solutions. From a behavioral perspective, several recommendations for research include better understanding how end users use and perceive the IoT and evaluating the adoption lifecycle ranging from non-adoption and adoption to discontinuance. Further, we make recommendations in privacy and security area for to evaluate new vulnerabilities, intellectual ownership, and privacy implications that affect the individual, organizational, and societal levels. We extend privacy research recommendations to also include ethical considerations along with regulatory

compliance and liability issues. From an organizational perspective, we make recommendations to evaluate the IoT ecosystem to help organizations generate business value by saving costs, generating revenue, operating more efficiently, and obtaining a competitive advantage.

As new technologies emerge and integrate with IoT systems, researchers will also need to adapt and be ready to address many new questions in evolving environments. Three other IoT-related research topics that researchers should consider based on emerging innovative technologies include: 1) the convergence of distributed ledger technology (i.e., blockchain) and the IoT; 2) the convergence of edge computing, fog computing, cloud computing, and the IoT; and 3) ethical standards and the IoT.

Significant IoT application design should lead to user trustworthiness. If users do not realize potential issues such as their responsibilities, smart device management and maintenance, and who (user, manufacturer, service provider, etc.) does updates, installs security patches, or replaces faulty devices, they will be wary and dissatisfied. To ensure that users are clear on IoT responsibilities, the IoT requires secure standards for interoperability and connection protocols. For security reasons, IoT developers and service providers must make sure that home LANs are isolated from the Internet and from other connections to ensure adequate privacy and security protection against potential threats. The systems must be resilient and resistant to misuse, and, more importantly, organizations must mandate recalls when they cannot make updates. Along with these design requirements, consumer IoT will also require oversight and liability regulation.

Recently, the IDC has estimated that artificial intelligence (AI) will become the underlying support for major IoT deployments (InItelliPaat, 2019). AI and machine learning identify patterns and make predictions based on gigantic data. Since AI represents the IoT's future, the two will have a tremendous synergistic effect. A Cisco study showed that about 60 percent of IoT project initiatives stall at the proof-of-concept stage and only 26 percent of companies have had an IoT project initiative that they considered a success (ITP, 2017). The Cisco study found that the most successful organizations engage the IoT partner ecosystem at every stage. We believe that researchers should study the IoT from multi-faceted research perspectives for a holistic view (Shim et al., 2019) rather than a silo perspective. Since much of the research remains in its nascence, we have much left to do in the IoT world.

References

AbacusNext. (2018). California Consumer Privacy Act (CCPA) compliance. *AbacusNext*. Retrieved from https://www.abacusnext.com/california-consumer-privacy-act-ccpa-compliance

Agarwal, Y., & Dey, A. K. (2016). Toward building a safe, secure, and easy-to-use Internet of things infrastructure. *Computer*, *49*(4), 88-91.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of things: A survey. *Computer Networks*, *54*, 2787-2805.

BBC. (2015). *Laser can "disable self-drive car"*. Retrieved from https://www.bbc.com/news/technology-34185372

Bondarenko, M. (2016). Industrial IoT innovation. *KaaIoT Technologies*. Retrieved from https://www.kaaproject.org/industrial-iot-innovation

Buchmann, A., & Koldehofe, B. (2009). Complex event processing. *Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik*, *51*(5), 241-242.

Caswell, D., & Dörr, K. (2018). Automated Journalism 2.0: Event-driven narratives. *Journalism Practice*, *12*(4), 477-496.

Columbus, L. (2018). 2018 roundup of Internet of things forecasts and market estimates. *Forbes*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#106ed527d838

Cook, S. (2019). 60+ IoT statistics and facts. *Comparitech*. Retrieved from https://www.comparitech.com/internet-providers/iot-statistics/

Davis, B. (2017). U.S. Navy - Condition based maintenance for aircraft fleet. *Teradata Partners Meeting*. Retrieved from https://static1.squarespace.com/static/5274112ae4b02d3f058d4348/t/5a14f1d6085229dcccf1c763/1511322075935/2017-2-8a.pdf

Davis, C. (2018). Jeep hacking class action lawsuit granted partial certification. *Top Class Actions*. Retrieved from https://topclassactions.com/lawsuit-settlements/lawsuit-news/851554-jeep-hacking-class-action-lawsuit-granted-partial-certification/

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly,13*(3), 319-340.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information systems security in organizations. *Information Systems Journal*, *16*(3), 165-314.

Dhillon, G., Carter, L., Abed, J., & Sandhu, R. (2016). Defining objectives for securing the Internet of things: A value-focused thinking approach. *Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy*.

Eriksson, L., Rossi, M., Shim, J. P., & Sorensen, C. (2019). Business and research perspectives of industrial Internet applications. In R. Ballardini, P. Kuoppamaki, & O. Pitkanen, (Eds.), *Regulating industrial Internet through IPR, data protection and competition law* (pp. 23-46). Netherlands: Kluwer.

Faragardi, H. R., Vahabi, M., Fotouhi, H., Nolte, T., & Fahringer, T. (2018). An efficient placement of sinks and SDN controller nodes for optimizing the design cost of industrial IoT systems. *Software: Practice and Experience, 48*(1), 1893-1919.

Fritzsche, B. (2015). Revealing the invisible: Information visualization in the Internet of things era. In *Proceedings of the Media Informatics Advanced Seminar on Human Computer Interaction in the Internet of Things Era* (pp. 18-25).

FTC. (2013). Internet of things—privacy and security in a connected world. *Federal Trade Commission.* Retrieved from https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

Gartner. (2019). *Magic quadrant for industrial IoT platforms.* Retrieved from https://www.gartner.com/doc/reprints?id=1-6QBCEWR&ct=190523&st=sb

Hasan, M. (2019). Choose the right IoT platform: Top 20 IoT cloud platforms reviewed. *UbuntuPIT.* Retrieved from https://www.ubuntupit.com/choose-the-right-iot-platform-top-20-iot-cloud-platforms-reviewed/

Hernandez, M. E. P., & Reiff-Marganiec, S. (2014). Classifying smart objects using capabilities. In *Proceedings of the International Conference on Smart Computing*.

Hossain, M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the Internet of things. In *Proceedings of the IEEE World Congress on Services.*

Hui, G. (2014). How the Internet of Things changes business models. *Harvard Business Review*. Retrieved from https://hbr.org/2014/07/how-the-internet-of-things-changes-business-models

IntelliPaat. (2019). How AI is used in IoT? June 20. Retrieved from https://intellipaat.com/blog/ai-used-iot/

ITP. (2017). *Cisco: 60% of IoT projects staff at PoC stage*. Retrieved from www.itp.net/612937-cisco-60-of-iot-projects-stall-at-poc-stage.

Jennex, M. E. (2017). Big data, the Internet of things, and the revised knowledge pyramid. *ACM SIGMIS Database*, *48*(4), 69-79.

Kamilaris, A., & Pitsillides, A. (2016). Mobile phone computing and the Internet of things: A survey. *IEEE Internet of Things Journal*, *3*(6), 885-898.

Koreshoff, T. L., Leong, T. W., & Robertson, T. (2013). Approaching a human-centered Internet of things. *In Proceedings of the 25th Australian Computer-Human Interaction Conference.*

KOS. (2016). Hacked cameras, DVRs powered today's massive Internet outage. *Krebs On Security*. Retrieved from https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Kreps, J., Narkhede, N., & Rao, J. (2011). KAFKA: A distributed messaging system for log processing. In *Proceedings of NetDB.*

Kumar, S., & Chaurasiya, V. (2019), A strategy for elimination of data redundancy in Internet of things (IoT) based wireless sensor network (WSN). *IEEE Systems Journal*, *13*(2), 1650-1657.

Laskowski, N. (2015). Ten analytics success stories in a nutshell. *SearchCIO TechTarget*. Retrieved from http://searchcio.techtarget.com/opinion/Ten-analytics-success-stories-in-a-nutshell.

Leeuw, K. D., & Bergstra, J. (2007). *The history of information security: A comprehensive handbook*. Amsterdam, Netherlands: Elsevier.

Lindqvist, U., & Neuman, P. G. (2017). Inside risks: The future of the Internet of things. *Communications of the ACM*, *60*(2), 26-30.

MacGillivray, C. (2016). *The platform of platforms in the Internet of things.* Retrieved from https://iotslam.com/wp-content/uploads/2016/06/IDC-Study-IoT-Platform-of-Platforms.pdf

Marjani, M., Nasaruddin, F., Abdullah, G., Karim, A., Hashem, I., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, *5*, 5247-5261.

Nadeau, M. (2018). General Data Protection Regulation (GDPR): What you need to know to stay compliant. *CSO*. Retrieved from https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

Newman, P. (2019). IoT report: How Internet of things technology growth is reaching mainstream companies and consumers. *Business Insider*. Retrieved from https://www.businessinsider.com/internet-of-things-report?IR=T

Nguyen, M.-A. (2015). Designing smart interactions for smart objects. In *Proceedings of the Media Informatics Advanced Seminar on Human Computer Interaction in the Internet of Things Era*.

Omnim2m. (2015). *IoT applications: Changing and influencing business behavior*. Retrieved from http://omnim2m.com/iot-applications-changing-influencing-business-behavior

Ozdemir, V., & Hekim, N. (2017). Birth of Industry 5.0: Making sense of big data with artificial intelligence, the Internet of things, and next-generation technological policy. *OMICS: A Journal of Integrative Biology*, *22*(1), 65-76.

Patten, K., Regan, E., & Wu, D. (2018). A systems perspective on how physicians can use IoT to improve coordination of care. In *Proceedings of the 10th Pre-ICIS Conference Workshop on Changing Nature of Work.*

Raymond, D. R., Marchany, R. C., Brownfield, M. I., & Midkiff, S. F. (2009). Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE Transactions on Vehicular Technology*, *58*(1), 367-380.

Robertson, J. (2012). $30 device available online blamed for spike in car thefts in Queensland. *Courier Mail*. Retrieved from https://www.couriermail.com.au/news/queensland/device-available-online-blamed-for-spike-in-car-thefts-in-queensland/news-story/93d962758b3c5d27c81f4065bb9ab5c1

Roscher-Nielsen, N., Ratliff, E., Rudy, G., & Petroules, J. (2017). *Internet of things and security* (panel discussion). QT.

Rullo, A., Serra, E., Bertino, E., & Lobo, J. (2019). Optimal placement of security resources for the Internet of Things. In F. Cicirelli, A. Guerrieri, C. Mastroianni, G. Spezzano, & A. Vinci, (Eds.), *The Internet of things for smart urban ecosystems.* Berlin: Springer.

Ryan, D. (2013). *High performance discovery in time series: Techniques and case studies*. Berlin: Springer.

SAP TV. (2016). *All aboard the IoT express* (video). Retrieved from https://www.youtube.com/watch?v=-522lNMapnI

Sharda, R., Delen, D., & Turban, E. (2019). *Analytics, data science, & artificial intelligence: Systems for decision support* (11th ed.).New York, NY: Pearson.

Shearer, C. (2000). The CRISP-DM model: The new blueprint for data mining. *Journal of Data Warehousing*, *5*(4), 13-22.

Shin, D. (2014). A socio-technical framework for Internet-of-things design: A human-centered design for the Internet of things. *Telematics and Informatics*, *31*(4) 519-531.

Shim, J. P. (2019). Cyber-physical systems and industrial IoT cybersecurity: Issues and solutions. In *Proceedings of 25th Americas Conference on Information Systems*.

Shim, J. P., Dam, R., Coursey, C., & Barnes, D. (2017a). Internet of things (IoT): Overview, monetizing, devices efficiency, platforms and security. In *Proceedings of the Wireless Telecommunication Symposium.*

Shim, J. P., Avital, M., Dennis, A., Sheng, O., Rossi, M., Sorensen, C., & French, A. (2017b). Internet of things: Opportunities and challenges to business, society, and IS research. In *Proceedings of 38th International Conference on Information Systems*.

Shim, J. P., Avital, M., Dennis, A., Rossi, M., Sorensen, C., & French, A. (2019). The transformative effect of the Internet of things on business and society. *Communications of the Association for Information Systems*, *44*, 129-140.

Smee, J. (2018). 5G NR theory and practice. In *Proceedings of the Wireless Telecommunication Symposium.*

Smith, J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Son, J., Lee, H. K., Jin, S., & Lee, J. (2019). Content features of tweets for effective communication during disasters: A media synchronicity theory perspective. *International Journal of Information Management*, *45*, 56-68.

Takefuji, Y. (2018). Connected vehicle security vulnerabilities. *IEEE Technology and Society Magazine*, *37*(1), 15-18.

Teradata. (2015). *The Internet of trains*. Retrieved from http://assets.teradata.com/resourceCenter/downloads/CaseStudies/EB8903.pdf

U.S. Chamber of Commerce. (2017). *The IOT revolution and our digital security: Principles of IoT security.* Retrieved from http://scglegal.com/meetings/denver/TR%201550%20PP%20-20The.IoT.Revolution.Our.Digital.Security.Final%20002%20WILEY%20REIN.pdf

Westerlund, M., Leminen, S., & Rajahonka, M. (2014). Designing business models for the Internet of things. *Technology Innovation Management Review*, *4*(7), 5-14.

Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*, *26*(1), 97-107.

Appendix A: Low Power Wide Area Network

Low-power wide area network has two spectrum types: unlicensed and licensed. The difference between these technology types include the radio spectrum that the technologies use (unlicensed versus licensed) and the commercial strategies that companies use. Several major technologies and standards are key players and competitors in the unlicensed spectrum (i.e., Sigfox, LoRaWAN, Ingenu.) Other technologies and standards are key players in licensed spectrum (i.e., LTE CAT-M1, EC-GSM, LTE CAT-M2) (Kamilaris & Pitsillides, 2016; Shim et al., 2017b). Organizations can deploy LTE CAT-M1 in existing LTE bands (i.e., compatible in existing LTE networks). LTE "CAT-M2" or NarrowBand IoT (NB-IoT) technology costs less than LTE CAT-M1.

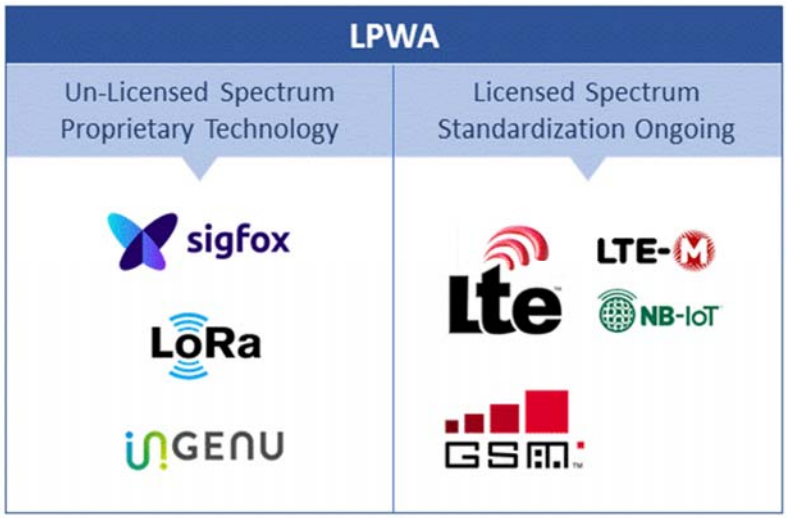

Figure A1. LPWA

Appendix B: 5G New Radio, Network Slicing, and Diverse Spectrum

According to several recent global mobile industry reports, such as the 3rd Generation Partnership Project (3GPP), the 5G cellular standard is 100 times faster than the 4G LTE standard currently available (Smee, 2018). We require 5G speeds and low latencies (i.e., 5G mobile systems, mobile terminal device with massive multiple-input-multiple-output (MIMO) antenna array multi-gigabit downlink speeds, and latencies as low as 1 millisecond) to meet the increasing connectivity requirements for high reliability and low latency services. 5G new radio (NR) evolves the orthogonal frequency division multiplexing (OFDM) of 4G into an adaptable and scalable waveform framework. Network slicing for enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLCs), and massive machine-type communications (mMTCs) represents a key technology for 5G. 5G diverse spectrum (mmWave, Sub-6 GHz, Sub-GHz) should be maximized all bands.

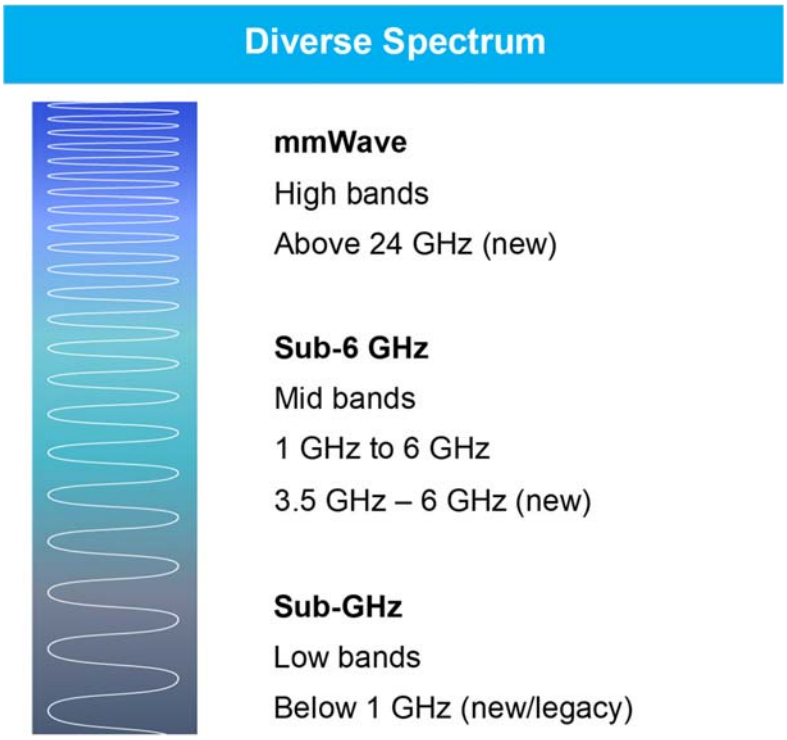

Figure B1. Diverse Spectrum

About the Authors

J. P. Shim is CIS faculty and KABC Director at Georgia State University and Adjunct Professor (dual appointment) at Georgia Tech. He was Professor, Notable Scholar, John Grisham Professor at Mississippi State University before joining GSU in 2011. He is Professor Emeritus at MSU. He received the PhD degree from the University of Nebraska-Lincoln, the MBA from Seoul National University, and completed IT Executive Education (invited) at Harvard Business School. He published several books and 100+ papers in big data and analytics, IoT, cybersecurity, kinetic threats, BYOD, social networking, AR/VR, and decision support technology in journals. He was the principal investigator for the National Science Foundation and has received grants from Microsoft, US Small Business Administration, ROK National IT Industry Promotion Agency, Japan Foundation, and Mississippi IHL. He worked as a consultant for Booz Allen, U.S. EPA, Kia Motors, and telecommunication companies. He has served as Wireless Telecom Symposium/IEEE Program Chair for 15 years and is faculty advisor for GSU Robinson Graduate Consulting Club.

Ramesh Sharda is Vice Dean for Research and Graduate Programs in the Spears School of Business at Oklahoma State University. His research has been published in major journals in management science and information systems including *Management Science*, *Operations Research*, *Information Systems Research*, *Decision Support Systems*, *Decision Science Journal*, and many others. He has coauthored two textbooks (*Business Intelligence, Analytics, and Data Science: A Managerial Perspective*, 4th Edition, Pearson, and *Analytics, Data Science, and Artificial Intelligence: Systems for Decision Support*, 11th edition, Pearson). He also serves as the Faculty Director of Teradata University Network, a worldwide portal for sharing teaching and learning resources in analytics and data science. He is a fellow of INFORMS.

Aaron M. French is an Associate Professor of Management Information Systems in the College of Business at the University of New Mexico. He received his PhD in Business Information Systems at Mississippi State University. He is active in software development and the evaluation emerging technologies. His research has been published in the *Journal of Information Technology*, *Decision Support Systems*, *Information & Management*, *Information Technology & People*, *Behaviour & Information Technology*, *Journal of Computer Information Systems*, *Communications of the Association for Information Systems*, and *Pacific Asian Journal of the Association of Information Systems*. His research interests include social networking, blockchain, cross-cultural studies and emerging technologies.

Rhonda A. Syler is Information Systems faculty and Associate Director of Enterprise Systems in the Sam M. Walton College of Business at the University of Arkansas. She teaches and conducts workshops worldwide in business analytics, enterprise resource planning, systems development, and blockchain. Her research focuses on the business value and organizational, security, and societal impacts of disruptive technologies such as Internet of Things (IoT) and Blockchain. Her interests include smart city design and development including autonomous and connected vehicles (AV/CV) and 5G. Examples of her work in this space include co-developing an Internet of Things Lab designed to provide a learning and innovation environment for big data, security, ERP, mobile development, and cloud computing and working on data- and analytic-driven curriculum projects with Fortune 500 companies.

Karen P. Patten, an Integrated Information Technology faculty member in the College of Engineering and Computing at the University of South Carolina, teaches telecommunications, networking, and IT project management. She received her PhD in Information Systems at the New Jersey Institute of Technology. She has published several books on managing IT within small businesses and an introductory IT ebook, *Thriving in the Age of Digital Disruption*. Her research has been published in *Information Management and Computer Security*, *Communications of the Association for Computing Machinery, and Communications of the Association for Information Systems.* Her research interests include executive IT management of disruptive technologies, IoT development, small business emerging wireless and mobile telecommunications management, and IT curriculum development.