Expert Systems With Applications 133 (2019) 97–108

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Review

The Internet of Things: Review and theoretical framework

Jeretta Horn Nord [a], Alex Koohang [b,*], Joanna Paliszkiewicz [c]

[a] Management Science and Information Systems Department, Oklahoma State University, Stillwater, OK 74078, USA
[b] Middle Georgia State University, Macon, GA 31206, USA
[c] Warsaw University of Life Sciences, Warsaw, Poland

ARTICLE INFO

Article history:
Received 2 March 2019
Revised 12 May 2019
Accepted 12 May 2019
Available online 13 May 2019

Keywords:
Internet of Things
IoT
IoT literature review
IoT priorities
IoT challenges
IoT theoretical framework

ABSTRACT

The Internet of Things (IoT) global arena is massive and growing exponentially. Those in the emerging digital world have recently witnessed the proliferation and impact of IoT-enabled devices. The IoT has provided new opportunities in the technology arena while bringing several challenges to an increased level of concern. This research has both practical and theoretical impetus since IoT is still in its infancy, and yet it is considered by many as the most important technology initiative of today. This study includes a systematic review and synthesis of IoT related literature and the development of a theoretical framework and conceptual model. The review of the literature reveals that the number of applications that make use of the IoT has increased dramatically and spans areas from business and manufacturing to home, health care, and knowledge management. Although IoT can create invaluable data in every industry, it does not occur without its challenges. The theoretical framework developed identifies IoT priority areas and challenges, providing a guide for those leading IoT initiatives and revealing opportunities for future IoT research.

1. Introduction

Executives believe the Internet of Things (IoT) to be the most important emerging technology, ranking it above others such as artificial intelligence and robotics (Insights Team, 2017e). Burrus (2014, par. 13) agrees, stating "Of all of the technology trends that are taking place right now, the biggest one is the Internet of Things; it's the one that's going to cause the most disruption as well as provide the most opportunity over the next five years." IoT has gained ground around the globe verified by a study published in Forbes Insights of more than 500 executives based in Europe, the Americas, and Asia-Pacific - representing a range of industries from companies with at least 500 employees. Ninety percent of surveyed executives who are leading IoT initiatives (Insights Team, 2017c) indicated that IoT will be important to the future of their business. Insights Team (2017d) reported that about 30 billion devices could be in play by 2020, and by 2025, the number could top 75 billion. Lund, MacGillivray, Turner, and Morales (2014) expect the worldwide market for IoT solutions to grow to $7.1 trillion in 2020. This revenue forecast encompasses the full breadth of the IoT ecosystem including intelligent and embedded systems shipments, connectivity services, infrastructure, purpose-built IoT platforms, applications, security, analytics, and professional services. Irrespective of the variation in numbers, all predictions point to tremendous growth in IoT adoption and usage.

With the IoT considered a disruptive emerging technology, yet an extremely important one, we believe that a comprehensive review inclusive of IoT priority areas and challenges will provide an integrated perspective of the IoT and serve as a repository for the accumulated knowledge. The goal is to synthesize the existing IoT literature to inform an understanding of the IoT. Building on this knowledge, we will provide a theoretical framework and conceptual model including the IoT adoption and implementation guide for practitioners and directions for future research.

Our review presents an analysis of IoT including proposed definitions, architectures, applications, and impact. Drawing from this extensive review, priority areas and challenges are identified as well as gaps in the literature, which provided substantive directions for a new theory. The theory, labeled "Theoretical Framework and Conceptual Model for IoT Adoption and Implementation", is discussed in detail. The paper is organized as follows: Foundations, boundaries, and research approach are addressed followed by an extensive review and analysis of the IoT literature. Based on this analysis, the theoretical framework and conceptual model are presented, and contributions of the theory are discussed.

* Corresponding author.
E-mail addresses: jeretta.nord@okstate.edu (J.H. Nord), alex.koohang@mga.edu (A. Koohang), joanna_paliszkiewicz@sggw.pl (J. Paliszkiewicz).

https://doi.org/10.1016/j.eswa.2019.05.014
0957-4174/

2. Foundations, boundaries, and approach

The Internet was developed with data created by people, while the IoT is about data created by things (Madakam, Ramaswamy, & Tripathi, 2015). Webster and Watson (2002) recommended that the literature review followed a concept-centric approach and the concepts determined the organizing framework of the review. Our literature review was not limited by publication outlet. While the focus was on the IoT, literature related to IoT priority areas and challenges determined through the literature review was used for supporting research and to aid in the development of the theoretical framework and conceptual model. We used Leidner and Kayworth (2006) approach as an example when developing a strategic approach to search literature related to IoT, selecting those studies to be included in the literature review and for the analysis and synthesis. A five-step approach was used to identify relevant literature: First, using the key terms *Internet of Things* and *IoT*, a database search of Google Scholar, and because of the nature and timeliness of the topic, Google was also searched for *IoT* business related literature including those with research results. Practitioner papers from reputable sources were included in the review because of the topic, the importance of currency, and the paucity of IoT empirical studies. In most cases, there was conformity between the concept papers and research papers reviewed. Second, an electronic search of each issue of each volume of the leading journals in the IS field (AIS Senior Scholars' Basket of Eight, 2011) was searched. Third, a search of scholarly academic databases was conducted for articles identified with the keywords *Internet of Things* and *IoT*. Fourth, articles listed in the references of key articles were viewed and relevant papers were selected for inclusion (Webster & Watson, 2002). Fifth, related topics identified through the literature analysis were selected as focal points including the top three functions - customer experience, finance, and asset management. These functions are viewed as IoT priority areas. Furthermore, based on the identified literature analysis, three areas providing IoT challenges - privacy, security, and trust - were searched using keywords related to these topics.

Given that the IoT is an emerging technology, research-based literature is somewhat limited so the majority of identified IoT articles, publications, and conference papers were included. Selected papers related to the focal points were also included. Those not included were due to the irrelevance or indirect relationship to the theme of the paper.

3. Literature review and synthesis

"A review of prior, relevant literature is an essential feature of any academic project. An effective review creates a firm foundation for advancing knowledge. It facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed (Webster & Watson, 2002, p. XIII)." Although a great deal has been written on concepts related to the IoT, there is a critical shortage of papers on IoT research-based studies and IoT literature reviews. Theory as related to IoT adoption and implementation appears to be non-existent. In Table 1 we show the IoT concept matrix and paper classification of the relevant papers reviewed. We used Webster and Watson (2002) Concept Metrix to develop the IoT concepts. The concepts were IoT overview, IoT architecture, IoT applications, IoT challenges, IoT priorities, theory, and other. The paper classifications were concept, research, and review.

As can be seen in Table 1, research-based and review literature are limited. A synthesis of our review to identify research-based studies and key issues/challenges in the IoT literature resulted in the following. Issues with trust management design, development, and solutions in IoT (Alshehri, Hussain, & Hussain, 2018; Bao, Chen, & Guo, 2013; Chen et al., 2011; Chen, Guo, & Bao, 2016; Insights Team, 2017c; Kowshayla & Valarmathi, 2017; Saied, Olivereau, Zeghlache, & Laurent, 2013), issues with standards, mobility support, authentication, influencing consumers' perception of usage benefits, adoption and/or privacy (Atzori, Iera, & Morabito, 2010; Hsu & Lin, 2016, 2018; Insights Team, 2017c; Jayaraman, Yang, Yavari, Georgakopoulos, & Yi, 2017; Lund et al., 2014; Malina, Hajny, Fujdiak, & Hosek, 2016); issues with structured list of IoT segments (Bartje, 2016); issues with mining Twitter to understand the public's perception of the IoT (Bian et al., 2016); issues with customer experience, finance, asset management, product development, environment & safety, supply chain, manufacturing, warehousing and logistics (Insights Team, 2017c); issues with security and security regulations (Koo & Kim, 2017; Lund et al., 2014; Luo, Ma, & Gao, 2016); issues with smart smartphone adoption behavior (Kim, Chun, & Lee, 2014); significance of Google, Twitter, and LinkedIn on conversations among people (Leuth, 2015); challenges of standards, global scalability, identifying priorities (Lund et al., 2014), issues with reuse of existing IoT sensors using negotiating agents (Mišura & Žagar, 2016), challenges and issues with using IPsec as a security mechanism for the IoT (Raza, Duquennoy, Höglund, Roedig, & Voigt, 2014).

In addition, the topics reviewed are IoT and supply chain management (Ben-Daya, Hassini, & Bahroun, 2017); trust computation models for service management in the IoT systems (Guo, Chen, & Tsai, 2017); culture in information systems research (Leidner & Kayworth, 2006); IoT overview with a focus on architectures and vital technologies (Madakam et al., 2015); Internet of Things applications and research challenges; (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012); value of IoT (Nicolescu, Huth, Radanliev, & Roure, 2018); ubiquitous IT and digital vulnerabilities (Ransbotham, Fichman, Gopal, & Gupta, 2016); security, privacy, and trust in the IoT (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015); theories in the information systems disciplines (Weber, 2012); control configuration and control enactment in information systems projects (Wiener, Mahring, Remus, & Saunders, 2016); and trust management on the IoT (Yan, Zhang, & Vasilakos, 2014).

Although IoT related topics identified in the literature support our theory, there were no papers inclusive of all components considered by the authors in the development of a theoretical framework leading to IoT adoption and implementation and subsequent recommended research. Drawing from IoT concept matrix and paper classification, the IoT key findings/issues/challenges, and the IoT topics, a comprehensive review, and synthesis of existing IoT literature were conducted to generate theoretical insights and implications. As recommended by Webster and Watson (2002), based on the IoT literature analysis, key concepts are presented within the boundaries of the topic, the review's contributions are discussed and explained including an in-depth analysis of IoT priority areas and challenges.

In the next section, our review and analysis of the IoT literature continue to include various definitions of IoT, IoT architecture, IoT applications, priority areas and challenges leading into building the theoretical framework and conceptual model with a discussion of the contributions of the theory.

3.1. Defining IoT

While the term IoT is now widely used, Wortmann and Flüchter (2015) contend that there is no common definition or understanding of what the IoT encompasses. Although there is no *standard* definition for IoT, it has been defined and explained numerous times in the literature (Huang, Craig, Lin, & Yan, 2016; Lund et al., 2014; Insights Team, 2017c; Ben-Daya et al., 2017; Gigli & Koo, 2011; Lee & Lee, 2015; Madakam et al., 2015; Ornes, 2016). The objective of IoT is similar in a broad sense, regardless

Table 1
The IoT concept matrix and paper classification.

Citation	Concepts							Paper classification		
	IoT overview	IoT architecture	IoT applications	IoT challenges	IoT priorities	Theory	Other	Concept paper	Research paper	Review paper
AIS (2011)							X	X		
Alshehri et al. (2018)		X		X					X	
Atzori et al. (2010)		X	X						X	
Baldini, Botterman, Neisse, and Tallacchini (2016)	X							X		
Bandyopadhyay et al. (2013)				X				X		
Bao et al. (2013)				X					X	
Bartje (2016)			X						X	
Ben-Daya et al. (2017)	X						X			X
Bian et al. (2016)				X	X				X	
BITAG (2016)				X				X		
						X		X		
Burrus (2014)	X	X						X		
Chaudhuri and Cavoukian (2018)				X				X		
Chen et al. (2011)				X					X	
Chen et al. (2016)				X					X	
De Leusse, Periorellis, Dimitrakos, and Nair (2012)		X		X				X		
DHS (2014)				X				X		
Fernandes et al. (2017)				X				X		
Fernandes et al. (2017)				X				X		
Gessner et al. (2012)		X		X				X		
Gigli and Koo (2011)			X					X		
Gillett et al. (2018)					X			X		
Gregor (2006)						X		X		
Guo et al. (2017)				X						X
Heer et al. (2011)				X				X		
Hsu and Lin (2016)	X			X					X	
Hsu and Lin (2018)	X			X			X		X	
Huang et al. (2016)				X				X		
Insights Team (2017a)					X			X		
Insights Team (2017b)				X				X		
Insights Team (2017c)	X		X	X	X				X	
Insights Team (2017d)				X				X		
Insights Team (2017e)				X				X		
Jaccard and Jacoby (2010)						X		X		
Javed and Wolf (2012)		X		X				X		
Jay (2018)				X	X			X		
Jayaraman et al. (2017)		X		X					X	
Junilla (2018)					X			X		
Kanuparthi et al. (2013)				X				X		
Kim et al. (2014)							X		X	
Koo and Kim (2017)				X					X	
Kothmayr et al. (2013)		X		X				X		
Kowshalya and Valarmathi (2017)				X					X	
Lee and Lee (2015)	X		X	X				X		
Leidner and Kayworth (2006)						X				X
Liu and Wang (2010)		X		X				X		
Leuth (2015)			X						X	
Lund et al. (2014)	X	X	X	X					X	
Luo et al. (2016)				X					X	

(*continued on next page*)

Table 1 (*continued*)

Citation	Concepts							Paper classification		
	IoT overview	IoT architecture	IoT applications	IoT challenges	IoT priorities	Theory	Other	Concept paper	Research paper	Review paper
Madakam et al. (2015)	X	X								X
Mäkinen (2015)	X			X	X			X		
Malina et al. (2016)				X					X	
Maple (2017)	X		X	X				X		
Marias et al. (2011)				X				X		
Miorandi et al. (2012)			X	X						X
Mišura and Žagar (2016)				X					X	
Nicolescu et al. (2018)	X									X
Ning et al. (2013)		X		X				X		
Ornes (2016)		X		X				X		
Peppet (2014)				X				X		
Perera et al. (2016)				X				X		
Petersen et al. (2014)		X		X				X		
Raferty (2017)					X			X		
Ransbotham et al. (2016)				X						X
Raza et al. (2014)				X					X	
Rekleitis, Rizomiliotis, and Gritzalis (2014)				X				X		
Rivard (2014)						X	X	X		
Roman et al. (2011)				X				X		
Roman et al. (2013)				X				X		
Saied et al. (2013)				X					X	
Samani et al. (2015)				X				X		
Shaikh, Zeadally, and Exposito (2017)		X	X	X				X		
Sicari et al. (2016)		X		X				X		
Sicari et al. (2015)				X						X
Stankovic (2014)	X	X		X				X		
Weber (2012)						X				X
Webster and Watson (2002)							X	X		
Weinberg et al. (2015)				X				X		
Wiener et al. (2016)						X				X
Wortmann and Flüchter (2015)		X	X	X				X		
Yan et al. (2014)				X						X
Ziegeldorf et al. (2014)				X				X		

Table 2
Components of various architecture model.

Architecture model	Components
European FP7 research project	• Leaves – Enables the creations of a maximal set of interoperable IoT systems • Trunk – Potentially necessary set of enablers or building • Roots – Interoperable technologies
International Telecommunications Union (ITU) architecture	• Sensing layer • Access layer • Network layer • Middleware layer • Application layer
IOT forum architecture	• Applications • Transportation • Processors
Qian Xiaocong, Zhang Jidong architecture	• Application layer • Transportation layer • Perception layer
Kun Han, Shurong Liu, Dacheng Zhang, and Ying Han architecture	• Near field communication • Network equipment management • High-speed internet

of variations in the definition. In general, IoT is about a network of networks of uniquely identifiable endpoints or "things" that capture and share data. For this paper, we chose the following IoT definition: "… the interconnection of machines and devices through the internet, enabling the creation of data that can yield analytical insights and support new operations. Insights Team (2017c, p. 4)" The IoT is composed of a multilayer stack of technologies that make up its architecture. To further an understanding of the IoT, a review of IoT architecture is imperative.

3.2. IoT architecture

"Technical specifications and reference architectures for IoT (systems of) systems are far from being completed and standardized (Nicolescu et al., 2018, p. 355)." Typical IoT communication architectures enable IoT devices to not only connect to the communication backbone - the Internet - using an infrastructure-based wireless network paradigm but also to communicate with one another autonomously (Petersen, Baccelli, Wählisch, Schmidt, & Schiller, 2014). Although there is no proposed standard for IoT architecture, Madakam et al. (2015) presented five architects or models developed by researchers, authors, and practitioners. Components included in each architecture model are listed in Table 2.

Although there are slight differences in the architectural models, an IoT system generally contains three layers: a *physical perception layer* that perceives physical environment and human social life; a *network layer* that transforms and processes perceived environment data; and an *application layer* that offers context-aware intelligent services in a pervasive manner (Yan et al., 2014). Wortmann and Flüchter (2015) also describe the combination of multiple software and hardware components in a multilayer stack of IoT technologies composed of three core layers, i.e., the thing or device layer, the connectivity layer, and the IoT cloud layer. Bandyopadhyay, Balamuralidhar, and Pal (2013) offer an explanation of each indicating that architecturally, IoT consists of three layers: the device layer which is the basic infrastructure of IoT that uses technologies such Radio Frequency Identification (RFID), Near Field Communication (NFC), wireless sensor networks, and embedded intelligence; the connection layer which includes gateways and the core network; and the application layer which is comprised of objects that are sensor equipped. Burrus (2014) points out that sensors measure, evaluate, and gather data. IoT comes together with the connection of sensors and machines. Furthermore, cloud-based applications are the key to using leveraged data. The IoT doesn't function without cloud-based applications to interpret and transmit the data coming from multiple sensors. Drawing from this research, a simplified IoT architectural model was developed. See Fig. 1. While the architecture is important for a complete understanding of IoT and to IoT development teams for the implementation and maintenance of IoT, researchers and practitioners are likely to have a greater interest in IoT applications.

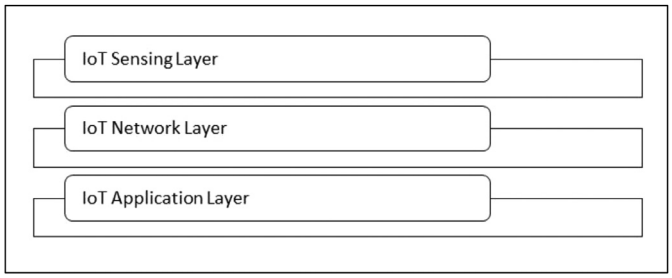

Fig. 1. IoT architectural model.

3.3. IoT applications

IoT applications are applicable to a massive number of areas ranging from personal to 'big' business. Lee and Lee (2015) support this notion, stating that the IoT facilitates the development of a myriad of industry oriented and user-specific IoT applications. Whereas devices and networks provide physical connectivity, IoT applications enable device-to-device and human-to-device interactions in a reliable and robust manner. Atzori et al. (2010) grouped IoT applications into four broad domains: Transportation and logistics, healthcare, smart environment (home, office, plant), and personal and social domain. Lee and Lee (2015) listed the *leading* four industries in terms of IoT value according to their research as manufacturing, retail trade, information services, finance, and insurance. In a study of 500 senior executives worldwide who were leading IoT initiatives, results revealed the extent of the importance of IoT applications within areas of their organizations (Insights Team, 2017e). Energy, financial services, healthcare, and manufacturing came in at the top of the list (see Table 3).

In a study regarding IoT applications, Lueth (2015) measured three things: What people search for on Google, what people talk about on Twitter, and what people write about on LinkedIn. The top 10 application categories were then ranked. This study found smart home, wearables, and smart city to be the top three categories. Bartje (2016) verified 640 actual enterprise-IoT projects and categorized the top 10 applications of IoT segments. Connected industry, smart city, and smart energy were top on the list of real IoT

Table 3
Top IoT application areas identified by study.

Atzori et al. (2010)	Lee and Lee (2015)	Insights Team (2017c)	Lueth (2015)	Bartje (2016)
Transportation and logistics	Manufacturing	Energy	Smart home	Connected industry
Healthcare	Retail trade	Financial services	Wearables	Smart city
Smart environment (home, office, plant)	Information services	Healthcare	Smart city	Smart energy
Personal and social	Finance and insurance	Manufacturing	Smart grid	Connected car
		Retail	Industrial internet	Other
		Information technology	Connected car	Smart agriculture
		Telecom	Connected health	Connected building
		Transport	Smart retail	Connected health
			Smart supply chain	Smart retail
			Smart farming	Smart supply chain

project areas. Table 3 shows the application areas identified by researchers to be of importance in the IoT arena (Atzori et al., 2010; Lee & Lee, 2015; Insights Team, 2017c; Bartje, 2016; Lueth, 2015).

Although the IoT is an emerging technology, it covers a broad spectrum of application areas and impacts a significant percentage of the population. Wortmann and Flüchter (2015) confirm this, indicating that the fields of application for IoT technologies are as numerous as they are diverse, as IoT technologies are increasingly extending to virtually all areas of everyday life.

As noted, IoT impacts almost every area of our lives, however, Bian et al. (2016) analyzed Twitter posts on the IoT for the period 2009–2015 and found that business and technology were the main areas of interest as they relate to IoT. Wortmann and Flüchter (2015) support this finding indicating that the most prominent areas of application are the smart industry with the development of intelligent production systems and connected production sites. Based on these findings, the focus from this point onward will be on IoT in a business environment.

3.4. Priority areas

In contrast to challenges, only a handful of articles consider *functions* perceived as high priority areas for IoT initiatives. A survey of 500 executives worldwide who were leading IoT initiatives within their companies asked to identify the *functions* they see as the highest priorities for IoT. Findings revealed that IoT is affecting many parts of organizations, but the top three priority areas are customer experience, finance, and asset management (Insights Team, 2017e).

First on the list of priority areas and one of the most broadly applicable manifestations of the IoT is in its potential to help organizations improve the customer experience. Gillett, Truog, van den Brink-Quintanilha, Matzke, and Gunderson (2018) offer four ways that IoT can help improve the customer experience:

- Monitor and improve customer experiences with company offerings.
- Personalize the situation for each specific customer.
- Improve and learn over time via automated updates to products and services.
- Reinvent product access and purchase.

"It's hard to overstate the value of delivering an excellent customer experience... Considering the proven value of loyal customers and the high cost of acquiring new ones, it only makes sense to keep them happy. The IoT can help." (Raferty, 2017, para. 1–2).

The second priority area is financial decision making. Jay (2018) suggests that the IoT will make it significantly easier for CFOs to measure and monitor business performance in a timely manner to ensure that their organization can respond to events in an agile fashion with data flowing into billing, enterprise resource planning, and accounting systems in real time. "The IoT can play an important role in financial decision making by providing real-time visibility that complements data from enterprise resource planning (ERP) and accounting systems and allows for a more holistic view of the enterprise (Insights Team, 2017a, para. 13)". Jay (2018) stresses that finance functions have already gained significant experience in data collection and predictive analytics, but they need to have an understanding and strategies in place to exploit IoT technology or risk falling behind those who have. The CFO should work with the CIO to make this happen.

The third area identified as being a high priority area for executives is asset tracking and management. IoT is changing asset management. Junnila (2018) explains asset management as the process of keeping track of a company's physical assets. Depending on the business, this could be equipment, computer devices, tools, or vehicles, for example. Utilizing IoT sensors attached to assets, companies can actively track information about their assets without human involvement. Further, wireless sensor networks (WSN) can cooperate with RFID systems to better track the status of things such as asset location, temperature, movements, and efficiency of equipment (Lee & Lee, 2015; Insights Team, 2017a; Atzori et al., 2010).

Top priority areas may vary depending on the industry, but those identified in the literature (customer experience, finance, and asset management) provide a foundation of functional areas for researchers and practitioners to evaluate. While we selected three functional areas as priority areas, clearly there are numerous others. IoT priority areas serve as one of the focal points of this paper and are considered *constructs* in the development of the theoretical framework. Others have identified the benefits or value of IoT (Nicolescu et al., 2018; Ornes, 2016), but not prioritized them which is important to those leading IoT initiatives. As important as it is to determine priority areas when implementing the IoT, related challenges cannot be ignored.

3.5. Challenges

"Every wave of technology adoption has its challenges, and IoT is no exception (Insights Team, 2017c, p. 9)." IoT based solutions are typically made up of several technologies, creating an environment that is complex and rapidly changing. The top five challenges identified by Insight Team, 2017c, p. 5) with *building out* IoT capabilities are "… investment, keeping the IoT secure, cross-department cooperation, integration of disparate data, and availability of skilled staff."

Insight Team (2017d) identified four challenges often encountered when *managing* IoT technologies. These are:

- Integrating new technologies into existing technologies.
- Managing complexity: Protocol proliferation.
- Bringing data from the edge: networking challenges.
- Too few best practices in the evolving area of IoT (Insights Team, 2017d)

Building out and managing IoT does not happen without challenges, but of significant concern and recurring throughout the IoT literature, are issues of privacy, security, and trust. Labeled as 'Challenges' and identified as *associations* in the development of the theoretical framework, privacy, security, and trust are discussed in further detail.

3.5.1. Privacy and security

IoT is seen as part of the future of virtually every industry from healthcare to financial services to transportation. The IoT is dependent upon sensors, wireless communications, networks, cloud, storage, software, etc. (Insights Team, 2017c) escalating concerns about privacy, security, and trust. Lund et al. (2014) support these concerns indicating that so much has *not* been raised and resolved formally around privacy and security within an increasingly IoT-connected world. According to a recent survey of U.S. technology decision-makers, the top hindrances to IoT growth are security and privacy concerns (Lund et al., 2014). A study by Hsu and Lin (2016) also found that the intended use of IoT is impacted by privacy and security concerns. Sicari et al. (2015) listed the following as the main security challenges in IoT: *access control, privacy, policy enforcement, trust, mobile security, secure middleware, confidentiality, and authentication*.

Extensive literature was found on IoT privacy and security as related topics. Lee and Lee (2015) conducted a survey of IoT practices and identified multiple challenges of IoT adoption including data management, data mining, privacy, and security. Supporting this finding, Insights Team (2017d) indicates that security is critical, as IoT devices are more frequently becoming a target for hackers and cyber terrorists. Peppet (2014) contends that the IoT is difficult to anonymize and secure, thus creating privacy issues. A general consensus exists around this contention and the concern that privacy and security are critical factors in IoT deployment (Marias et al., 2011; Ransbotham et al., 2016; Sicari et al., 2015; Sicari, Cappiello, De Pellegrini, Miorandi, & Coen-Porisini, 2016; Gessner, Olivereau, Segura, & Serbanati, 2012) with some offering advice on regulating the IoT including guidelines, best practices, and solutions (Gessner et al., 2012; Malina et al., 2016; Maple, 2017; Stankovic, 2014; Rekleitis et al., 2011; DHS, 2014; BITAG, 2016). The U.S. Department of Homeland Security (DHS, 2014, p.3) offers the following regarding IoT vulnerabilities in this realm:

> Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely adopted international norms and standards for IoT security (p. 3).

The following principles established by DHS (2014, p. 3–4) offer stakeholders a way to organize their thinking about how to address these IoT security challenges:

- Incorporate security at the design phase
- Advance security updates and vulnerability management
- Build on proven security practices
- Prioritize security measures according to potential impact
- Promote transparency across IoT
- Connect carefully and deliberately

Security is of utmost concern in the financial realm. Jay (2018) emphasizes that the CFO will need to work closely with the CIO to ensure all devices are capable of withstanding attacks that could detrimentally impact their organization's dealings and maintain constant vigilance. Of real concern in this domain according to Sicari et al. (2015) is the fact that a unified vision regarding the assurance of security and privacy requirements in such a heterogeneous environment, involving different technologies and communication standards is still missing. Different approaches to protecting users' privacy in the IoT have been addressed (Hsu & Lin, 2016; Jayaraman et al., 2017; Miorandi et al., 2012; Perera, Liu, Ranjan, Wang, & Zomaya, 2016; Samani, Ghenniwa, & Wahaishi, 2015; Weinberg, Milne, Andonova, & Hajjat, 2015; Ziegeldorf, Oscar, & Klaus, 2014). Kanuparthi, Karri, and Addepalli (2013) identified four key challenges in designing a secure IoT: data management, identity management, trust management, and privacy. Ning, Liu, and Yang (2013) point out that there is a broad array of challenges in terms of general system security, network security, and application security and address this according to the three layers of IoT architecture. Huang et al. (2016) looked at different dimensions of IoT security – authenticity and confidentiality, integrity, and availability – and developed a framework around the results. Although there is a lack of IoT security standards, there is no shortage of literature written on the vulnerabilities of IoT (Javed & Wolf, 2012; Kothmayr, Schmitt, Hu, Brünig, & Carle, 2013; Roman, Zhou, & Lopez, 2013; De Leusse, Periorellis, Dimitrakos, & Nair, 2012; Fernandes, Rahmati, Eykholt, & Prakash, 2017; Raza et al., 2014; Koo & Kim, 2017; Insights Team, 2017b; Heer et al., 2011; Ransbotham et al., 2016).

"While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation (DHS, 2014, p. 2)." IoT privacy and security concerns must be addressed before user trust in IoT applications can be established.

3.5.2. Trust

Trust is a complicated concept regarding confidence, beliefs, and expectations (Yan et al., 2014). The concept of trust is used in many different contexts and with diverse meanings. Miorandi et al. (2012) agree, indicating that although it is widely recognized as being important, trust is a complex notion about which no consensus exists in the information systems literature. Sicari et al. (2016) describes the concept of trust as being associated with source reputation and thus reliability. Mišura and Žagar (2016) suggest that application trustworthiness can be quantitatively evaluated by the similarity between the application's behavior and the behavior expected by the user. In this same context, Roman et al. (2013) point out that there are two dimensions of trust as related to IoT, i.e., (1) trust in the interaction between entities, and (2) trust in the system from the point of view of the user. Trust is essential when adopting and implementing IoT. It encompasses how users feel while interacting in the IoT (Roman, Najera, & Lopez, 2011).

"Trust management plays an important role in IoT for reliable data fusion and mining, qualified services with context-aware intelligence, and enhanced user privacy and information security" (Yan et al., 2014, p. 120). Other contributions to the literature on trust management include (Alshehri et al., 2018; Bao et al., 2013; Chen et al., 2016; Kowshalya & Valarmathi, 2017; Liu & Wang, 2010; Luo et al., 2016; Saied et al., 2013). Fernandez-Gago, Moyano, and Lopez (2017) established a framework for developers to include trust concerns in IoT systems. The framework suggests that trust should be included in all phases of the development of IoT systems following a proactive approach. Guo et al. (2017) conducted a survey of trust computation models for IoT concluding with directions for trust computation research. While privacy, security, and trust are all critical to the success of IoT, privacy and security are precursors to trust and must be an ongoing consideration. Despite these challenges, a study reported

by Insights Team (2017c) revealed that 42% of the respondents indicated that their IoT programs are doing what they should be doing - saving money, making the company more efficient or earning new revenues.

4. Theoretical framework and conceptual model

Researchers place a high value on theoretical frameworks. Despite this, the development of new theory and the refinement of existing theories have been relatively neglected within the information systems discipline (Weber, 2012). Confirming the sparse number of publications on theory development in IS fields and especially in IoT, an extensive review of literature produced a limited number of papers in this space. *Evaluating and Developing Theories in the Information Systems Discipline* was published by Weber (2012) and is rich in content. It is written in a clear and concise manner. Leidner and Kayworth (2006) published a review and theory paper on Information Technology culture conflict. Wiener et al. (2016) developed an expanded theoretical framework for Information Systems Projects, while Chaudhuri and Cavoukian (2018) published a framework for IoT privacy. The high-quality theory is believed to enhance the knowledge of the researcher and other scholars' knowledge within the theory's domain. It may also serve to enhance practitioners' capabilities to operate effectively and efficiently within the theoretical framework (Weber, 2012).

Weber (2012) describes several ways in which a theory might make novel contributions to a discipline:

- A theory's focal phenomena might not have been covered by prior theories;
- A theory might be considered novel because it frames or conceives existing, well-known focal phenomena in new ways; and
- A theory's novelty might arise because of important changes it makes to an existing theory – possibly adding or deleting constructs and associations, defining existing constructs and associations more precisely, or specifying the boundary of the theory more precisely.

The theoretical framework proposed in this paper falls under a *theory's focal phenomena has not been covered by prior theories* described by Weber (2012). Theories provide a representation of someone's perception of how a subset of real-world phenomena should be described (Weber, 2012). Weber (2012) further states that theories can be conceived as specialized ontologies – instances of a general ontology (a theory about the nature of and makeup of the real work, in general). Weber (2012) emphasize the main traits of the real world – in a clear and systematic method – to produce a unified picture of reality. Although the challenges of privacy, security, and trust have been widely discussed in the literature, a gap exists in both establishing IoT priority areas and the theoretical framework for IoT adoption and implementation considering the priority areas and challenges. Drawing from our analysis of previous research, the theoretical framework and conceptual model is shown in Fig. 2 was developed following Type IV of Gregor's (2006) taxonomy – theories for explanation and prediction – and Weber's (2012) proposed framework structure. The intention of this framework was to establish IoT theory and provide a clear and concise explanation and prediction of the main components of the IoT with the intention of guiding practitioners on IoT adoption and implementation and scholars on future research related to IoT.

Gregor (2006) identified a taxonomy of theories based on a thorough review of existing literature and identified five ways in which the term "theory" has been used: Type I – theories for analysis; Type II – theories for explanation; Type III – theories for prediction; Type IV – theories for explanation and prediction; and Type V – theories for design and action. Weber (2012) contends that Type I theories are typologies and not theories and that Type V theories are models but not theories lacking some characteristics important to a theory. Weber (2012) further argues that Type II theories and Type III theories may not be rigorous enough to constitute theories. Thus, Weber (2012) aligns with Gregor's (2006) Type IV taxonomy with the contention that the existence of a model is a necessary condition for the existence of a theory, but not a sufficient condition. The existence of a theory, however, is a sufficient condition for the existence of a model (Weber, 2012).

Hsu and Lin (2018) conducted a study examining factors seen as contributing to IoT service adoption using a research model based on the value-based adoption model (VAM). Their study examined the impact of perceived benefits (i.e. perceived usefulness and enjoyment and perceived sacrifices (i.e. perceived privacy risk and perceived costs) on perceived value and intent to use. As explained by Weber (2012), theories that have dynamic phenomena (events that occur to things) have four parts; their constructs, their associations; the states they cover, and the events they cover. Each of the four parts encompasses inside and outside boundaries.

Based on the Gregor's (2006) Type IV taxonomy - a theory for explanation and prediction - and parts of a theory proposed by Weber (2012), a theoretical framework and conceptual model was developed and is presented in Fig. 2 followed by a discussion.

The four parts of the theoretical framework illustrated in Fig. 2 are discussed in the following sections. Left bottom: States – the states space that falls with a theory's boundary, the range of values that each construct in the theory might cover first needs to be determined (Weber, 2012). The left bottom quarter of the circle defined as the *inside boundary state* is *Usage when considering IoT priority areas* vs. *challenges.* Uncertainties, especially concern about privacy and security, may impact usage. Users have been, in some cases, willing to take risks in this realm if the benefits are great enough. The *outside boundary state* shown in the left bottom rectangle of the model *includes IoT usage change as people gain trust in IoT.* Much like all technologies, as users gain trust in the system, it is predicted that the usage will increase which should be tested through further research. Left top: Events – "The events space that falls within the theory's boundary must also be articulated (Weber, 2012, p. 12)." The left top quarter of the circle defined as the *inside boundary event* is *Adoption of IoT*. This theoretical framework revolves around IoT in business which closely associates with the *outside boundary events* shown in the left top rectangle of the model – *Network of Devices and Applications*.

Right top: Constructs – represented inside the right top quarter of the circle defined as the *inside boundary construct* is *IoT stakeholders*. A construct in a theory represents an attribute in general of some class of things in its domain (Weber, 2012). He further emphasizes that the classes of things to which attributes in general pertain should be defined precisely to ensure that the meanings of each class and the things in each class are clear. Otherwise, the exact nature of the things that the theory covers will not be clear. Stakeholders are defined as humans impacted by or having an interest in The Internet of Things.

> The Internet of Things is not really about machines, says Hitachi Vantara's Kinsey. It is really about people and transformation. If you can make it work with people, you will see success (Insights Team, 2017c, p. 18).

The *outside boundary constructs* shown in the right top rectangle of the model includes *IoT high priority areas*. These will obviously vary by organization, but as previously discussed as one of the focal points for purposes of this paper, the authors are drawing from global studies (Insights Team, 2017c; Bartje, 2016) that identified the top IoT priority areas as customer experience, finance, and

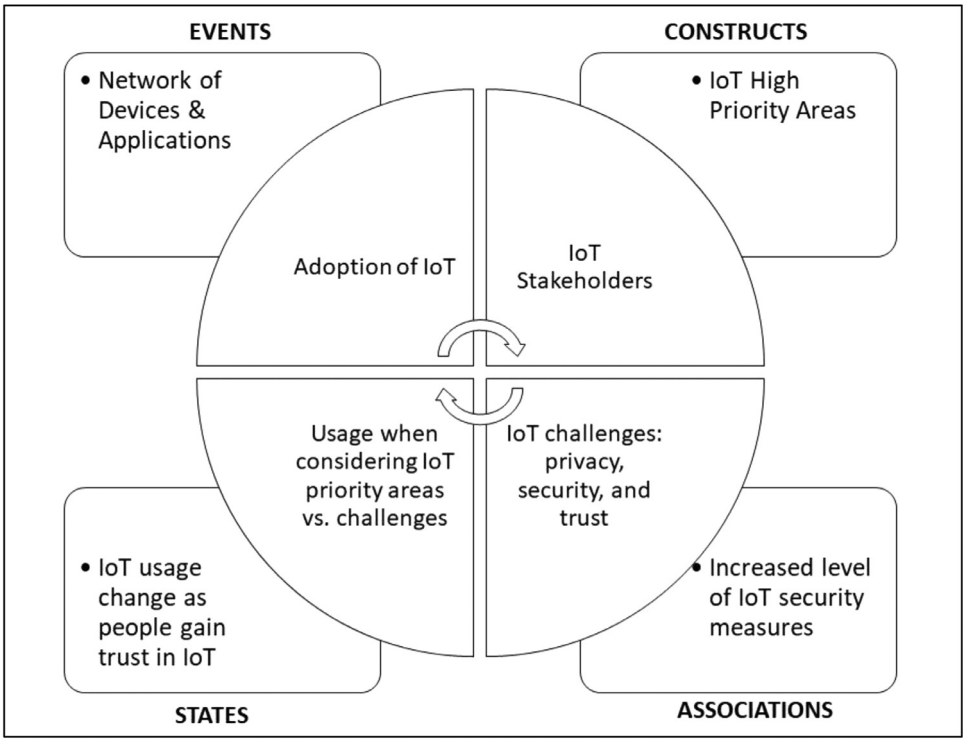

Fig. 2. IoT theoretical framework and conceptual model.

asset management. Right bottom: Associations – the right bottom quarter of the IoT theoretical framework and conceptual model shown in Fig. 2 reveal the associations. Associations in a theory can have multiple meanings (Weber, 2012). "Usually, a theory does not cover all possible associations among its constructs. Instead, researchers seek to make astute decisions about what associations to include in the theory and what associations to omit from the theory. The omission of an association among constructs in a theory does not necessarily mean none exists among the constructs (Weber, 2012, p. 11)."

Most theoretical models that are developed in the IS domain are either variance or process models (Rivard, 2014). Jaccard and Jacoby (2010) suggest that theory development be approached from a process perspective indicating that the researcher might theorize about the event or stages that would constitute adopting a technology. This approach was followed which led to the identification of the associations, states, and events. Represented inside the right bottom quarter of the circle defined as the *inside boundary associations* are *IoT challenges: privacy, security, and trust*. IoT challenges were identified as the second focal point of this paper and discussed extensively in a previous section. The *outside boundary associations* shown in the right bottom rectangle of the model includes an *increased level of IoT security measures*. As a result of the increased concerns about privacy, security, and trust as related to the IoT, increased the level of IoT security measures is imperative for IoT success and establishment of user trust.

Adoption of IoT involves much more than the architecture. Insights Team (2017c, p. 19) states that IoT is the digital transformation of business and "… building the business case and directing the IoT to solve business objectives are keys to success." As noted in the theoretical framework and conceptual model, priority areas must be identified, challenges addressed, and trust established to achieve the optimal benefits of an IoT system.

4.1. Contributions of the theoretical framework

Knowledge gained from the results of the IoT literature review and related concepts led to the development of a theoretical framework to enhance researchers' knowledge for further IoT studies. It is also intended to serve as an explanation of IoT and usage prediction which may guide practitioners when adopting and implementing IoT. This framework falls under Type IV – theories for explanation and prediction – taxonomy proposed by Gregor (2006) and further discussed by Weber (2012). An overall contribution of our framework is the establishment of theory on the IoT for IoT adoption and implementation which is virtually non-existent in the literature. There have been a handful of theories proposed and models developed, but this is the first that has integrated the components of stakeholders, challenges, and priority areas in an adoption and implementation theoretical framework and conceptual model. Challenges have been widely addressed and benefits have been briefly discussed in the literature, but very few have touched on the importance of identifying IoT priority (functional) areas to gain optimal benefits specific to the industry. Further addressed are additional contributions of the framework components as related to industry and research.

First, even though IoT involves machines communicating with machines, the human component cannot be taken out of the model. Stakeholders are crucial to the ultimate success of the IoT. Keeping this in mind, consideration of priority areas and challenges leading to IoT adoption are critical and both must be carefully addressed prior to IoT implementation. The IoT is much more than a multilayer stack of technologies. This theory contributes to IoT knowledge including priority areas in business which guides practitioners and most importantly is a reminder that the challenges of privacy and security must be addressed to gain user trust and successful usage of IoT. In support of this argument, Wortmann and Flüchter (2015) emphasized that as the

number of connected devices rises, at a strategic level, executives are forced to evaluate the opportunities and threats which the emergence of the IoT might present to their companies. Further indicating that existing business models may have to be adapted or redefined. The theoretical framework and conceptual model presented in this paper serve this purpose.

Second, the theoretical framework and conceptual model contribute to the body of knowledge in the IoT area giving scholars further explanation and prediction based on the theory components, thus, opening opportunities for a diverse range of research. There is ample space for testing this theory and components of the theory should be further studied separately as well. Hsu and Lin (2018) agree, stating that there is a need to further explore reasons that establish the IoT service adoption.

Third, as suggested by Wiener et al. (2016), researchers in the technology area may be inspired to expand and develop a review and theoretical framework with other components where research gaps may exist.

5. Conclusions

The purpose of this paper was to establish an extensive review and explanation of the IoT, including discussion of IoT architecture, applications, and impact. In addition, IoT priority areas and challenges were identified and a theoretical framework and conceptual model based on these findings were developed.

Research shows that companies are 'doubling down' on the IoT (Insights Team, 2017c). Despite the IoT recent emergence as a viable construct, research confirms its value to the business, consumers, and government. Our theoretical framework for IoT adoption – intended for both researchers and practitioners – establishes an integrated view providing the impetus for further research and successful adoption and implementation of IoT systems. As IoT continues to proliferate, standards, protocols, and connectivity must keep up the pace. Along with this, privacy and security should be a major focal point in the adoption and implementation of IoT platforms. By applying an understanding of IoT systems while keeping in mind the challenges, priority areas, and theoretical framework presented in this paper, researchers and practitioners alike should experience increased trust, benefits, and opportunities in the rapidly growing domain of the IoT.

As stated by Stankovic (2014, p. 2), "The spectrum of research required to achieve IoT at the scale envisioned requires significant research along many directions." Our recommendations based on our extensive review of the IoT literature are as follows. Future research should be conducted to validate the theoretical framework proposed in this paper. Additionally, research should be conducted on IoT in the business including challenges faced and lessons learned. As per Sicari et al. (2016), the huge amount of data handled in the IoT context poses new research challenges on security and privacy topics. Therefore, these topics merit attention for future research. Further research should be conducted regarding IoT priority areas to provide guidance to IoT implementation teams. Research should be conducted on trust as related to IoT.

As noted by Weber (2012), additional theories might arise because of important changes it makes to an existing theory – possibly adding or deleting constructs and associations, defining existing constructs and associations more precisely, or specifying the boundary of the theory more precisely. Research directions should draw from the theoretical framework developed in this paper proposing new theories or changes in the existing theory. Finally, global IoT studies should be conducted for comparison purposes among countries.

Conflict of interest

The authors declare that to the best of our knowledge, there is no known conflict of interest in writing this manuscript.

Credit authorship contribution statement

Jeretta Horn Nord: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Writing - original draft, Writing - review & editing, Visualization, Supervision, Project administration. **Alex Koohang:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Writing - original draft, Writing - review & editing, Visualization, Supervision. **Joanna Paliszkiewicz:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Writing - original draft, Writing - review & editing, Visualization.

References

AIS Senior Scholars Basket of Eight (2011). Retrieved from https://aisnet.org/?SeniorScholarBasket, (Accessed 12 December 2018).

Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the Internet of Things (CITM-IoT). *Mobile Networks and Applications*, 1–13. https://doi.org/10.1007/s11036-018-1017-z.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2016). Ethical design in the Internet of Things. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-016-9754-5.

Bandyopadhyay, S., Balamuralidhar, P., & Pal, A. (2013). Interoperations among IoT standards. *Journal of ICT Standardization, 1*, 253–270. https://doi.org/10.13052/jicts2245-800X.12a9.

Bao, F., Chen, I. R., & Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. In *2013 IEEE eleventh international symposium on autonomous decentralized systems (ISADS)* (pp. 1–7). https://doi.org/10.1109/ISADS.2013.6513398.

Bartje, J. (2016). The top 10 application areas – Based on eeal IoT projects. *IoT Analytics*. Retrieved from https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/. Accessed 11 November 2018.

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2017). Internet of Things and supply chain management: A literature review. *International Journal of Production Research*, 1–24. https://doi.org/10.1080/00207543.2017.1402140.

Bian, J., Yoshigoe, K., Hicks, A., Yuan, J., He, Z., Xie, M., et al. (2016). Mining twitter to assess the public perception of the 'Internet of Things'. *PLoS One, 11*(7). https://doi.org/10.1371/journal.pone.0158450.

BITAG (2016). Internet of Things (IoT) security and privacy recommendations. BITAG Broadband Internet Technical Advisory Group, November 2016. Retrieved from https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf, (Accessed 11 November 2018).

Burrus, D. (2014). The Internet of Things is Far Bigger than Anyone Realizes. Retrieved from https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/, (Accessed 11 November 2018).

Chaudhuri, A., & Cavoukian, A. (2018). The proactive and preventive privacy (3P) framework for IoT privacy by design. *EDPACS, 57*(1), 1–16. https://doi.org/10.1080/07366981.2017.1343548.

Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things. *Computer Science and Information Systems, 8*(4), 1207–1228. https://doi.org/10.2298/CSIS110303056C.

Chen, I. R., Guo, J., & Bao, F. (2016). Trust management for SOA-Based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482–495. https://doi.org/10.1109/TSC.2014.2365797.

De Leusse, P., Periorellis, P., Dimitrakos, T., & Nair, S. K. (2012). Self-managed security cell, A security model for the Internet of Things and services. In *Proceedings of the first international conference on advances in future internet* (pp. 47–52). https://doi.org/10.1109/AFIN.2009.15.

DHS (2014). Strategic principles for securing the Internet of Things (IoT). Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf, (Accessed 12 December, 2018).

Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017). Internet of Things security research: a rehash of old ideas or new intellectual challenges. *IEEE Security & Privacy, 15*(4), 79–84. https://doi.org/10.1109/MSP.2017.3151346.

Fernandez-Gago, C., Moyano, F., & Lopez, J. (2017). Modelling trust dynamics in the Internet of Things. *Information Sciences, 396*, 72–82. https://doi.org/10.1016/j.ins.2017.02.039.

Gessner, D., Olivereau, A., Segura, A. S., & Serbanati, A. (2012). Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications* (pp. 998–1003).

Gigli, M., & Koo, S. (2011). Internet of Things: Services and applications categorization. *Advances in Internet of Things, 1*(2), 27–31. https://doi.org/10.4236/ait.2011.12004.

Gillett, F. E., Truog, D., van den Brink-Quintanilha, J., Matzke, P., & Gunderson, A. (2018). *Forrester Report* retrieved from https://www.forrester.com/report/Boost+CX+Quality+By+Using+IoT+In+Customer+Journeys/-/E-RES137069 Accessed 01 January 2019.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30*(3), 611–642.

Guo, J., Chen, I. R., & Tsai, J. J. P. (2017). A survey of trust computation models for service management in Internet of Things systems. *Computer Communications, 97*, 1–14. https://doi.org/10.1016/j.comcom.2016.10.012.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security challenges in the IP-based Internet of Things. *Wireless Personal Communications, 61*(3), 527–542. https://doi.org/10.1007/s11277-011-0385-5.

Hsu, C., & Lin, J. C. (2016). An Empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior, 62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023.

Hsu, C., & Lin, J. C. (2018). Exploring factors affecting the adoption of Internet of Things services. *Journal of Computer Information Systems, 58*(1), 49–57. https://doi.org/10.1080/08874417.2016.1186524.

Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: A security framework for the Internet of Things. *Security and Communication Networks, 9*(16), 3083–3094.

Jaccard, J., & Jacoby, J. (2010). *Theory construction and model-building skills: A practical guide for the social scientist*. New York: The Guilford Press.

Javed, N., & Wolf, T. (2012). Automated sensor verification using outlier detection in the Internet of Things. In *Proceedings of the 32nd international conference on distributed computing systems workshops* (pp. 291–296). doi:10.1109/ICDCSW.2012.78.

Jay, E. (2018). *The IoT and the finance function*. Innovation Enterprise Retrieved from https://channels.theinnovationenterprise.com/articles/the-iot-and-the-finance-function Accessed 01 February 2019.

Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, (76), 540–549. https://doi.org/10.1016/j.future.2017.03.001.

Junnila, A. (2018). *What the Internet of Things brings to asset management*. Trackinno Retrieved from https://trackinno.com/2018/02/05/internet-things-iot-brings-asset-management/ Accessed 01 February 2019.

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of Internet of Things. In *Proceedings of the ACM conference on computer and communications security* (pp. 61–65). https://doi.org/10.1145/2517968.2517976.

Kim, D., Chun, H., & Lee, H. (2014). Determining the factors that influence college students' adoption of smartphones. *Journal of Association for Information Science Technologies, 65*(3), 578–588. https://doi.org/10.1002/asi.

Koo, C., & Kim, J. (2017). Enforcing high-level security policies for Internet of Things. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-017-2201-9.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks, 11*(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003.

Kowshalya, A. M., & Valarmathi, M. L. (2017). Trust management in the social Internet of Things. *Wireless Personal Communications, 96*(2), 2681–2691. https://doi.org/10.1007/s11277-017-4319-8.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008.

Leidner, D. E., & Kayworth, T. (2006). Review: A review of culture in information systems research: toward a theory of information technology culture conflict. *MIS Quarterly, 30*(2), 357–399.

Liu, Y., & Wang, K. (2010). Trust control in heterogeneous networks for Internet of Things. In *Proceedings of the international conference on computer application and system modeling (ICCASM)* (pp. 632–636). https://doi.org/10.1109/ICCASM.2010.5620458.

Lueth, K. L. (2015). *The 10 most popular Internet of Things applications right now*. IoT Analytics Retrieved from https://iot-analytics.com/10-internet-of-things-applications/ Accessed 12 December 2018.

Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). *Worldwide and regional Internet of Things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand*. Framingham, MA, USA: Int. Data Corp. *Tech. Rep*. 248451.

Luo, W., Ma, W., & Gao, Q. (2016). A dynamic trust management system for wireless sensor networks. *Security and Communication Networks*, (9), 613–621. https://doi.org/10.1002/sec.1384.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, 3*(5), 164–173. https://doi.org/10.4236/jcc.2015.35021.

Mäkinen, J. (2015). Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things. *Information & Communications Technology Law, 24*(3), 262–277. https://doi.org/10.1080/13600834.2015.1091128.

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the Internet of Things. *Computer Networks, 102*, 83–95. https://doi.org/10.1016/j.comnet.2016.03.011.

Maple, C. (2017). Security and privacy in the Internet of Things. *Journal of Cyber Policy, 2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536.

Marias, G. F., Barros, J., Fiedler, M., Fischer, A., Hauff, H., & Herkenhoener, R. (2011). Security and privacy issues for the network of the future. *Security and Communication Networks, 5*(9), 987–1005.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016.

Mišura, K., & Žagar, M. (2016). Negotiation in Internet of Things. *Automatika, 57*(2), 304–318. https://doi.org/10.7305/automatika.2016.10.1193.

Nicolescu, R., Huth, M., Radanliev, P., & Roure, D. D. (2018). Mapping the values of IoT. *Journal of Information Technology*. https://doi.org/10.1057/s41265-018-0054-1.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer, 46*(4), 46–53. https://doi.org/10.1109/MC.2013.74.

Ornes, S. (2016). The Internet of Things and the explosion of interconnectivity. In *Proceedings of the National Academy of Sciences: 113* (pp. 11059–11060).

Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(1), 85–179.

Perera, C., Liu, C., Ranjan, R., Wang, L., & Zomaya, A. Y. (2016). Privacy-knowledge modeling for the Internet of Things: A look back,. *Computer, 49*(12), 60–68. https://doi.org/10.1109/MC.2016.366.

Petersen, H., Baccelli, E., Wählisch, M., Schmidt, T. C., & Schiller, J. (2014). The role of the Internet of Things in network resilience. *International Internet of Things Summit*, 283–296.

Raferty, T. (2017). *How to enrich the customer experience using Internet of Things*. Forbes retrieved from https://www.forbes.com/sites/sap/2017/12/21/how-to-enrich-the-customer-experience-using-internet-of-things/#115119cf5bb0 Accessed 12 December 2018.

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special section introduction – Ubiquitous IT and digital vulnerabilities. *Information Systems Research, 27*(4), 834–847.

Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2014). Secure communication for the Internet of Things – A comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks, 7*(12), 2654–2668. https://doi.org/10.1002/sec.406.

Rekleitis, E., Rizomiliotis, P., & Gritzalis, S. (2014). How to protect security and privacy in the IoT: A policy-based RFID tag management protocol. *Security and Communication Networks, 7*, 2669–2683. https://doi.org/10.1002/sec.400.

Rivard, S. (2014). The ions of theory construction. *MIS Quarterly, 38*(2), 3–13.

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *Computer, 44*(9), 51–58. https://doi.org/10.1109/MC.2011.291.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018.

Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Computers & Security, 39*, 351–365. https://doi.org/10.1016/j.cose.2013.09.001.

Samani, A., Ghenniwa, H. H., & Wahaishi, A. (2015). Privacy in Internet of Things: A model and protection framework. *Procedia Computer Science, 52*, 606–613. https://doi.org/10.1016/j.procs.2015.05.046.

Shaikh, F. K., Zeadally, S., & Exposito, E. (2017). Enabling technologies for green Internet of Things. *IEEE Systems Journal, 11*(2), 983–994. https://doi.org/10.1109/JSYST.2015.2415194.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers, 18*(4), 665–677. https://doi.org/10.1007/s10796-014-9538-x.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008.

Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet of Things Journal, 1*(1), 3–9. https://doi.org/10.1109/JIOT.2014.2312291.

Team, Insights (2017a). *5 Areas where the IoT is having the most business impact*. Forbes Insights Retrieved from https://www.forbes.com/sites/insights-hitachi/2017/12/18/5-areas-where-the-iot-is-having-the-most-business-impact/#58b5e104396c Accessed 01 February 2019.

Team, Insights (2017b). *Don't get caught unprepared when it comes to IoT security*. Forbes Insights Retrieved from https://www.forbes.com/sites/insights-hitachi/2017/12/18/dont-get-caught-unprepared-when-it-comes-to-iot-security/#74e9c7f4d800 Accessed 01 February 2019.

Team, Insights (2017c). *The Internet of Things: From theory to reality*. Forbes Insights Retrieved from info.forbes.com/rs/790-SNV-353/images/Hitachi IoT Report.pdfAccessed 01 February 2019.

Team, Insights (2017d). *4 Ways to overcome the complexity of IoT implementation*. Forbes Insights Retrieved from https://www.forbes.com/sites/insights-hitachi/2017/12/18/4-ways-to-overcome-the-complexity-of-iot-implementation/#269cad527034 Accessed 01 February 2019.

Team, Insights (2017e). *Why collaboration is essential for successful IoT implementation*. Forbes Insights Retrieved from https://www.forbes.com/sites/insights-hitachi/2017/12/18/why-collaboration-is-essential-for-successful-iot-implementation/#27effdde10e0 Accessed 01 February 2019.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems, 13*(1), 1–30.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), 13–23.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615–624.

Wiener, M., Mahring, M., Remus, U., & Saunders, C. (2016). Control configuration and control enactment in information systems projects: Review and expanded theoretical framework. *MIS Quarterly, 40*(3), 741–774.

Wortmann, F., & Flüchter, K. (2015). Internet of Things. *Business & Information Systems Engineering, 57*(3), 221–224. https://doi.org/10.1007/s12599-015-0383-3.

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014.

Ziegeldorf, J. H., Oscar, G. M., & Klaus, W. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728–2742. https://doi.org/10.1002/sec.795.