A Systematic Mapping study on Internet of Things challenges

Aleksandr Lepekhin
Graduate School of Business and Management
Peter the Great St.Petersburg Polytechnic University
St.Petersburg, Russia
lepekhinalexander@gmail.com

Alexandra Borremans
Graduate School of Business and Management
Peter the Great St.Petersburg Polytechnic University
St.Petersburg, Russia
Borremans_ad@spbstu.ru

Igor Ilin
Graduate School of Business and Management
Peter the Great St.Petersburg Polytechnic University
St.Petersburg, Russia
Ivi2475@gmail.com

Sami Jantunen
School of Engineering Sciences
LUT University
Lappeenranta, Finland
sami.jantunen@lut.fi

***Abstract*—The challenge of developing IoT-based systems has been found to be a complex problem. It is influenced by number of factors: heterogeneous devices/resources, various perception-action cycles and widely distributed devices and computing resources. Increasing complexity and immaturity to deal with it have resulted in growing range of problems and challenges in IoT development. This paper identifies essential IoT-related challenges by conducting a systematic mapping study of existing IoT literature. To this end, we distil information with respect to IoT-related: 1) challenges, 2) experimental studies, and 3) recommendations for future research. We then discuss our findings in order to understand better the general state of IoT research, potential gaps in research, and implications for future research.**

Keywords—Internet of Things, IoT, IoT Challenges, IoT Development, Systematic mapping study

I. INTRODUCTION

Due to advances in the field of Internet technologies and wireless sensor networks (WSN), a new trend in the era of ubiquity is being realized. The huge increase in internet users and the modification of interworking technologies allow the creation of networks of everyday objects called Internet of Things (IoT). Implementation of this technology is rapidly gaining momentum as technological, public and competitive pressures push firms to innovate and transform. The entire infrastructure of different domains changes with the introduction of IoT, creating a so-called intelligent infrastructure.

As IoT technology advances, an increasing number of firms have started to adopt the technology in different sectors: Health Care, Transportation, Waste Management, Food Supply Chains, and Energy & Utilities. IoT does not only bring certain changes in those domains, but it enables fundamentally new paradigm, which can be called as an extension and expansion of Internet-based network. It expands the communication from human and human to human and things or things and things. IoT is not subversive revolution over the existing technologies, it is comprehensive utilizations of existing technologies [1].

Development of IoT-based solutions is currently a widely discussed topic. The challenge of developing IoT-based systems has been found to be a complex problem. It is influenced by number of factors: heterogeneous devices/resources, various perception-action cycles and widely distributed devices and computing resources [2]. Another issue, pointed out by researchers, is the shift of focus in software development. It changes from goal-oriented to user-oriented, distributed intelligence and machine-to-machine and machine-to-human collaboration [3].

Increasing complexity and immaturity to deal with it have resulted in growing range of problems and challenges in IoT development. This paper identifies essential IoT-related challenges by conducting a systematic mapping study of existing IoT literature. To this end, we distil information with respect to IoT -related: 1) challenges, 2) experimental studies, and 3) recommendations for future research. We then discuss our findings in order to understand better the general state of IoT research, potential gaps in research, and implications for future research.

The structure of our study is as follows. Section 2 describes the research method. Section 3 presents the results of our systematic mapping study. Section 4 identifies recommendations for future IoT research and compares these findings with the results of Section 3. Finally, Section 5 concludes the paper.

II. RESEARCH METHODS

We have conducted a systematic literature mapping [4]. This type of research requires a prior definition of the review protocol, that describes and justifies the research questions and outlines a method for studying, evaluating and synthesizing different types of research. In our study, following research questions were specified:

1. What IoT-related challenges have been reported?
2. How identified IoT challenges have been addressed?
3. What implications the findings have on future IoT research?

An important part of systematic mapping study is the specification of inclusion and exclusion criteria [5]. We decided to include Computer Science-related studies that described IoT challenges. Those studies that could not be accessed without additional investments were decided to be excluded from this mapping study.

Definition of the search strategy and data sources is the next step of systematic mapping study. Kitchenham [6]

suggests that researchers should indicate their rationale for using an electronic or manual search or a combination of both. In this study, we used electronic search procedure to identify the studies that help to answer the research questions and exclude human factor (when manual search is done). Electronic search procedure was chosen because it is represented as an essential contribution toward ensuring accuracy and completeness of the evidence [7]. The electronic search was applied on the Scopus search engine, because almost 80% of Scopus records include abstract, which makes analysis easier, and high quality of search outcomes [8]. The following search string was applied:

TITLE-ABS-KEY (iot AND challenges) AND (LIMIT-TO (ACCESSTYPE(OA))) AND (LIMIT-TO (SUBJAREA, "COMP"))

The search resulted with 79 open-access research papers (45 journal papers and 34 conference proceedings). Three papers were excluded from the analysis as they were country specific (India, South Korea, Netherlands). The sources of research papers are summarized in Table I.

TABLE I. IDENTIFIED PAPERS

Publication Source (# of identified papers)	Included papers
Papers in Conference proceedings (34)	***33***
Procedia Computer Science (28)	27
Other Conference proceedings (6)	6
Papers in Journals (45)	***43***
Mobile Information Systems (8)	8
Eurasip Journal On Wireless Communication and Networking (6)	6
Digital Communications And Networks (3)	3
Procedia Manufacturing (3)	3
Other Journals (25)	23
Total (79)	**76**

III. RESULTS

Our systematic mapping revealed that the reviewed papers addressed six different categories of IoT challenges (Table II). This section describes these six types of IoT challenges and shows how the reviewed papers addressed these challenges.

TABLE II. IDENTIFIED CATEGORIES OF IOT CHALLENGES AND THE PAPERS ADDRESSING THESE CHALLENGES

IoT Opportunities in different contexts	[9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27][28][29][30][31][32][33][34][35]
Communication technologies	[10][36][37][38][39][40][41][42][43][44][45][46][47][48][49][50][51][52][53][54][55][56]
Interoperability	[10][38][57][58][59][60][61][62][63][64][65]
Security	[10][11][13][34][66][67][68][69][70]
Data and Privacy	[3][15][16][22][30][63][68][71][72][73][74][75]
IoT Development considerations	[3][14][58][76][77][78][79][80][81][82][83]

A. IoT Opportunities in different contexts

IoT technology has already been utilized in a wide variety of contexts [9][10]. One of the most recognizable and notable contexts is healthcare and medicine [11][12][13][14][15][16][17][18][19]. IoT infrastructure has the potential to revolutionize the practice of medicine and transform how people manage their health [10]. Within this context privacy and security particularly important. To this end, [11] have developed a secure and efficient authentication and authorization architecture for IoT-based healthcare, and [16] sought to define a mechanism for prioritizing threats and aspects that are likely to be affected when devices may be added, removed, or changed. Since safety and privacy is heavily influenced by legislation, [13] analyzed relevant legislative frameworks and presented a case study how legislation affected the design of mobile application in digital health. Another challenge is to support the interoperability among several heterogeneous devices from different manufacturers. This challenge has been addressed by [12] with their implementation of a web middleware platform for connecting doctors and patients using attached body sensors. Such high degree of interconnectivity and sensitivity of data also raise ethical questions. These considerations are addressed in [14], which articulates various levels of trust among the concerned stakeholders in the service ecosystem and suggests value-sensitive design considerations, anchored on the principles of trust, for future IoT-enabled assistive care services.

Smart city is another context, where IoT is already heavily used. In some studies it is also called «Programmable city», highlighting its ability to develop smart physical infrastructure [20]. The amount of data in this context is considerably bigger than in any other context, bringing forward the challenges of data storage, management, security and analysis [21][22]. This challenge has been addressed by [23], with a framework proposal called Cloud-based Context-aware Internet of Things services in smart cities (C2IoT), that is intended to ease the deployment, development and offering of new smart services for the future smart city [23]. Urbanization context of IoT is linked to environmental issues, which created a concept of Green IoT [24][25]. IoT in Smart city is also considered in the context of transportation system. Researches analyze how intelligent transportation system can be implemented based on wireless networks [26][27].

IoT has also been argued to create opportunities to manufacturing industry for improving sustainability, performance and quality of production [28]. Such Industrial adaptation of IoT is often called Smart Factory and the trend of utilizing IoT in manufacturing is often referred as Industry 4.0 (German technological strategic initiative) [29][34][35]. A practical example of using IoT in manufacturing context is provided by [28], with a proposal of a smart injection molding system framework based on real-time manufacturing data considering the characteristics of injection molding processes, modules that compose the framework, and their detailed functions. As another example, [30] presented the design, implementation and proof of concept evaluation of an industrial, semantic Internet of Things positioning architecture, using low-power embedded wireless sensors.

IoT has also been used on more personal contexts. One of the well-known context is Smart Homes, that enables people to instrument their own homes [10][31]. The opportunities for using IoT in gaming context has been studied by [32]. Sports environment is viewed as another context of IoT adaptation, where IoT adoption could significantly improve

the sport experience and also the safety level of team sports [33].

B. Communication technologies

Existing network protocols have largely been designed for stationary devices with reasonable computational and memory resources [10]. Since many IoT devices do not have access to a continuous power source, the way devices compute and communicate are significantly constrained. This creates needs for low-power communication. Furthermore, new network protocols and architectures need to also be able to support vast numbers of devices that are possibly mobile and that interact with the physical world, human users, and the cloud [10][36][37].

A review of currently used wireless data communication technologies have been provided in [38][39]. Our literature mapping identified several experimental studies that sought to improve communication in terms of scalability, power consumption and end-to-end delay by: 1) modifying Bluetooth low energy (BLE) retransmission model [40]; 2) reducing signaling cost of mobile IoT devices, by grouping devices with similar movement behavior with a PMIPv6-based group binding update method [41][42]; 3) reducing the number of transmitted packets by proposing Conditional Observation-function, where clients tell the servers the criteria for notifications [43]; 4) optimizing a Media Access Control (MAC) protocol for linear network topologies [44]; 5) introducing a new enhanced data streaming route optimization scheme that uses an optimized Transmission Control Protocol (TCP) realignment algorithm [45]; 6) developing an efficient scheme to estimate the number of unidentified tags for Dynamic Framed Slotted Aloha (DFSA) based RFID system [46]; 7) envisioning a scenario where many in-home sensors are communicating with a smart gateway over the BLE protocol, while at the same time harvesting RF energy transmitted from the gateway wirelessly via a dedicated radio interface [47]; 8) applying a multi-objective evolutionary optimization algorithm to reduce network energy consumption through optimization of sensor distribution [48]; 9) proposing a QoS based vertical handover scheme for M2M communications [49][50][51]; 10) presenting a novel data aggregation and multiplexing scheme for mobile M2M traffic [54]; 11) proposing novel access and scheduling schemes can reduce the collision rate dramatically during the IoT random access procedure and improve the performance of IoT communication [53]; 12) creating a scalable two-level index scheme (STLIS) for RDF data which can respond to the complex query in real time [55]; 13) developing an on-demand CSaaS to provide users with standardized access to various sensor networks and a level of abstraction that hides the underlying complexity [56].

The need to support Internet of Things (IoT) and device-to-device (D2D) communication also require a major paradigm shift in the way cellular networks have been planned in the past. This challenge has been addressed in [52].

C. Interoperability

IoT would benefit from ways to let multiple applications (and sets of associated IoT devices) control their own fate over a shared network infrastructure [10]. This would lead to Internet of services that is highly dynamic and continuously changing due to constant degrade, vanish and possibly reappear of the devices [57]. In such scenario, we are shifting from code-heavy monolithic applications to a set of smaller, self-contained microservices, each offering narrowly focused, independently deployable services [58]. To this end, [59] presents challenges and technological enablers that will allow things to evolve and act in a more autonomous way, becoming more reliable and smarter.

Some of the essential challenges addressed in the reviewed papers are resource discovery and selection [60][61][57]. Another major challenge is to guarantee that the system is always configured correctly, despite of being in constant flux. It has been argued [10] that this can be achieved only with automation and with higher-level policy languages that allow users and administrators to specify high-level intent rather than configure low-level mechanisms. This challenge has been addressed by [59] with a presentation of architecture allowing things to learn based on others experiences and introducing situational knowledge acquisition and analysis techniques for things to be aware of conditions and events affecting IoT-based systems behavior.

To reduce the frequency and increase the effectiveness of debugging, IoT systems and devices will need to constantly monitor their own "health" [10]. To this end, IoT systems could adopt Structural Health Monitoring (SHM) processes of gathering basic information that allows detecting, locating and quantifying vulnerabilities early on (fatigue cracking, degradation of boundary conditions, etc.), thereby improving, the resilience of the IoT System [38]. When problems are detected, IoT systems need to be able to learn from errors and automatically repair themselves [10]. An example of developing methods to automatically achieve a self-configurable system, where associations and data can be adapted by self-learning is presented in [62]. Moreover, in order to provide heterogeneous connectivity, graph theory and system models can be applied for IoT network optimizations [64]. It was also noted that for supporting the task of high-level IoT applications the semantic-web based approach can be used [63]. To prevent compatibility problems, it is proposed to use the model-driven development approach at the stage of system modeling and create interoperability-specific models. Such models can support and be used in different applications that are allowing them to be used by both professional and non-expert application developers [65].

D. Security

Traditional security solutions and protocols cannot be implemented well in IoT specific environment that is typically constrained by limited computing and power resources [66][67]. Consequently, devices and objects may interact together using many different security techniques and using different operational environments [68]. Added with the challenge of insufficient security expertise among device manufacturers and end users, IoT devices may not always defend themselves appropriately [10]. It is even more difficult to maintain and to improve security when there are frequent software changes, which is the case in agile environments [69].

Some of the well-known IoT-related security challenges include risks of attackers to [66]: 1) access devices which control physical access to home or business such as electronic doors, locks etc.; 2) access smart devices that can be potentially used to act as botnets; 3) exploit IoT devices

for purposes that they were not intended for, leading businesses to monetary losses; 4) monitor and collect valuable data from compromised IoT devices in a home or enterprise; 5) discover the location of the IoT device.

In a recent literature review, [69] identified 17 security challenges with regards to *technical*, *organizational* and *methodological* perspectives, where technical challenges relate to security concerns when designing and implementing IoT applications, organizational challenges relate to company's policies, factors about market and external stakeholders, and methodological challenges relate to the difficulties companies found in integrating security identification, analysis, testing and monitoring in their development methodology [69]. It has been argued that companies would need support with tailoring a process to address these security challenges [69] and that that security challenges can be effectively addressed, if security is introduced prior to development and deployment of IoT by relying on secure software, secure hardware and secure communications [66]. To this end, IoT applications need to consider a comprehensive system, from a cloud-based storage and data analysis, end user applications, middleware and hardware devices and their connectivity [69]. In this line of work, [68] have detailed a systemic and cognitive approach for the IoT, along with a description of: 1) the state-of-the-art of IoT security research activities, 2) the major technological solutions and projects according to this systemic and cognitive approach, and 3) the main standardization activities related to IoT security.

Due to the heterogeneous and irregular composition of IoT systems, it becomes necessary to define a different evaluation of trust for objects, humans, and services [68]. Furthermore, securing IoT devices requires deliberation to create balance between security mechanism and intended operation of a device [66]. Majority of security challenges can be addressed by considering appropriate protocols for the problem and by following best practices during design and development stage, such as [66]: 1) Categorizing IoT devices according to their functionality and communication requirements and then omitting all unnecessary communication modules from the devices; 2) Paying attention to access and authentication mechanisms; 3) Embedding cryptography functions on a hardware level; 4) Considering appropriate key distribution mechanism 5) Making policy decisions related to secure storage capability within the device; 6) Considering how to update or patch the device firmware.

As some practical security-related studies: [13] presents a case study on security and privacy implications on the design of a mobile application in digital health, which utilizes sensing technologies and capabilities of the Internet of Things (IoT), [11] describes an implementation of a secure and efficient authentication and authorization architecture for IoT-based healthcare, [70] proposes to optimize elliptic curve cryptography for 16-bit devices without hardware multiplier by shifting primes, [22] describes the model-based security toolkit, which is applied in a management framework for IoT devices, and [34] highlights Industry 4.0 - related security issues raising awareness for security good practices within Industry 4.0.

E. Data and Privacy

Internet of Things (IoT) applications rely on networks composed of set of heterogeneous sensors and smart devices, which have the capability to constantly, observe the surroundings and generate massive amounts of data [63][71], that need to be processed and stored [3]. The heterogeneity of the devices leads to heterogeneity of generated raw data, which makes the task to interpret such data and detect events in the real world more complex [63][71]. Another challenge with data is the uncertainty caused by noise, sensor error or wireless communication techniques [72]. Data heterogeneity leads to interoperability problems between IoT applications. This challenge has been addressed by using Semantic Web (SW) technologies to model and integrate data from different sources on the web [63]. Semantically annotating contextual information to IoT data is a fundamental step toward developing smarter and interoperable IoT applications. This topic has been addressed by [73][63][74][30].

The necessity to manage data leads also to the challenge of privacy that can be further decomposed to the issues of data privacy and access privacy. Data privacy must be considered throughout the different phases of data usage, including collection, transmission, and storage. Access privacy emphasizes the manner in which people can access to personal information [68]. These topics have been discussed and addressed in [75][68][15][16].

F. IoT Development considerations

Our study revealed several studies working towards new software development approaches. As practical examples, [76] investigated challenges of integrating IoT products into enterprise architecture, and [77] addressed issues related to battery life and power usage, arguing that these are fundamental elements of design in the IoT ecosystem that play a significant role in market success. The topic of guaranteeing the Quality of Service (QoS) was addressed by [58] [78].

IoT is accelerating the transition from application development approaches to application composition approaches [58]. To this end, [79] presents state-of-the-art survey in 13 existing Visual Programming Languages (VLS) being used for IoT application development. Furthermore, large number of connected heterogeneous things and objects require simplifying the development of new applications and services [3]. To address this challenge [80] studied middleware technologies, that are situated between things and applications and create a reliable platform for communication among things with different interfaces, operating systems, and architectures.

IoT is also shifting the development focus from one-time delivery towards continuous delivery, causing currently widely used development methods, such as waterfall or serial methods to crumble [81]. Another issue with traditional development approaches is that development tend to happen in silos, whereas developing IoT solutions would require close communication among relevant stakeholders [81]. It has been argued [81] that agile methodologies' ability to support collaboration and automated tools supporting continuous delivery are particularly suitable to deal with these new IoT-related demands, resulting with shorter lead times, faster overall development efficiency, and more product updates and releases [81]. Furthermore, [82] suggests that combining elements of universal and

participatory design provides users the opportunity to contribute to the invention of solutions that are more compatible with their daily lives.

Despite of advances in ways of developing IoT solutions, [3] argues that there is still a paucity of studies on the social, behavioral, economic, and managerial aspects of the IoT. In particular, the insufficient understanding of IoT business models and how they are connected to the underlying ecosystem calls for greater attention to emerging IoT ecosystems from the business perspective [83] and human relationships and trust within the ecosystem [14].

IV. Discussion

Developing software for complex IoT systems require new approaches to software development including abstractions, tools, and practices [10]. However, best IoT development practices are still emerging, and suitable test and validation environments are still in their infancy [84]. Two of the reviewed papers [10][58] outlined recommendations for future IoT research. In this section, we will compare the findings of our mapping study with these recommendations.

In this literature mapping study, we identified several examples of utilizing IoT in different domains. Our observation from these studies is that they typically focus on a single domain (such as healthcare, smart city, etc.). Support for research that considers architectures and solutions transcending these specific application domains is hence needed [10].

We identified several studies improving communication technologies in terms of scalability, power consumption and end-to-end delay. This line of work require interdisciplinary collaboration in signal processing and wireless communication, as well as computer architecture and operating systems [10].

Our review related to interoperability challenges revealed a tendency towards microservices architecture, where IoT subsystems can control their own fate over a shared network infrastructure. This creates challenges of discovering relevant services and challenges of ensuring the integrity of system at any given time. Since IoT systems need to be continually modifiable and maintainable to meet changing requirements that were not envisaged at design time, we need novel methods to support software adaptability, scalability and maintainability [58]. These needs call for research to facilitate the construction, deployment, and automated analysis of multicomponent systems with complex and dynamic dependences [10]. Some of the main challenges include the development of models, methods and design tools for going beyond formal methods research to create abstractions and formalisms for constructing and reasoning about systems with diverse and more difficult-to-characterize components [10][58]. There is also a need to further research design patterns at the architectural level describing the obligations/constraints to be fulfilled by the system in which the software is running, and to validate and standardize them [58].

Security was identified to be one of the essential challenges of IoT systems. The reviewed papers suggested that this is best to be tackled in a holistic manner already at design stage. Further research is needed on the unique challenges and opportunities in IoT security, such as minimal operating systems to create IoT devices with smaller attack surfaces, new ways detect and prevent anomalous network traffic, and high-level policy languages for specifying permissible communication patterns [10]. On a more general level, we need research that addresses cross-cutting issues, such as: networking, security, privacy, and impact of the physical on the cyber, real-time. [10]. These aspects need to be taken into account when software development methodologies are evolving towards supporting IoT systems development [58].

The ability of IoT systems to generate wide range of data, not only raises challenges of turning raw data into meaningful knowledge and events, but also raises concerns of privacy. These concerns are closely related with the topic of security.

IoT systems consisting of independent microservices, that are possibly created and maintained by several different parties, create a complex and dynamic software-powered ecosystem that is flexible and constantly evolving. Existing Requirements Engineering approaches do not account well for such dynamicity of use and unknown requirements [58]. Hence, there is the need for a radically divergent approach to capture emerging behavior from systems and users [58]. The fact that we can now access enormous amount of data about the system creates an exciting new opportunity. We have now better possibilities to make informed decisions based on gathered user feedback and data showing the usage of the system [58]. This calls for novel software production methodologies to actually enable controlled management of feature experimentation with short development cycles [58]. An example of this kind of new methodology is Hypothesis Experiment Data-Driven Development (HYPEX-model) [85], that is used for initiating, conducting and evaluating feature experiments with customers with the intent to improve decision-making and prioritization within software development companies. However, more research is needed for supporting decision-making that is based on real data gathered from experiments with customers. Despite the ability to capture large amounts of data related to the behavior of an application, limited progress has been achieved in developing feedback analysis tools [43]. Moreover, in order to reduce the development time as much as possible, we need simulators, benchmarks, and code bases to be able to quickly conduct realistic (and repeatable) experiments and to evaluate new ideas with reasonable investments of time and money [10]. We also need approaches that can increase the anti-fragility of systems, reduce the meantime-to-restore-service (MTRS), and develop accelerated methodologies to test quality through staging and canary testbeds [58].

Our review also revealed that the diversity of stakeholders within the business ecosystem creates essential challenges that are not yet sufficiently researched, creating the need to study business aspects, value creation as well as social aspects within the ecosystem.

V. Conclusions

We have in this paper conducted a systematic mapping study of existing IoT literature, with the intent to distill IoT - related: 1) challenges, 2) experimental studies, and 3) recommendations for future research. Our work resulted with the identification of six categories of IoT challenges and with identification of the papers addressing these challenges

(Table II). Our study provides details on the progress of research with respect of each type of IoT challenges and argues that software development style is likely to change towards experimentation and data-driven development. The paper also points out the insufficient attention to business and human aspects, when working within an IoT ecosystems.

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014.

[2] N. K. Giang, M. Blackstock, R. Lea, and V. C. M. Leung, "Developing IoT applications in the Fog: A Distributed Dataflow approach," in *2015 5th International Conference on the Internet of Things (IOT)*, Seoul, South Korea, 2015, pp. 155–162.

[3] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, Jul. 2015.

[4] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering.," in *EASE*, 2008, vol. 8, pp. 68–77.

[5] J. Popay *et al.*, "Guidance on the conduct of narrative synthesis in systematic reviews," *Prod. ESRC Methods Programme Version*, vol. 1, p. b92, 2006.

[6] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[7] M. Sampson, J. McGowan, E. Cogo, J. Grimshaw, D. Moher, and C. Lefebvre, "An evidence-based practice guideline for the peer review of electronic search strategies," *J. Clin. Epidemiol.*, vol. 62, no. 9, pp. 944–952, 2009.

[8] A. Aghaei Chadegani *et al.*, "A comparison between two main academic literature collections: Web of Science and Scopus databases," 2013.

[9] S. Albishi, B. Soh, A. Ullah, and F. Algarni, "Challenges and Solutions for Applications and Technologies in the Internet of Things," *Procedia Comput. Sci.*, vol. 124, pp. 608–614, Jan. 2017.

[10] "[1604.02980] Systems Computing Challenges in the Internet of Things." [Online]. Available: https://arxiv.org/abs/1604.02980. [Accessed: 24-Dec-2018].

[11] S. R. Moosavi *et al.*, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jan. 2015.

[12] P. Maia *et al.*, "A Web Platform for Interconnecting Body Sensors and Improving Health Care," *Procedia Comput. Sci.*, vol. 40, pp. 135–142, Jan. 2014.

[13] M. Volk, J. Sterle, and U. Sedlar, "Safety and Privacy Considerations for Mobile Application Design in Digital Healthcare," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 10, p. 549420, Oct. 2015.

[14] S. Bhattacharya, D. Wainwright, and J. Whalley, "Internet of Things (IoT) enabled assistive care services: Designing for value and trust," *Procedia Comput. Sci.*, vol. 113, pp. 659–664, Jan. 2017.

[15] Y. O'Connor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by Design: Informed Consent and Internet of Things for Smart Health," *Procedia Comput. Sci.*, vol. 113, pp. 653–658, Jan. 2017.

[16] S. Darwish, I. Nouretdinov, and S. D. Wolthusen, "Towards Composable Threat Assessment for Medical IoT (MIoT)," *Procedia Comput. Sci.*, vol. 113, pp. 627–632, Jan. 2017.

[17] A. Abdelgawad and K. Yelamarthi, "Internet of things (IoT) platform for structure health monitoring," *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017.

[18] Abinaya, V. Kumar, and Swathika, "Ontology based public healthcare system in internet of things (IoT)," presented at the Procedia Computer Science, 2015, vol. 50, pp. 99–102.

[19] R. Cortés, X. Bonnaire, O. Marin, and P. Sens, "Stream processing of healthcare sensor data: Studying user traces to identify challenges from a big data perspective," presented at the Procedia Computer Science, 2015, vol. 52, pp. 1004–1009.

[20] P. M. N. Martins and J. A. McCann, "The Programmable City," *Procedia Comput. Sci.*, vol. 52, pp. 334–341, Jan. 2015.

[21] L. Tian, H. Wang, Y. Zhou, and C. Peng, "Video big data in smart city: Background construction and optimization for surveillance video processing," *Future Gener. Comput. Syst.*, vol. 86, pp. 1371–1382, Sep. 2018.

[22] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: A Model-based Security Toolkit for the Internet of Things," *Comput. Secur.*, vol. 54, pp. 60–76, 2015.

[23] S. Faieq, R. Saidi, H. Elghazi, and M. D. Rahmani, "C2IoT: A framework for Cloud-based Context-aware Internet of Things services for smart cities," *Procedia Comput. Sci.*, vol. 110, pp. 151–158, Jan. 2017.

[24] H. Chen, H. Hui, Z. Su, D. Fang, and Y. Hui, "Real-Time Pricing Strategy Based on the Stability of Smart Grid for Green Internet of Things," *Mobile Information Systems*, 2017. [Online]. Available: https://www.hindawi.com/journals/misy/2017/5039702/abs/. [Accessed: 24-Dec-2018].

[25] J. Shuja *et al.*, "Greening emerging IT technologies: techniques and practices," *J. Internet Serv. Appl.*, vol. 8, no. 1, p. 9, Jul. 2017.

[26] A. Al-Saadi, R. Setchi, and Y. Hicks, "Cognitive network framework for heterogeneous wireless networks," *Procedia Comput. Sci.*, vol. 60, pp. 216–225, 2015.

[27] K. Ashokkumar, B. Sam, R. Arshadprabhu, and others, "Cloud based intelligent transport system," *Procedia Comput. Sci.*, vol. 50, pp. 58–63, 2015.

[28] H. Lee, K. Ryu, and Y. Cho, "A Framework of a Smart Injection Molding System Based on Real-time Data," *Procedia Manuf.*, vol. 11, pp. 1004–1011, Jan. 2017.

[29] S. Simons, P. Abé, and S. Neser, "Learning in the AutFab – The Fully Automated Industrie 4.0 Learning

Factory of the University of Applied Sciences Darmstadt," *Procedia Manuf.*, vol. 9, pp. 81–88, Jan. 2017.

[30] S. G. Pease, P. P. Conway, and A. A. West, "Hybrid ToF and RSSI real-time semantic tracking with an adaptive industrial internet of things architecture," *J. Netw. Comput. Appl.*, vol. 99, pp. 98–109, Dec. 2017.

[31] M. Spadacini, S. Savazzi, and M. Nicoli, "Wireless home automation networks for indoor surveillance: technologies and experiments," *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, no. 1, p. 6, 2014.

[32] H.-Y. Kim, "A design and implementation of a framework for games in IoT," *J. Supercomput.*, vol. 74, no. 12, pp. 6516–6528, Dec. 2018.

[33] L. Catarinucci, D. De Donno, L. Mainetti, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An IoT-aware Architecture to improve Safety in Sports Environments," vol. 13, no. 2, pp. 44–52, Jun. 2017.

[34] T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within Industry 4.0 paradigm," *Procedia Manuf.*, vol. 13, pp. 1253–1260, Jan. 2017.

[35] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, "Intelligent Manufacturing in the Context of Industry 4.0: A Review," *Engineering*, vol. 3, no. 5, pp. 616–630, 2017.

[36] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018.

[37] B. Negash, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "LISA: Lightweight internet of things service bus architecture," presented at the Procedia Computer Science, 2015, vol. 52, pp. 436–443.

[38] L. Alonso, J. Barbarán, J. Chen, M. Díaz, L. Llopis, and B. Rubio, "Middleware and communication technologies for structural health monitoring of critical infrastructures: A survey," *Comput. Stand. Interfaces*, vol. 56, pp. 83–100, Feb. 2018.

[39] P. Fremantle and P. Scott, "A survey of secure middleware for the internet of things," *PeerJ Comput. Sci.*, vol. 2017, no. 5, 2017.

[40] R. Rondón, M. Gidlund, and K. Landernäs, "Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications," *Int. J. Wirel. Inf. Netw.*, vol. 24, no. 3, pp. 278–290, Sep. 2017.

[41] J. Guan, I. You, C. Xu, and H. Zhang, "The PMIPv6-Based Group Binding Update for IoT Devices," *Mobile Information Systems*, 2016. [Online]. Available: https://www.hindawi.com/journals/misy/2016/7853219/abs/. [Accessed: 24-Dec-2018].

[42] S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Mobility management for IoT: a survey," *Eurasip J. Wirel. Commun. Netw.*, vol. 2016, no. 1, 2016.

[43] G. K. Teklemariam, J. Hoebeke, I. Moerman, and P. Demeester, "Facilitating the creation of IoT applications through conditional observations in CoAP," *EURASIP J. Wirel. Commun. Netw.*, vol. 2013, no. 1, p. 177, Jun. 2013.

[44] R. Sokullu and E. Demir, "Investigating Energy Efficiency and Timeliness for Linear Wireless Sensor Networks," *Procedia Comput. Sci.*, vol. 37, pp. 24–31, Jan. 2014.

[45] B. Park, A. Hwang, and H. Latchman, "Design of Optimized Multimedia Data Streaming Management Using OMDSM over Mobile Networks," *Mobile Information Systems*, 2017. [Online]. Available: https://www.hindawi.com/journals/misy/2017/2867127/abs/. [Accessed: 24-Dec-2018].

[46] H.-W. Wang, "Efficient DFSA Algorithm in RFID Systems for the Internet of Things," *Mobile Information Systems*, 2015. [Online]. Available: https://www.hindawi.com/journals/misy/2015/942858/abs/. [Accessed: 24-Dec-2018].

[47] O. Galinina, K. Mikhaylov, S. Andreev, A. Turlikov, and Y. Koucheryavy, "Smart home gateway system over Bluetooth low energy with wireless energy transfer capability," *EURASIP J. Wirel. Commun. Netw.*, vol. 2015, no. 1, p. 178, Jun. 2015.

[48] A. Rodriguez, A. Ordóñez, H. Ordoñez, and R. Segovia, "Adapting NSGA-II for Hierarchical Sensor Networks in the IoT," *Procedia Comput. Sci.*, vol. 61, pp. 355–360, Jan. 2015.

[49] A. Ahmad, A. Paul, M. M. Rathore, and S. Rho, "Power Aware Mobility Management of M2M for IoT Communications," *Mobile Information Systems*, 2015. [Online]. Available: https://www.hindawi.com/journals/misy/2015/521093/. [Accessed: 24-Dec-2018].

[50] Y. Mehmood, C. Görg, M. Muehleisen, and A. Timm-Giel, "Mobile M2M communication architectures, upcoming challenges, applications, and future directions," *Eurasip J. Wirel. Commun. Netw.*, vol. 2015, no. 1, pp. 1–37, 2015.

[51] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digit. Commun. Netw.*, vol. 1, no. 1, pp. 1–19, 2015.

[52] A. Taufique, M. Jaber, A. Imran, Z. Dawy, and E. Yacoub, "Planning Wireless Cellular Networks of Future: Outlook, Challenges and Opportunities," *IEEE Access*, vol. 5, pp. 4821–4845, 2017.

[53] Z. Jiang, B. Han, P. Chen, F. Yang, and Q. Bi, "On Novel Access and Scheduling Schemes for IoT Communications," *Mob. Inf. Syst.*, vol. 2016, 2016.

[54] S. N. Khan Marwat, Y. Mehmood, C. Görg, and A. Timm-Giel, "Data aggregation of mobile M2M traffic in relay enhanced LTE-A networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2016, no. 1, p. 110, Apr. 2016.

[55] Y. Leng, Z. Chen, and Y. Hu, "STLIS: A Scalable Two-Level Index Scheme for Big Data in IoT," *Mob. Inf. Syst.*, vol. 2016, 2016.

[56] M. Kim, M. Asthana, S. Bhargava, K. K. Iyyer, R. Tangadpalliwar, and J. Gao, "Developing an on-demand cloud-based sensing-as-a-service system for internet of things," *J. Comput. Netw. Commun.*, vol. 2016, 2016.

[57] M. Ahmed, L. Liu, J. Hardy, B. Yuan, and N. Antonopoulos, "An Efficient Algorithm for Partially Matched Services in Internet of Services," *Pers.*

Ubiquitous Comput, vol. 20, no. 3, pp. 283–293, Jun. 2016.

[58] G. Casale *et al.*, "Current and Future Challenges of Software Engineering for Services and Applications," *Procedia Comput. Sci.*, vol. 97, pp. 34–42, Jan. 2016.

[59] D. Kyriazis and T. Varvarigou, "Smart, Autonomous and Reliable Internet of Things," *Procedia Comput. Sci.*, vol. 21, pp. 442–448, Jan. 2013.

[60] M. Blackstock and R. Lea, "IoT interoperability: A hub-based approach," in *2014 International Conference on the Internet of Things (IOT)*, 2014, pp. 79–84.

[61] Y. Jung, M. Peradilla, and A. Saini, "Software-defined Naming, Discovery and Session Control for IoT Devices and Smart Phones in the Constraint Networks," *Procedia Comput. Sci.*, vol. 110, pp. 290–296, Jan. 2017.

[62] B. Xiao, T. Kanter, and R. Rahmani, "Constructing Context-centric Data Objects to Enhance Logical Associations for IoT Entities," *Procedia Comput. Sci.*, vol. 52, pp. 1095–1100, 2015.

[63] M. Al-Osta, B. Ahmed, and G. Abdelouahed, "A Lightweight Semantic Web-based Approach for Data Annotation on IoT Gateways," *Procedia Comput. Sci.*, vol. 113, pp. 186–193, Jan. 2017.

[64] I. Sohn, "Small-World and Scale-Free Network Models for IoT Systems," *Mobile Information Systems*, 2017. [Online]. Available: https://www.hindawi.com/journals/misy/2017/6752048/abs/. [Accessed: 24-Dec-2018].

[65] P. Grace, B. Pickering, and M. Surridge, "Model-driven interoperability: engineering heterogeneous IoT systems," *Ann. Telecommun.*, vol. 71, no. 3, pp. 141–150, Apr. 2016.

[66] "Internet of things (IoT) design considerations for developers and manufacturers - IEEE Conference Publication." [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7962762. [Accessed: 24-Dec-2018].

[67] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci.*, vol. 34, pp. 532–537, 2014.

[68] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, Apr. 2018.

[69] A. N. Duc, R. Jabangwe, P. Paul, and P. Abrahamsson, "Security challenges in IoT development: a software engineering perspective," presented at the Proceedings of the XP2017 Scientific Workshops, 2017, p. 11.

[70] L. Marin, A. Jara, and A. Skarmeta Gomez, "Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier," *Math. Comput. Model.*, vol. 58, no. 5–6, pp. 1155–1174, 2013.

[71] F. Alam, R. Mehmood, I. Katib, and A. Albeshri, "Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT)," presented at the Procedia Computer Science, 2016, vol. 58, pp. 437–442.

[72] Y. H. Wang, K. Cao, and X. M. Zhang, "Complex event processing over distributed probabilistic event streams," *Comput. Math. Appl.*, vol. 66, no. 10, pp. 1808–1821, Dec. 2013.

[73] H. Rahman, R. Rahmani, and T. Kanter, "Multi-Modal Context-Aware reasoNer (CAN) at the Edge of IoT," *Procedia Comput. Sci.*, vol. 109, pp. 335–342, Jan. 2017.

[74] X. Su, H. Zhang, J. Riekki, A. Keränen, J. K. Nurminen, and L. Du, "Connecting IoT Sensors to Knowledge-based Systems by Transforming SenML to RDF," *Procedia Comput. Sci.*, vol. 32, pp. 215–222, Jan. 2014.

[75] A. Alkhalil and R. A. Ramadan, "IoT Data Provenance Implementation Challenges," *Procedia Comput. Sci.*, vol. 109, pp. 1134–1139, 2017.

[76] K. Julia, S. Kurt, and S. Ulf, "Challenges in Integrating Product-IT into Enterprise Architecture – a case study," *Procedia Comput. Sci.*, vol. 121, pp. 525–533, Jan. 2017.

[77] C. Armstrong, "Debug and analysis considerations for optimizing power in your internet of things design," in *2017 IEEE International Symposium on Electromagnetic Compatibility Signal/Power Integrity (EMCSI)*, 2017, pp. 15–19.

[78] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," *J. Syst. Softw.*, vol. 132, pp. 186–203, Oct. 2017.

[79] P. P. Ray, "A Survey on Visual Programming Languages in Internet of Things," *Scientific Programming*, 2017. [Online]. Available: https://www.hindawi.com/journals/sp/2017/1231430/abs/. [Accessed: 24-Dec-2018].

[80] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things: a survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 176–188, Aug. 2018.

[81] A. Wallgren, "As the IoT expands, agile is the way forward," *TechBeacon*. [Online]. Available: https://techbeacon.com/iot-expands-agile-way-forward. [Accessed: 24-Dec-2018].

[82] D. Gkouskos and J. Burgos, "I'm in! Towards participatory healthcare of elderly through IOT.," *Procedia Comput. Sci.*, vol. 113, pp. 647–652, Jan. 2017.

[83] S. Leminen, M. Westerlund, M. Rajahonka, and R. Siuruainen, "Towards IOT Ecosystems and Business Models," in *Internet of Things, Smart Spaces, and Next Generation Networking*, 2012, pp. 15–26.

[84] J. Favaro, "Strategic research challenges in the Internet of Things," in *IEEE International Conference on Research Challenges in Information Science (RCIS)*, 2015.

[85] H. H. Olsson and J. Bosch, "The HYPEX Model: From Opinions to Data-Driven Software Development," in *Continuous Software Engineering*, J. Bosch, Ed. Cham: Springer International Publishing, 2014, pp. 155–164.