International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 11055-11061

Internet of Things Architecture: Current Challenges and Future Direction of Research

M. A. Burhanuddin[1], Ali Abdul-Jabbar Mohammed[2], Ronizam Ismail[3] and Halizah Basiron[4]

[1,2,4] Faculty of Information and Communications Technology, UTeM, Melaka, Malaysia.
[3]Kolej Universiti Islam Melaka, Kuala Sg Baru, Melaka, Malaysia.

ORCID ID: [1]0000-0001-8976-7416, [2]0000-0002-7040-7098, [3]0000-0002-7570-4470

Abstract

The Internet of Things (IoT) is a new paradigm that can enable collecting and exchanging data that have never been attainable before. It able to communicate and report user's information in a more secure way. The reports of Cisco analysts estimate that the IoT will have more than 50 billion of smart sensors and other smart devices or gadgets, all connecting and communicating real time data on the internet by 2020. This will provide deeper insights with data analytics using the IoT paradigm to establish new business, enhance productivity and efficiency, and develop innovative revenue streams. Furthermore, the IoT architecture may combine features and technologies suggested by various methodologies. Since, this architecture is designed where the digital and real worlds are integrating and interacting constantly, various technologies are merged together to form IoT, such as; sensing technologies, pervasive computing, ubiquitous computing, internet protocols, smart objects, embedded parts, etc. When a regular device utilizes intelligent agents, it becomes a smart object. In this way, it is not only used to gather the environment information or interact with the physical world, yet more than that, it must be interconnected with various network devices to exchange and communicate data over the internet. Therefore, the significant measure of available data which is produced by the immense number of interconnected devices will offer opportunities to generate information that will deliver significant benefits to the economy, environment, individuals, and society. In this paper, we present past, current, and future direction of IoT. This paper provides overview and clear examination of the IoT architecture paradigm with the description of its fundamental requirements along with the implementation challenges and future directions. Thus, it will open issues that will face the IoT by new world generation.

Keywords: Internet of Things, Information System, Machine to Machine communications, Wireless Networking, Embedded Systems

INTRODUCTION

Today, Internet of Things (IoT) is a rising network of interrelated computing devices and sensors that contain embedded technology which is enable these objects to collect and exchange data with the Internet. The IoT incorporates various smart objects, which are allocated exceptional characters of its own [1]. It is a wide-ranging network of physical smart objects, i.e. devices, sensors, transports, and constructions, associated with programs, electronics, hardware and network connectivity that empowers these things to accumulate and exchange data. The unique identity administration is very significant for ensuring the system efficiency of IoT network [2]. Since IoT is a task-oriented network, there is a necessity to provide coupling relation among its unique identity's. The IoT allows the connected smart objects to remain distinguished and remotely controlled by the existing system, lead up to achieve upgraded accuracy, better efficiency, and monetary favourable position. All objects are unique and identifiable with the embedded software [3]. Due to the tremendous headways in the remote communication systems field, the deployments of mobile devices and global services expand quickly in the previous decade. Nowadays, the major role played by IoT is never again restricted to connect user devices and appliances over the Internet. Yet, it has been growing turning into a chance to interlink the physical world with the Cybernet world [4], prompting the rise of Cyber-Physical Systems. The idea of Cyber-Physical Systems introduces the coming era of embedded systems in Information and communication technology where computation and network interacting are joint with physical procedures. Accordingly, these systems control and deal with their dynamic forces to be proficient, solid, adaptable, and more secure [5], [6]. The information that represent the physical procedures are exchanged, prepared, and utilized as a part of the digital world, as example, information gathered by varies sensors. Yet, this information may likewise affect and impact the physical procedures by input feedback loops, such as, utilizing actuators [4]. The idiosyncrasies of Cyber-Physical Systems are including an integrated design of the Information and communication technology systems combined with the physical mechanisms to increase the general adequacy. Therefore, these lines being interestingly with the traditional systems for the reason of including electronics, processing, communication and technology in one operating system. The IoT is reached out with a huge number of sensors and actuators. Some late examinations into the studies assess that the IoT will comprise about 50 billion objects by 2020 [7].

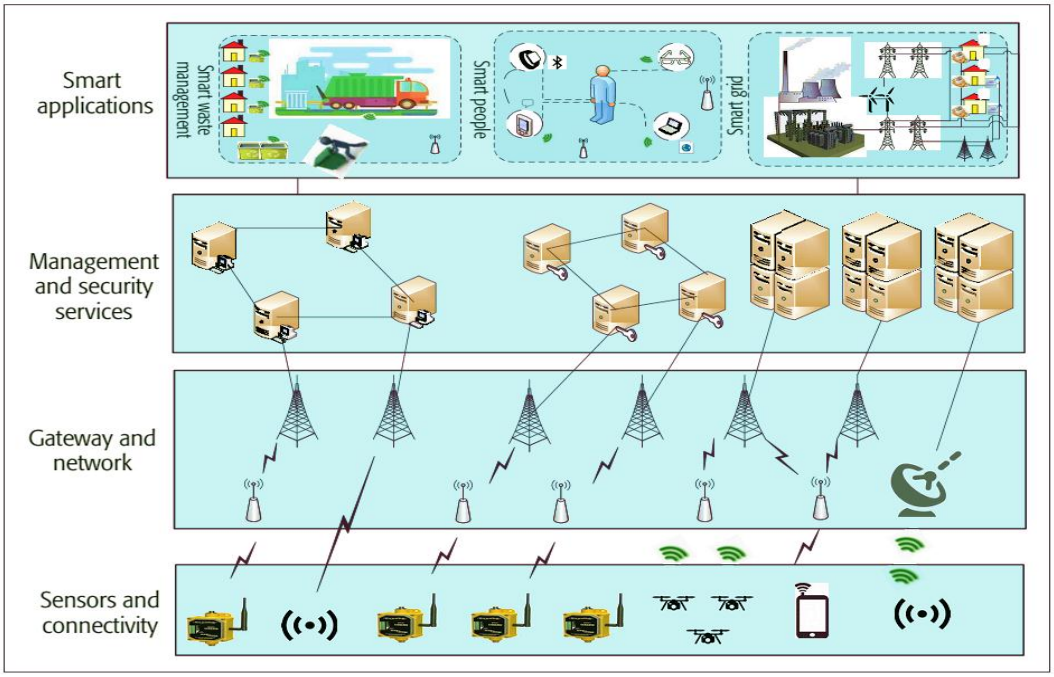

Figure 1: IoT Communication infrastructure [8]

THEORETICAL BACKGROUND

IoT is a complete system of interconnected smart devices involved in electrical, mechanical, and digital machines accompanied with the animals or people environments. These smart devices are equipped by unique identifiers and it can communicate through the network without needing of human interactions. The (Figure 1) demonstrates the foundation of IoT infrastructure and its connection associations.

As Luigi Atzori, et. al [9] talked about IoT as a system of interrelated computing devices, computerized mechanical machines, items, or individuals that are given typical identifiers and have the capacity to exchange data through the network without expecting human collaboration. In their study, IoT is proclaimed to be a fundamental system of connected smart devices or objects equipped with data gathering Technologies. Thus, those devices or objects can connect and communicate with each other autonomously. The machine-to-machine data that is created has an extensive variety of uses, but it is usually observed as a method to decide accountability of governing of real significance in the IoT [9]. As business proceedings and information interactions are brought out through that system, it is vital for the included groups to know how the individual activities will be examined. Besides, if commercial transactions fall flat for the reason of shortcomings in the system, organizations need to know whom to consider responsible. The likelihood of holding governing bodies responsible for their failures for the most part enhances their administrations because of the risk of approvals. The IoT, which needs to adapt to the particularities in the different portions of society, needs to catch up on a multi-stake holder approach way to deal with responsibility. Governance would get more grounded if norms were orchestrated in a way that makes governing bodies responsible, at any rate at the hierarchical organizational level of IoT. Daniele Miorandi, et, al. [10] investigated large and growing body of IoT, which envision digital and physical linked and appropriate information and communication technologies which businesses can rely on it. The information ought to be more fitting information and the more promptly accessible and recipients of accountability. Extraordinary thought has to be by [9], [10], which are concentrated on standards to be presented that considers representing bodies responsible and this help the improvement of security in IoT. Furthermore, Boundless organization of spatially distributed devices with embedded identification, detecting or incitation abilities are proposed.

In [10], [11], the researchers emphasized that virtual things like world-wide-web, internet or cloud will be presented more physical and replace hardware technologies in a near future. They proposed that which digital and physical can be connected means fitting information and communication technologies will improve virtualization for all areas in IoT. Daniele Miorandi, et, al. [10] introduced a study of Technologies, applications, and research challenges for IoT, while Verdouw et al. [11] appears on how IoT idea can be utilized to upgrade virtualisation of supply chains in the floricultural division. Giuseppe Colistra, et al. [12] detailed IoT model in communication between devices by placing knowledge into smart objects to be interconnected with one another over the internet to exchange their data and information. Thus, the full transparency is obtainable with not so much inefficiencies but rather additional quality. They design intelligence insight by actualize key interoperability abilities into smart objects in a

case study. This is by get resource allocation for the placement of distributed applications in the IoT and open issues and identified problems and difficulties in research to be confronted with the IoT recognition in the real application. Giuseppe Colistra, et al. [12] revealed on emerging all kinds of smart object that implement systems of cooperative intelligent nodes or objects. By using IoT, they proved promising paradigm that provide a pervasive information access through cooperation among nodes. Sahraoui Somia, et al. [13] enhanced the model provided in [12] by showing different methods for both studies. They proposed a compromise protocol for the participation among network objects in accomplishing the target application. Besides, they suggest an IPv6 over Low-power Wireless Personal Area Networks compression for the header of Host Identity Protocol packets, as well as, an adjusted sharing structure of security computational load in HIPBaseEXchange. The distinctive case studies examination for [12], [13] are utilized resource allocation for the deployment of distributed applications in the IoT. Correspondingly, the design and functionalities of appropriate middleware that tends to a conceivable reaction for this matter, material and technological heterogeneity. Furthermore, the asymmetric behaviour of the communications between the sensor nodes and the conventional Internet hosts are making security a challenging issue [14], [15].

In [13], [16], the researchers discussed the challenging problem of security about the technological heterogeneity of IoT technologies along with the asymmetric behaviour in communications among the conventional Internet hosts and the sensor nodes. They proposed a similar objective which is incorporated in the management structure for IoT devices. Perhaps, adequately energy proficient with a little settlement delay of security, underpins effective assessment of security strategies to empower the assurance and protection of client data. Ricardo Neisse, et. al [16] examined security and data quality risk of using IoT technologies. The researcher proposed a different model "Based Security Toolkit Model", which is coordinated in a management framework for IoT devices. Furthermore, in the distributed IoT architecture, a light weight and cross-domain prototype is proposed. This prototype is giving least data caching functionality likewise in-memory data handling. Sabrina Sicari, et. al [17] presented algorithms that can be used for the evaluation of data quality and security. The algorithms incorporate determination and effective assessment of security strategies to empower the assurance and safety of IoT data. The research studies in [17], [18] have common goals as the huge amount of heterogeneous interconnected devices and the omnipresence of IoT devices increase the demand of jointly security and privacy requirements. They examine the light weight and cross-domain prototype that proposed for the distributed architecture of IoT, giving least data caching functionality as well as minimum in-memory data handling. They also carried out detail performance evaluation for the widely utilized cryptographic algorithms on constrained objects or things which is accustomed in IoT networks.

CRITICAL LITERATURE AND ANALYSIS

The IoT have developed from the integration of internet systems, wireless technologies, microservices, micro-electromechanical, and electrical fields. The modern technologies certainly create viability of the IoT concept. The (Figure 2) summarized the adoption of different connectivity technologies in IoT domain. However, These technologies are not amalgamate with the scalability and efficiency that they would demand [9]. With the due concern of the IoT applications by various industries, Luigi Atzori, et al. [9] believe that orating these topics in upcoming years will be a dominant driving factor for networking and communication researches in both industrial and academic fields.

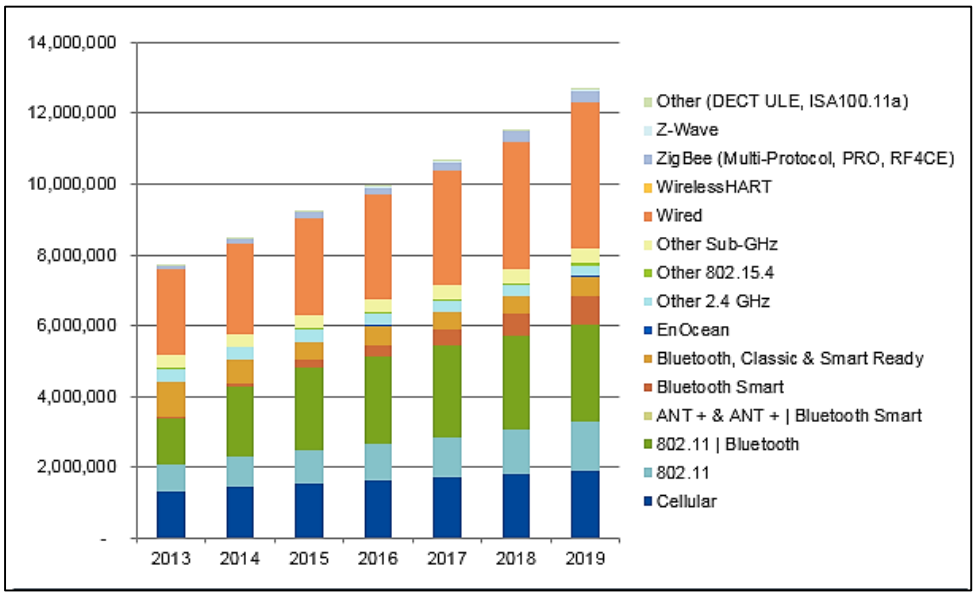

Figure 2: the adoption of different connectivity technologies in IoT

According to Weber [19], the utility of development in technologies are to:

- improve participation procedures;
- offer information on significant concerns for the community and civil society in good time.
- form the opportunities as the elementary contrivance to interchange of perceptions.
- deliver adequate context and background information for literature to assist the concerned market participants to apprehend the subjects being the topics of accountability.
- explain authorizations regarding non-compliance with accountability necessities.

Moreover, it leads to alleviate the security in the IoT. The exploration in this segment indicates that impending challenges are rather alarmed with functional and organizational matters than just technology problems (like most IoT trials as sermonized in literature) [11]. Verdouw [11] presented work on the design and implementation of novel elucidations for the discoursed challenges in the supply chain. The paper has measured how the IoT can ameliorate virtualization in floriculture. Daniele Miorandi, et al. [10] presented a synopsis of the vital topics allied to the development of IoT technologies and services. Numerous research challenges have been empathized such as security, which are anticipated to turn into major research trends in the future [10]. Additionally, Borgia [20] discussed the major challenges that must be encountered to sustain the IoT vision, which encompasses varies areas to study, such as: data management, data processing, discovery, architecture, communication, handling security and privacy, etc. Various recommended solutions have been proposed, which are intended for resolving those challenges. Nevertheless, these proposed solutions are not comprehensive and do not deal with all the different characteristics. Consequently, many undeveloped matters reckons for suitable solutions [20].

The outcomes of the assessment had an obvious reveal that the solution is adequately efficient in energy saving within dual category-messages communication and security establishment [13]. A few instruments and studies treat the security and protection of privacy in the IoT [18]. Furthermore, Ricardo Neisse, et. al [16] revealed that the trust is an efficient factor for using IoT. In the previous literature, numerous factors have been well observed and studied, for example; security, trust, privacy protection, etc. These factors and aspects are serving the IoT but insufficient enough to address and handle it in public and private sectors. Therefore, many studies need to be done in this field by researchers in the future. Moreover, IoT needs more attention from non- academic disciplines such as, software and architecture engineers. The patterns of convergence have supported the conjunction between the information technology and operational technology. This is permitting the unstructured data, which is generated by operational machines to be investigated for knowledge insights that will drive continual enhancements.

IoT IMPLEMENTATION REQUIREMENTS

The IoT implementation requirements are considered as critical requirements for the upcoming IoT architectures, which are described in the following subsections:

- **Scalability:**

With the huge number of objects that connected to the IoT infrastructure, it is considered that every connected object has its own virtual representation [21]. Therefore, scalability requirement is desirable to extend the functionality of open standards for future IoT applications. Moreover, while the expansion of IoT is growing via the widespread adoption of new applications, the future IoT architectures must be meet scalability requirements.

- **Interoperability:**

The requirement of empowering the communications amongst various objects by different service providers is highly important in the future IoT architectures [22]. Therefore, the IoT architectures requires interoperability standards to create parallel or open platforms that support the comprehensive potentials of seamless connection practice among all types of IoT applications and devices. Moreover, to enable the communication practices amongst all things in the future IoT architectures regardless of its origin.

- **Security:**

Strengthening security is a significant aspect of IoT applications, due to the challenging task of protecting the sensitive information transmitted and processed in the hostile environments around IoT [23]. Thus, it can be truly considered as a future key requirement of IoT deployments to prevent these large scales of IoT applications being controlled by unauthorized parties. Moreover, the security mechanisms of IoT design strategy should be a lightweight enough because of resource constrained properties of IoT devices. Accordingly, the lack of security policy the future IoT architectures can threaten the users trust, so this will lead up to the failure of the whole technology [24].

- **Resource Control and Management:**

The accessibility and configuration of the participating smart objects among IoT applications should be performed remotely. This will help controlling the resources efficiently if the administrators are not available at their certain places. Besides, redundant resource constraints may affect the IoT systems, which need to balance the load for appropriate resource utilization [25].

- **Energy Efficiency:**

The life time is the most functioning sustainability apprehension in the smart objects that participating among IoT applications [17]. Therefore, the energy awareness is very important to reduce the resource constraints by eliminating redundant energy consumption. Accordingly, the design strategy of IoT architecture should be minimize energy consumption by the development of lightweight properties of the communication techniques and methods.

- **Quality of Service (QoS):**

The ability of providing satisfactory service to users is a significant requirement of IoT system architectures. QoS is a non-functional facility factor, that can be obtained by organizing the services provided and retrieval [15]. As example, real time processing applications impose a high precedence to perform typical performance. Correspondingly, only the compulsory information should be retrieved in response to the addressed request.

DISCUSSION ON CHALLENGES AND FUTURE DIRECTION IN IoT ARCHITECTURES

Several requirements have to be accomplished to achieve a functional implementation of IoT architecture. The section discusses some of the issues and challenges that remaining for implementing the future IoT system architectures. The purpose is to provide a clear examination for the current challenges and give some research directions in the IoT domain. Therefore, we will focus in this paper on the issues and challenges regarding scalability, interoperability, and security requirements in the IoT architecture, as the following:

- **Scalability:**

With the huge number of interacting entities, the future IoT systems are expected to deal with numerous challenges because of the significant differences in the interaction patterns and communication behaviours [26]. The challenge of providing available service to the different types of IoT devices concerning their demands is very critical for the reason of the various and plentiful applications of IoT. Thus, it a requirement to scale up the IoT architectures to handle huge number of connected entities. The scalability development process of IoT systems can be accelerated with the fast-growing number of IoT devices [27]. Nevertheless, the existing scalability management protocols do not deal well with the rapid expansion of IoT devices due to their resource limitations and constraints.

- **Interoperability:**

The interoperability challenges in the future IoT applications can be divided to three main challenge types as follow:

The technical interoperability challenges: this type of challenges has a concern with the capabilities, standards, and protocols of the IoT connected devices, which are aiming to support seamless connection practice within the same computing paradigm among all types of IoT applications. Therefore, the successful technical interoperability can be achieved through the implementation of agent based mediation among all IoT related standards, and protocols.

The semantic challenges: is the apprehension of the ability of different components in IoT architecture to be trustworthy for processing and handling the exchanged data.

The pragmatic challenges: is the apprehension of the ability of the IoT system to observe the intentions of different participating parties. Therefore, the requirement of pragmatic interoperability can be realized by the design a predefined specifications strategy for the components and behaviour of the IoT system.

- **Security:**

The IoT architecture is complex in nature because of the vast range and heterogeneity of IoT applications, which leads to several security challenges [23]. This IoT architecture is assumed to deal with billions of sensors and objects, which are interacting with each other and with other entities, such as human beings or virtual entities [28]. It is essential to secure and protect all these interactions with preservation of the highest system performance and limiting total incidents which are affecting the entire IoT system. The implementation of security standards can be delivered through the bottom-up manner. The IoT architecture should follow the bottom-up manner by delivering a secure system booting process, end user authentication procedures, firewall regulations, and access control rules. Furthermore, the IoT system must track and follow the security updates and patches in non-disruptive direction. Accordingly, it is essential to apply the appropriate security mechanisms for all IoT system levels and stages with the physical and non-physical system components.

CONCLUSION

The expansion of computational objects and things have been equipped with communication and interactive capabilities of embedded intelligence. This innovation motivates in the direction of the rapid development of the IoT field. Toward the emergent IoT paradigm, a global dynamic network will connect everything and anything by forming virtual linkage of integrated and addressable devices. Henceforward, the consequence will boost users to expand novel solutions to be a durable and powerful fundamental structure to the worldwide. Consequently, the trends of IoT domain have been discussed in this paper in the perspective of different research areas such as; architecture, data management, data processing, communication, security and privacy. Thus, this paper provides overview and clear examination of the essential definition of IoT architecture paradigm. Finally, we have discussed the main

IoT fundamentals along with the implementation challenges and future directions of its requirements.

ACKNOWLEDGEMENT

The authors would like to thank UTeM Zamalah scheme, Universiti Teknikal Malaysia Melaka (UTeM) for providing financial support and facilities in this study. Also, gratefully we would like to acknowledge and thank Kolej Universiti Islam Melaka (KUIM) to support this research.

REFERENCES

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[2] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things???A survey of topics and trends," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015.

[3] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012.

[4] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Tröster, G. Tsudik, and F. Zambonelli, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyberphysical convergence," *Pervasive Mob. Comput.*, vol. 8, no. 1, pp. 2–21, 2012.

[5] L. Insup, O. Sokolsky, I. Lee, O. Sokolsky, C. Electronic Design Automation, A. C. M. S. I. G. on D. Automation, C. Ieee, L. Insup, O. Sokolsky, I. Lee, O. Sokolsky, C. Electronic Design Automation, A. C. M. S. I. G. on D. Automation, C. Ieee, L. Insup, and O. Sokolsky, "Medical Cyber Physical Systems," *Des. Autom. Conf. (DAC), 2010 47th ACM/IEEE*, pp. 743–748, 2010.

[6] S. Barro-Torres, T. M. Fernández-Caramés, H. J. Pérez-Iglesias, and C. J. Escudero, "Real-time personal protective equipment monitoring system," *Comput. Commun.*, vol. 36, no. 1, pp. 42–50, 2012.

[7] S. Agrawal and D. Vieira, "A survey on Internet of Things," *Abak{ó}s, Belo Horiz.*, vol. 1, no. 2, pp. 78–95, 2013.

[8] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, 2017.

[9] L. Atzori, A. Iera, and G. Morabito, "The Internet of Thinags: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[10] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7. pp. 1497–1516, 2012.

[11] C. N. Verdouw, A. J. M. Beulens, and J. G. A. J. van der Vorst, "Virtualisation of floricultural supply chains: A review from an internet of things perspective," *Comput. Electron. Agric.*, vol. 99, pp. 160–175, 2013.

[12] G. Colistra, V. Pilloni, and L. Atzori, "The problem of task allocation in the Internet of Things and the consensus-based approach," *Comput. Networks*, vol. 73, pp. 98–111, 2014.

[13] S. Sahraoui and A. Bilami, "Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things," *Comput. Networks*, vol. 91, pp. 26–45, 2015.

[14] M. Gerla, D. Maggiorini, C. E. Palazzi, and A. Bujari, "A survey on interactive games over mobile networks," *Wirel. Commun. Mob. Comput.*, vol. 13, no. 3, pp. 212–229, 2013.

[15] W. Wang, S. De, R. Toenjes, E. Reetz, and K. Moessner, "A comprehensive ontology for knowledge representation in the internet of things," in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012, pp. 1793–1798.

[16] 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.

[17] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "A secure and quality-aware prototypical architecture for the Internet of Things," *Inf. Syst.*, vol. 58, pp. 43–55, 2016.

[18] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," *Comput. Networks*, vol. 102, pp. 83–95, 2016.

[19] R. H. Weber, "Accountability in the Internet of Things," *Comput. Law Secur. Rev.*, vol. 27, no. 2, pp. 133–138, 2011.

[20] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54. pp. 1–31, 2014.

[21] D. Uckelmann, M. Harrison, and F. Michahelles, "An Architectural Approach Towards the Future Internet of Things," in *Architecting the Internet of Things*, 2011, pp. 97–129.

[22] A. Bröring, S. Schmid, C. K. Schindhelm, A. Khelil, S. Käbisch, D. Kramer, D. Le Phuoc, J. Mitic, D. Anicic, and E. Teniente, "Enabling IoT Ecosystems through Platform Interoperability," *IEEE Softw.*, vol. 34, no. 1, pp. 54–61, 2017.

[23] J. Carlson, B. Creighton, D. Meyer, J. Montgomery, and A. Reiter, "The Internet of Things : Security Research Study," 2015.

[24] G. Matuszak, G. Bell, and D. Le, "Security and the IoT ecosystem," *Kpmg*, 2015.

[25] A. Sehgal, V. Perelman, S. Kuryla, J. Schonwalder, and O. In, "Management of resource constrained devices in the internet of things," *Commun. Mag. IEEE*, vol. 50, no. 12, pp. 144–149, 2012.

[26] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling technologies for green internet of things," *IEEE Syst. J.*, vol. 11, no. 2, pp. 983–994, 2017.

[27] Y. Shen, T. Zhang, Y. Wang, H. Wang, and X. Jiang, "MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 86–93, 2017.

[28] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.