International Journal of Engineering & Technology, 7 (2) (2018) 956-961

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Internet of things between reality or a wishing-list: a survey

Mowafaq Salem Alzboon *

[1] *Faculty of Science and Information Technology, Jadara University, Irbid, Jordan*
**Corresponding author E-mail: malzboon@jadara.edu.jo*

Abstract

Internet of Things is considered to represent a platform in which daily devices and their processing get more intelligent than ever where daily communications get further informative. While the Internet of Things remains searching its particular shape, its influences have gazed in producing inconceivable steps as a universal solution media pertaining to the linked scenario. The architecture of particular research regularly controls the confirmation pertaining to the corresponding domain. The lack of the whole architectural knowledge is currently motivating researchers to obtain the scope related to Internet of Things centric methods. The literature reviews the Internet of Things oriented architectures, which can develop the comprehension of corresponding technology, method, and tool in order to ease the requirements related to a developer. Additionally, research issues are examined to integrate the lacuna within the present tendencies of particular architectures in order to inspire many organizations and academics to search for conceivable methods that are inconsistent with the precise robustness of Internet of Things. The major contribution related to this paper is based on summarizing the present state-of-the-art regarding the Internet of Things by highlight technical, sensing issues as well as the future direction toward.

Keywords: *Internet of Things; Mobile Crowd Sensing; Sensorsnetworks; Service-Oriented Architecture*

1. Introduction

Internet of Things (IoT) is commonly being a current disseminated and everywhere found network model presenting disseminated and transparent facilities [1]. Based on the IoT notion, several intelligent devices are linked together, such as mobile phones, sensors, and many different intelligent devices. Such intelligent devices are able to connect with each other and interchange information [2]. Based on the IDC statistical report, more than 50 billion IoT devices around the globe can produce more than 60ZB data by 2020 [3]. By gathering the data related to these IoT devices and analyzing such data for sensing and comprehending the atmosphere, complicated systems are created in order to improve life's quality, such as the situation of the machine condition, human body performances, health monitoring, localization and operational monitoring [2]. Based on the commonly and frequently used IoT, enormous sensors and devices are creating enormous data and many different IoT applications are improved in order to obtain further accurate and fine-grained facilities for users. Such IoT big data are more operated and analyzed for providing intelligent performance for IoT service users and providers [4]. The evolving IoT applications include several data-driven analytic processes for effectively using big IoT sensing data [5]. Currently, AI algorithms are presented through IoT data analytic processes [6]. During the last decade, Artificial Intelligence (AI) performed an efficient performance by improving computing technologies related to cloud computing, Graphics Processing Unit (GPU) computing and further hardware improvements [7]. Machine learning is considered to be the most illustrative AI algorithm that has is being used through many domains, comprising Natural Language Processing (NLP), decision making, speech recognition, intelligent control, computer vision, and computer graphics. Likewise, machine learning provides a possible advantage for a computer network [8]. Few studies are performed in order to understand the way machine learning is being used for solving various networking issues, such as security, resource allocation, traffic engineering, and routing [9]–[11]. Machine learning is considered to be an important technology for an autonomous smart/intelligent network management and operation. In particular, the majority of IoT systems are being increasingly complicated, heterogeneous and dynamic. Therefore, managing such IoT systems is considered an uneasy process. Furthermore, the facilities of these IoT systems are required to be further enhanced based on their efficiency and variety to entice as many users as possible. Several studies have applied machine learning to IoT. Consequently, it is found that IoT is able to get advantage from gaining assistance from machine learning. By applying machine learning for IoT allows users to acquire deep analytics and improve effectiveness for various smart IoT applications. The reason behind this is that machine learning offers seamless solutions for mining information and invisible characteristics in IoT data [12], [13], [22], [14]–[21]. The rest of the paper is outlined as follows. Section 2 discusses the open technical issues of the IoT. Section 3 explains the use of open mobile crowd sensing issues for IoT devices. Section 4 highlights the future direction toward IoT. At last, the paper is concluded in Section 5.

Copyright © Mowafaq Salem Alzboon. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Open technical issues

This section analyses different technical issues that are in relation to the present IoT architectures. It is commonly known that IoT applications and technologies remain within their infancy [23], [24]. There exist extensive research issues for organizational use (e.g. privacy, security, standardization, and technology) [25]. Future efforts are required to highlight such issues and test the features of various organizations in order to assure an appropriate fit of IoT devices within human-centric environments. An adequate understanding of organizational features and needs on such factors as risk, privacy, security, and cost, which are definitely needed prior to applying IoT that is commonly being agreed to be distributed through to the entire fields [14]. Accordingly, some issues are discussed, which comprise:

a) IoT is an extremely complex heterogeneous network platform, and hence, it improves the complexity through many different kinds of devices based on several different communication technologies that show the unwanted performance of a network to be non-standardized, delayed and fraudulent. The authors in [12], [22], [26] state that linked objects are managed based on simplifying co-operative performance among various components, such as software services and/or hardware components, and managing them after delivering an address, identification and optimisation through to particular protocol and architectural levels, which is considered a critical research issue.
b) Design of Service-oriented Architecture (SoA) for IoT is considered to form an enormous issue where service-based objects might encounter different issues from performance and cost problems. The SoA requires managing an enormous number of devices that are linked to the system that addresses different scalability problems. Currently, such issues as management, processing, and data transfer issues are considered an encumbrance based on service provisioning [27].
c) IoT is degraded over a conventional network oriented ICT atmosphere. It is regularly influenced by any connection with it. Accordingly, the demand for united information infrastructure is required to be accomplished. An enormous number of linked devices provide real-time data flow that should be managed by an increased bandwidth frequency path [28]–[30]. Consequently, a uniform architectural base is generated in order to sophistically fulfill the requirements pertaining to infrastructure.
d) In terms of the network services, it is obvious that a lack of a Service Description Language (SDL) exists. Otherwise, it would make the service development, deployment, and resource integration would not be easy to expand the product distribution time leading to a loss in the market. Therefore, a well-known consented SDL must be generated in order to implement object naming services and robust service discovery approaches along together [31], [32]. Novel SDL can be improved to deal with product distribution after assessing the requite SDL particular architecture [22].
e) The originated data might be extremely massive with its size by which a new database management system cannot manage in a real-time way. Proper solutions are required to be optimized. IoT based data is created at a fast speed. The collected data from the end of the receivers are efficiently maintained in which a new RAID technology is incapable of an IoT based data service-centric architecture is required to be studied in order to manage this issue.
f) Data is defined as a raw fact, which regularly does not deal with unrelated handouts. In terms of IoT, a significant role is considered as an action to be taken by data for decision making. The data value is obtained after the filtering phase is conducted over a pool of data. Such expressive information is just provided by an orientation of understanding, analyzing and mining it. Big data issue is considered adequate for managing the same regression. It is obvious that the related architectural framework could have analytics, data mining and decision making facilities. The big data domain is possible to be gathered accordingly [33].
g) Various devices are connected to IoT, which puts down data of many different types, sizes, and layouts [28], [33]. Such disparities must be engaged with a futuristic technology that includes multi-varied architectural ideas pertaining to its optimum indentation. A researcher must be able to propose a new large IoT Data particular design where data is effectively managed.
h) Additionally, organizations should search for issues of hardware-software coexistence within IoT. Many different devices are connected with various communication protocols within TCP/IP or improved software stacks can definitely operate web services that are performed through many different middleware solutions [5], [34]. Specific architecture leveraging the simplification of heterogeneous protocols is planned.
i) The IoT is perceived in order to involve an extremely increased number of nodes. The whole connected devices and data are retrievable. Accordingly, the unique identifier should be provided for an effective point-to-point network configuration. IPv4 protocol determines every node within a 4-byte address. Additionally, it is common that existing IPv4 numbered addresses are rapidly reduced by approaching to zero address within the following few years where new addressing policies will take into effect where IPv6 is a robust contender. This is a region where the maximum care is required to track the ability of device identification and naming where the suitability of architectural proficiency should be taken into account [35], [36].
j) The extensive applicability related to IoT and different related technologies will massively be based on the network security cum information and data privacy defense [33]. Being increasingly complicated and heterogeneous in nature, IoT frequently encounters risky privacy and security threats.
k) Based on the perspective of service, the non-existence of a well-known consented service description language switches the service improvement and resources incorporation of physical items through to value-added services in an uneasy manner. The improved services can be dissonant with various applied and communicative atmospheres [25]. Furthermore, robust service discovery approaches and item naming services should be improved in order to disseminate the technology of IoT [37], [38]. Scientists must pave original constructions in order to manage such problems.
l) Standardization is an extra clot that might exactly be performed for developing IoT. Standardization in IoT indicates to lesser primarily barriers pertaining to active users and service providers, creating interoperability problems among various methods or applications and to observe more effective competition within the improved services or products through the level of application. Identification standards, communication standards, and security standards are required to get involved based on disseminating IoT technologies when formulating developing technologies within a horizontal equivalence. Additionally, fellow researchers represent industry-particular guidelines and stipulate demanded and significant architectural standards for effective application of IoT [21], [28].

Complexity, mobility and deployment represent the major issues, which limit IoT to be protected [12], [15], [17], [39], [40] declare that privacy defense in IoT atmosphere is further vulnerable in comparison with the conventional ICT network because of the increased number of existing attack vectors over IoT entities. For instance, IoT-based health care monitoring system gathers the data pursuant to the involved patient, such as respiration, body temperature, pulse, heart rate and so on. After that, it immediately delivers the information through to the hospital or physician's office based on a particular network. As the time of data transfer over the network, if the patient's data is taken or mislaid, severe risks might emerge leading to death occurrence for the user. Based on this case, it is realized that privacy is not included by the majority of architectures, and security concepts within the respective concept that is a disadvantage, which requires

to be elucidated. However, available network security technologies allow IoT to be preserved from many different intimidations where further works remain to be taken into consideration. A robust, efficient and consistent security protection method for IoT is considered the highest of most priority.

The authors in [24] depict that the subsequent topics for which a research is conducted comprise: (i) a definition of privacy and security from a cultural, legal and social perspective, (ii) reputation and trust management, (iii) end-to-end encryption, (iv) user data and privacy of communication, and (v) applications and security on services. It is more comprehended that despite the fact that available network security technologies give a base for security and privacy within IoT, further progress remains to be carried out.

A consistent security protection method for IoT requires to get studied and determined based on the subsequent concepts: (i) The definition of privacy and security from the perspective of culture, legal and social manner; (ii) reputation and trust method; (iii) communication security, for example, an end-to-end encryption; (iv) user data and privacy of communication; (v) applications and security on services [24].

3. Open mobile crowd sensing issues

a) Resource confines: Sensing devices, such as cellular and sensors normally possess a limited number of resources, and resource restrains emerge as an issue for crowd sensing. Although further resources, such as bandwidth and computing are given to cellular in comparison to mote-class sensors, cellular remain encountering the issue of resource restrains [41]. Various kinds of sensed data can be independent of each other due to the multi-modality sensing abilities of sensing devices. In real-world scenarios, various kinds of sensed data are applied for a similar purpose. Nonetheless, the varieties over the resource and quality consumption pertaining to the sensed data encounter a consequence for developing data quality with reduced resource consumption. Consequently, such a case remains an issue for developing data quality and reducing resource consumption [32].

b) Data integrity, security, and privacy: The sensing devices can possibly gather sensitive data about many users [18], [22], [42]–[44], and hence, privacy appears to represent an important consequence. For instance, GPS sensor readings normally store the private information of users, such as the routes they obtain at their daily travels and regions. By disseminating the GPS sensor measurements, the privacy of users is likely to be identified. Therefore, it is significant to protect the privacy and security of a user. Additionally, the GPS stores the information that is derived from daily travels that are disseminated through to an enormous social and is applied to understand the information of traffic congestion within a city [19], [32].

c) Automated configuration of sensors: through conventional pervasive/omnipresent computing, just a restricted number of sensing devices (e.g. sensors) are linked through to different implementations, such as smart river and smart farm. Nonetheless, a massive number of sensing devices in IoT are anticipated to get linked all with each other through the Internet. Consequently, the configuration and connection of sensing devices to applications represent an important issue that needs to be further solved. It is not possible to link the entire sensing devices in a manual way through to middleware or to an application [45]. A semi-automated or automated procedure must exist to link sensing devices with many different applications. In order to achieve the functions of linking sensing devices with various applications, it is important that such applications could be able to understand the sensing devices (e.g. to understand their abilities). Many current improvements like the Transducer Electronic Data Sheet (TEDS), Open Geospatial Consortium (OGC) Sensor Web Enablement related standards as Sensor Markup Languages (SensorML) represent the future tendencies of conducting research progress for highlighting the issue of configuration and connection of sensors to applications [46].

Hence, it is important to involve the crowd sensing implementations in order to make users comprehend what surrounds them more effectively and to eventually take advantage of their information dissemination. In order to efficiently protect a large quantity of private information for users, not just methodological performances are required but are systematic researches as well. In [47], the AnonySense architecture is produced in order to improve many different privacy aware implementations according to the crowd sensing issue. Additionally, it is significant to ensure that a user's data is not identified to unreliable third parties. For instance, malicious users normally subsidize to enhance an erroneous sensor data. By referring to their particular advantage, these users can deliberately contaminate the sensing data. The inexistence of control methods for ensuring data accuracy and source validity may lead to encounter different information credibility problems. Accordingly, it is significant to enhance trust protection and abnormal detection techniques in order to assure having an appropriate quality pertaining to the acquired data. Furthermore, the issue of data integrity which assures the integrity of users' sensor data requires to be efficiently mentioned. Although a few methods in [36] and [18] are produced, they are practically based on a co-located substructure, which might not be connected as a witness and encounter inadequate scalability that produces some types of methods that are prohibitive and not existing at all times. The ground around this refers to the fact that the method is based on the inputs that are derived from structuring a cost-effective connection. A further method for managing the issue of data integrity relies on signing the sensor data, such as reliable built-in hardware on cellular is being applied for such a need). In other words, an SHA-1 digest relates to the sensor data is signed by a reliable platform module. Such a method is considered problematic because of the involved verification procedure that is performed within the given software.

4. Future direction toward IoT

The subsection suggests particular and typical implemented methods that are not mentioned in the literature or are not supported by the entire research societies. The IoT indicates to an Internet of any architecture (where 'IoT' is normally assumed to be 'all' in computing). Architectures are unceasingly acquiring significance and can manage the lower basis of IoT. According to the architect's/developer's perspective, the initial job of formulating a new philosophy to be implemented is based on establishing an important method that represents the covered contents and the way these contents are linked together. An extensive study must highlight a novel notion based method for completing the subsequent details, which comprise: social, defense, automation, sports, governance, tourism, robotics, and mining. Since IoT remains within its emerging phase, IoT must be taken into account in order to appropriately generate an effect. Intelligent healthcare, demotics, transport, agriculture, and environment are presently being searched for based on IoT [48]. Researchers are continually working toward obtaining essential platforms for solving these issues within the upcoming future. The IoT aspect revolutionizes IoT technologies by covering unhandled regions including the combined ones. This will handle the diagonal, vertical, crisscross and horizontal through the entire major contents related to the IoT through to the generalized implementations. IoT is entirely a hypothetical aspect, which should be followed by. Hybrid, digital, and analogy items must represent the 'things' part. Not just solid, but as well liquid, partially liquid and crystallized kind of materials can form a partition of it. System on the lab, Integrated Chips (IC), FPGA, lab on chip

and ASIC, flexible electronic items reduce the distance between pure digital and digital method. The standard OSI network method is to be revisited for improved layer based IoT. The entire network protocols must suitably be used within its particular layers. CoAP, MQTT, web sockets, XMPP, SOAP, RESTful, and IPv6 are involved in a new method such that scripted web-based pages would talk to the portion by benefiting from NoSQL, SPARQL, Graph database, parallel database, Hadoop, HBase, RDF, OWL oriented setups. Task manager, API moderator, APP based Plug-in enabler, storage monitor, service coordinator, risk analysis, resource management, predictive analyzer, data analytics, and graphical visualization are entirely installed in order to extemporize IoT-as-a-Service (IoTaaS). Limitless implementations roof up the layer in order to alleviate the user's experience towards a new height. Human being cherishes augmented maps, environment monitoring, health track, identification and sensing, smart city, governance, smart transportation, loss apprehension, mobile ticketing, smart plant, smart taxi, intelligent museum, comfortable home, historical queries, data collection, theft monitoring, enhanced game environment, theft monitoring, logistics, assisted driving and social networking.

Mining sites are enclosed by IoT where tourism, defense, travel, and sports tools are linked together. RSA, SHA-3, 3-DES and AES algorithms required to be studied in order to be fitted within the control of a resource. Multimedia might rely on IoT by capturing many different streaming algorithms while discrete messages are attached after encountering many different payloads related to transmitted packets. ''Sensor Model Language" (SensorML) is revised in order to bring a strong and semantically-tied meaning of outlining different procedures and operative contents that are in relation to the post-measurement and pre-measurement conversion of particular annotations (Open geospatial) [49]. The basic aim of the SensorML operates the interoperability by applying semantic mediation and ontologies. This might be successively performed through semantic and syntactic levels where obtained sensors and procedures could be more effectively comprehended, used and disseminated by machines within complicated workflows, and among smart sensor web nodes, respectively. Most hybrid and digital devices related to the conventional network are based on modern ''Operating Systems" (OSs).

Little OS is issued in the market relating to IoT invasion. IoT operating systems (e.g. Contiki-OS and RIOT-OS) represent the most prevalent versions that exist within the market. However, they are in need of obtaining semantic means and hardware interoperability. Accordingly, further performance is conducted in order to improve current variations of universal IoT-OS. Actuator layer can represent a different valuable part related to IoT. To the best knowledge, such a part does not exist within the literature. Based on the sensor, actuators are being raised in terms of exponential rate. Demanding a central controlling and monitoring environment is important where IoT occupies the gap. Some future research directions pertaining to crowd sensing of IoT comprise:

a) Social Internet of Things: Real humans can comprehend and answer more effectively in comparison to a machine where these humans represent the most "intelligent machines" [50]. A massive number of users involved in a social network delivers more effective answers to complex issues compared to one user or a knowledgeable user [51]. The smart cooperative developing social networks assist users to seek information (e.g. answers to encountered issues) that attracts several interests. Social networks can benefit from effectively exploring and disseminating services where social networks are used by several systems (e.g. Facebook and Yahoo! Answers) for disseminating the information, such as knowledge among users [52]. There exist an increased possibility and view for incorporating social networking through the Internet of Things that is considered a significant future research direction [43].
b) Privacy protection: is defined as the main problem, which is still yet to be introduced, particularly, within the crowd sensing region. There exist extensive research to be carried out, which concentrates on privacy protection [53]. The CAROMM framework applies the data content from user's smartphone, bears increased risks in order to seepage the privacy information that is related to users as the information, such as time and location are needed to be preserved. The privacy risk should be minimized to a suitable level prior to conducting any crowd sensing action. Otherwise, the privacy of a user can be revealed to the public. The authors in [53] carry out a study on automatic data anonymization by covering specific information from raw data that is sensed via a local smartphone.
c) Optimization of several factors, such as energy budget, prediction, and localization, the trade-off between increased location accuracy and reduced energy consumption pertaining to mobile crowd sensing tools is considered essential when efficiently applying many different related algorithms [54], [55]. In the produced solution by Lane et al. [10], in order to reduce the energy overhead according to the content information (e.g. position), its real-world action struggles from the imprecise localization method. Additionally, more than a single sensor for mobile crowd sensing (e.g. smartphone-based platform) is applied in order to gather the data and sense the content, such as noise magnitude, localization, and dynamic status [56]. Therefore, the consistency and the quantity of information pertaining to a context might raise through a particular progress [39] in which the CAROM method can obtain many different stream data coming out from multiple cellular devices and manages them according to an enclosed content (e.g. the time mark and location on photos) [57]. The method enhances the crowd sensing's performance.

5. Conclusion

The Internet proves its availability through our lives by interacting through a virtual level along towards social relationships. IoT provides a current possibility through to the internet based on allowing communications among items and human, producing a more intelligent and smarter planet. This causes the perspective that expresses ''anytime, anywhere, anyway, anything" communications basically in a factual sense. It is realized that IoT must be represented as the major part pertaining to the available internet according to its future research direction that is clearly and especially dissimilar to the new stage of the internet that is being viewed and applied. Accordingly, the architectural aspect is taken into account. Architecture is defined as a technological approach that allows things to communicate and interrelate with alike or different items by putting in place a human to represent a layer over it. It is obvious that the present IoT paradigm is effective for M2M communications and is currently obtaining a restricted number of factors. Current designs are unavoidable for the livelihood of IoT that represents a robust idea for the researcher to proceed with. From the above survey, it is found that publish/subscribe based IoT is flourishing nowadays and is successively used in many applications. Consequently, it must be known that people are solemnizing their beliefs according to architectural vertical silos. If this tendency remains until the next near years, it is obligatory that IoT might not perform its objective based on different problems as addressability, scalability, concurrency, interoperability, and flexibility. Crowdsourcing is combined into the architectural succinctness. Defense, military, intelligence services, robotics, and many different domains remain unrecovered by IoT. Context, socially awareness, governance, multimedia, education, and tourism that are based on IoT architectures are not considered practical. Vertical silos should be synchronized with the horizontal perception for effective measures of the IoT. Within this paper, a definition and background of IoT are provided. Secondly, complete analyses related to various research issues are indicated. Additionally, a new aspect "IoT" is produced according to many different external inputs and theoretical nomenclature. Apart from other IoT survey researches, the major contribution pertaining to this paper is based on particular region archi-

tectures related to IoT implementations. This contribution aims at highlighting different related issues and potential research chances for future researchers in IoT who can possibly perform efficiently in architectures including the entire IoT field.

References

[1] Knud Lasse Lueth, "Why the Internet of Things is called Internet of Things : Definition , history , disambiguation Internet of Things definition Why Google ' s Internet of Things definition is inaccurate," *IOT Anal.*, vol. 1, no. 9 Dicember 2014, p. 1, 2015.

[2] Juniper Research, "'INTERNET OF THINGS' CONNECTED DEVICES TO ALMOST TRIPLE TO OVER 38 BILLION UNITS BY 2020," *Press release*, 2015. [Online]. Available: http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[3] R. von der Meulen, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," *Gartner*, 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3165317.

[4] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza, "A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4. pp. 2392–2431, 2017. https://doi.org/10.1109/COMST.2017.2727878.

[5] S. K. Sharma and X. Wang, "Live Data Analytics with Collaborative Edge and Cloud Processing in Wireless IoT Networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017. https://doi.org/10.1109/ACCESS.2017.2682640.

[6] D. H. Chau, A. Kittur, J. I. Hong, and C. Faloutsos, "Apolo : Making Sense of Large Network Data by Combining Rich User Interaction and Machine Learning," in *Proc. ACM CHI*, 2011, pp. 167–176. https://doi.org/10.1145/1978942.1978967.

[7] S. Suthaharan, "Big data classification: Problems and challenges in network intrusion prediction with machine learning," in *Performance Evaluation Review*, 2014, vol. 41, no. 4. https://doi.org/10.1145/2627534.2627557.

[8] M. Usama *et al.*, "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," 2017.

[9] S. Ayoubi *et al.*, "Machine Learning for Cognitive Network Management," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 158–165, 2018. https://doi.org/10.1109/MCOM.2018.1700560.

[10] Z. M. Fadlullah *et al.*, "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017. https://doi.org/10.1109/COMST.2017.2707140.

[11] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, "Machine Learning for Networking: Workflow, Advances and Opportunities," *IEEE Network*, vol. 32, no. 2. pp. 92–99, 2018. https://doi.org/10.1109/MNET.2017.1700200.

[12] J. Dizdarevic, F. Carpio, A. Jukan, and X. Masip-Bruin, "Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration," vol. 1, no. 1, pp. 1–27, 2018. https://doi.org/10.1145/3292674.

[13] N. T. Le, M. A. Hossain, A. Islam, D. Y. Kim, Y. J. Choi, and Y. M. Jang, "Survey of promising technologies for 5g networks," *Mob. Inf. Syst.*, vol. 2016, 2016. https://doi.org/10.1155/2016/2676589.

[14] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for Internet of Things," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 8, pp. 1399–1417, 2018. https://doi.org/10.1007/s13042-018-0834-5.

[15] A. Bansal, M. K. Ahirwar, and P. K. Shukla, "A Survey on Classification Algorithms Used in Healthcare Environment of the Internet of Things," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 7, pp. 883–887, 2018. https://doi.org/10.26438/ijcse/v6i7.883887.

[16] F. Liang *et al.*, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access*, vol. 6, no. c, pp. 6900–6919, 2017. https://doi.org/10.1109/ACCESS.2017.2778504.

[17] M. A., A. Mohammed, and M. Yamani, "A Brief Survey on 5G Wireless Mobile Network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, pp. 52–59, 2017. https://doi.org/10.14569/IJACSA.2017.081107.

[18] S. Lee, M. Bae, and H. Kim, "Future of IoT Networks: A Survey," *Appl. Sci.*, vol. 7, no. 10, p. 1072, 2017. https://doi.org/10.3390/app7101072.

[19] F. Jalali, S. Khodadustan, C. Gray, K. Hinton, and F. Suits, "Greening IoT with Fog: A Survey," *Proc. - 2017 IEEE 1st Int. Conf. Edge Comput. EDGE 2017*, pp. 25–31, 2017. https://doi.org/10.1109/IEEE.EDGE.2017.13.

[20] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *Journal of Industrial Information Integration*, vol. 10. pp. 1–9, 2018. https://doi.org/10.1016/j.jii.2018.01.005.

[21] B. N. Karthik, L. Durga Parameswari, R. Harshini, and A. Akshaya, "Survey on IOT & Arduino Based Patient Health Monitoring System," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2018 IJSRCSEIT*, vol. 1, no. 3, pp. 1414–1417, 2018.

[22] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3. King Saud University, pp. 291–319, 2018. https://doi.org/10.1016/j.jksuci.2016.10.003.

[23] L. Da Xu, "Enterprise Systems: State-of-the-Art and Future Trends," *IEEE Trans. Ind. INFORMATICS*, vol. 7, no. 4, 2011. https://doi.org/10.1109/TII.2011.2167156.

[24] Li, Xu, and Zhao, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, pp. 2787–2805, 2014. https://doi.org/10.1016/j.comnet.2010.05.010.

[25] G. Atzori, L., Iera, A., Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805., 2010. https://doi.org/10.1016/j.comnet.2010.05.010.

[26] S. H. Alsamhi, O. Ma, M. S. Ansari, and Q. Meng, "Greening Internet of Things for Smart Everythings with A Green-Environment Life: A Survey and Future Prospects," pp. 1–14, 2018.

[27] M. Drives and D. Transformation, "The Future is 5G."

[28] J. S. Kumar, "Green Smart World (Internet of things)," *Int. J. Eng. Sci. Invent.*, pp. 32–35, 2018.

[29] C. Zhu, V. C. M. Leung, L. Shu, and E. C. H. Ngai, "Green Internet of Things for Smart World," *IEEE Access*, vol. 3, pp. 2151–2162, 2015. https://doi.org/10.1109/ACCESS.2015.2497312.

[30] M. Maksimovic, "The Role of Green Internet of Things (G-IoT) and Big Data in Making Cities Smarter, Safer and More Sustainable," *Int. J. Comput. Digit. Syst.*, vol. 6, no. 4, pp. 175–184, 2017. https://doi.org/10.12785/IJCDS/060403.

[31] H. Wang, "Toward a Green Campus with the Internet of Things–the Application of Lab Management," *World Congr. Eng. 2013*, vol. III, no. 5, pp. 195–200, 2013.

[32] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, no. c, pp. 3619–3647, 2017. https://doi.org/10.1109/ACCESS.2017.2779844.

[33] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Comput. Networks*, vol. 141, pp. 199–221, 2018. https://doi.org/10.1016/j.comnet.2018.03.012.

[34] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of Environmental Internet of Things on water quality management of urban scenic river," *Int. J. Sustain. Dev. World Ecol.*, vol. 20, no. 3, pp. 216–222, 2013. https://doi.org/10.1080/13504509.2013.785040.

[35] P. V. C. M. Leung, "Green Internet of Things for Smart Cities," 2015.

[36] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, 2018. https://doi.org/10.1109/JIOT.2017.2750180.

[37] H. Sundmaeker, P. Guillemin, P. Friess, and Sylvie Woelfflé, *Vision and Challenges for Realising the Internet of Things*, vol. 1, no. March. 2010.

[38] O. Vermesan, P. Friess, P. Guillemin., S. Gusmeroli, H. Sundmaeker, and A. Bassi, *Internet of things strategic research roadmap. The Cluster of European Research Projects*. 2011.

[39] N. Human-cyber-physical, J. S. Baras, and C. Papagianni, "IoT and 5G as Enablers for Systems," 2017.

[40] M. A. M. Albreem *et al.*, "Green internet of things (IoT): An overview," in *2017 IEEE International Conference on Smart Instrumentation, Measurement and Applications, ICSIMA 2017*, 2018, vol. 2017-Novem, no. March 2018, pp. 1–6. https://doi.org/10.1109/ICSIMA.2017.8312021.

[41] B. Guo *et al.*, "Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 7:1-7:30, 2015. https://doi.org/10.1145/2794400.
[42] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018. https://doi.org/10.1016/j.jisa.2017.11.002.
[43] J. Liu, H. Shen, and X. Zhang, "A survey of mobile crowdsensing techniques: A critical component for the internet of things," in *2016 25th International Conference on Computer Communications and Networks, ICCCN 2016*, 2016. https://doi.org/10.1109/ICCCN.2016.7568484.
[44] G. Kaur, P. Tomar, and P. Singh, "Internet of Things and Big Data Analytics Toward Next-Generation Intelligence," *Springer Int. Publ. AG 2018*, vol. 30, pp. 315–333, 2018. https://doi.org/10.1007/978-3-319-60435-0_13.
[45] C. Perera, P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Dynamic configuration of sensors using mobile sensor hub in internet of things paradigm," in *Proceedings of the 2013 IEEE 8th International Conference on Intelligent Sensors, Sensor Networks and Information Processing: Sensing the Future, ISSNIP 2013*, 2013, vol. 1, pp. 473–478. https://doi.org/10.1109/ISSNIP.2013.6529836.
[46] S. Chen, R. K. Coleman, P. Flittner, and K. Cornett, "IEEE Std 1451.5-2007, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators -- Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats," 2007.
[47] C. Cornelius, A. Kapadia, and D. Kotz, "Anonysense: privacy-aware people-centric sensing," *MobiSys*, pp. 211–224, 2008. https://doi.org/10.1145/1378600.1378624.
[48] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture," 2009.
[49] OGC, "The Open Geospatial Consortium," 2010.
[50] H. Shen, Z. Li, J. Liu, and J. E. Grant, "Knowledge sharing in the online social network of Yahoo! Answers and its implications," *IEEE Trans. Comput.*, vol. 64, no. 6, pp. 1715–1728, 2015.
[51] A. Luigi, I. Antonio, M. Giacomo, and N. Michele, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Networks*, vol. 56, no. 16, pp. 3594–3608, 2012. https://doi.org/10.1016/j.comnet.2012.07.010.
[52] M. B. Mowafaq Salem Alzboon, Saleh Ali Alomari, Mohammad Subhi Al-batah, "The Characteristics of The Green Internet of Things and Big Data in Building Safer, Smarter, and Sustainable Cities.," *Int. J. Eng. Technol.*, vol. 6, no. 3, pp. 83–93, 2017.
[53] N. D. Lane *et al.*, "Piggyback CrowdSensing (PCS) : Energy Efficient Crowdsourcing of Mobile Sensor Data by Exploiting Smartphone App Opportunities," in *CHI EA '18 Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 2013, pp. 1–14.
[54] S. Hasan and E. Curry, "Approximate Semantic Matching of Events for the Internet of Things," *ACM Trans. Internet Technol.*, vol. 14, no. 1, pp. 1–23, 2014. https://doi.org/10.1145/2633684.
[55] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Opportunistic spatio-temporal event processing for mobile situation awareness," 2013, p. 195. https://doi.org/10.1145/2488222.2488266.
[56] J. Howe, "The Rise of Crowdsourcing," *Wired Magazine*, pp. 1–4, 2006.
[57] W. Sherchan, P. P. Jayaraman, S. Krishnaswamy, A. Zaslavsky, S. Loke, and A. Sinha, "Using on-the-move mining for mobile crowdsensing," in *Proceedings - 2012 IEEE 13th International Conference on Mobile Data Management, MDM 2012*, 2012, pp. 115–124. https://doi.org/10.1109/MDM.2012.58.