Internet of Things and Its Applications: a Comprehensive Survey

Roaa Alrekabi, Hazem Alades, Taha Almafraji and
Namer Alzubaedi

December 17, 2021

Internet of Things and Its Applications:
A Comprehensive Survey

CONTENTS

Abstract:

With the evolution of the fifth-generation (5G) wireless network, the Internet of Things (IoT) has become a revolutionary technique that enables a diverse number of features and applications. It can able a diverse amount of devices to be connected in order to create a single communication architecture. As it has significantly expanded in recent years, it is fundamental to study this trending technology in detail and take a close look at its applications in the different domains. It represents an enabler of new communication possibilities between people and things. The main asset of this concept is its significant influence through the creation of a new world dimension. The key features required for employing a large-scale IoT are low-cost sensors, high-speed and error-tolerant data communications, smart computations, and numerous applications. This research work is presented in four main sections, including a general overview of IoT technology, a summary of previous correlated surveys, a review regarding the main IoT applications, and a section on the challenges of IoT. The purpose of this study is to fully cover the applications of IoT, including healthcare, environmental, commercial, industrial, smart cities, and infrastructural applications. This work explains the concept of IoT and defines and summarizes its main technologies and uses, offering a next-generation protocol as a solution to the challenges. IoT challenges were investigated to enhance research and development in the fields. The contribution and weaknesses of each research work cited are covered, highlighting eventual possible research questions and open matters for IoT applications to ensure a full analysis coverage of the discussed papers.

Keywords: IoT applications; IoT protocols; healthcare; environmental; smart cities; commercial; industria

Introduction

With an extensive growth in demand for a higher throughput, larger capacity, and lower latency for users, the 5G network is greatly expected to fulfill the desired requirements [1]. The throughput is expected to be very high, the energy consumption will be significantly lower, and the end-to-end will be reduced to less than 1 ms, which all comply with the International Mobile Telecommunications (IMT) standard for the beyond 5G wireless networks [2]. To achieve this milestone, research and industrial communities have both suggested that future wireless systems will take advantage of the numerous emerging technologies, such as the Millimeter-Wave (mm-wave) frequency band [3,4]; Cognitive Radio (CR) [5]; Massive-Multiple Input Multiple Output (M-MIMO) [6]; Cooperative Networks (CR) using Relay Nodes (RNs) [7]; Coordinated Multipoint Operation (CoMP) [8]; Wireless Sensor Networks (WSN) [9]; Mobile Ad Hoc Networks (MANETs) [10,11]; Device-to-Device (D2D) communication [12,13]; Internet of Things (IoT) [14,15]; Ethernet Passive Optical Networks (EPON) [16]; Heterogeneous Networks (HetNet) [17]; and cellular cloud computing, including big data [18]. Moreover, the use of various power optimizations [19], handover processes [20], interference cancellation [21], data security management [22], routing protocols [23], and scheduling algorithms [24] with optimal enhancement can also deliver ultimate results. New approaches, such as satellite communication in the mmWave spectrum [25], Artificial Intelligence [26], machine learning-based communication [27,28], block chain [29], and human-centric communication [30], are promising ideas for designing efficient base stations in future networks [31,32]. The next-generation networks will provide ubiquitous internet and cellular services to cater to the more than fifty billion devices forecasted to be internet-enabled, including the human-type and machine-type communication systems [33]. Indeed, being able to provide wireless services to such an unprecedented number of smart nodes will be the aim of the next generations of wireless networks [34]. The term IoT has been considered as an expanding technique applied in various applications and functions, from smart environments and houses to personal healthcare and others [35].

It is described as a smart concept for the internet relating everything to the Internet and data organization and information exchange [36]. Large-scale IoT intelligent systems have become more efficient and effective by using the properties of “symmetry” and “asymmetry”. This can help in a range of IoT applications, for example, in water quality analytics, bee colony status monitoring, accurate agriculture, data communication balancing, smart traffic management, spatiotemporal predicting, and intelligent engineering. Several studies are currently working on IoT technologies to sustain their necessity in platforms developing technology [37]. Although there are diverse definitions and explanations for understanding IoT, it has a subsequent edge associated with the assimilation of the physical world with the virtual one of the internet [38]. The paradigm of IoT is simplified as any-time, any-place, and any-one connected [39]. The implementation of this technology makes things and people closer and everyday life easier [40]. The purpose of IoT is to ensure a connection between devices, where each provides information and data. These devices are generally personal objects that are frequently carried, including smartphones, vehicles, healthcare devices, and office connected devices [41]. Moreover, Radio-Frequency Identification (RFID) is considered to be one of the first applications that saw the light and has played a crucial role in numerous technologies, such as sensors, smart objects, and actuators [42]. However, Machine-to-Machine communication (M2M) [43] and Vehicle-to-Vehicle communication (V2V) [44] represent the actual applications showing the significant advantages of IoT [45,46].

2. Methodology

The main objective of this paper is to systematically categorize and investigate the definitive research procedures regarding IoT application methods and approaches. It explores the expansion and growth of IoT, along with its deployment in various application fields. The main areas covered in this study include healthcare, environmental, smart city, commercial, industrial, and infrastructural aspects of IoT applications. The next section shows that extensive research has been conducted to ensure full comprehension of IoT technology, including an overview, its architecture, and protocols. It presents various related literature studies that have been conducted on several aspects of IoT, such as its architecture, protocols, and specific applications. However, to the best of the author’s knowledge, no such work has been conducted where all of these aspects are collectively discussed while focusing on various IoT applications, i.e., healthcare, environmental, smart city, commercial, industrial, and infrastructural applications. Moreover, the IoT architecture layers represented are the main focus of this paper, which include the network, perception, interface, and service layers. It investigates the robust standardization issue, security, software and hardware elements, cost decrease, scalability problems, and proper compatibility. The strength of this review consists of providing a complete overview of the issues and challenges faced in IoT; however, the approaches related to artificial intelligence and the compatibility of the approaches are not covered. Figure 1 represents the topics that are discussed in this study

Figure 1. Review methodology.

3. Background

The principal advantage of IoT consists of its ability to enable communication between an infinite amount of machines incorporated into a large-scale wireless network [47]. These automated devices and sensors together produce and transmit information in real-time, which is useless in the case of incorrect or insufficient filtering and data processing. Moreover, data storage and transmission are the most important and challenging matters in a dynamic IoT network. This section discusses the structure and protocols that have been used in the IoT network [48]. A hybrid IoT architecture consists of the things involved, followed by the insight data processes which end with the action that needs to be done (as shown in Figure 2) [49,50]. The benefit of it is that it can comprise several subsystem architectures [51]. Listed below are the functions of each component in a conventional IoT architecture, as shown in Figure 2: • IoT Edge Devices form the smart IoT actuator since they are able to conduct some processing themselves; • IoT Sensors are connected to the cloud, where they can transmit and receive the data; • Device Provision helps to connect a large number of devices to be registered; • IoT Gateway/Framework proves a cloud hub to the IoT devices and provides command, management, and control of the devices; • Stream Processing analyzes complex execution using time windowing ductions, stream aggregation, and external source combing; • Machine Learning allows the algorithms to be predicted and executed using extreme data. It also analyzes and enables predictive maintenance, according to different scenarios; • Reporting Tools help to hold and store the data, while providing the necessary tools for batch processing; • User Management can restrict and permit which users or groups are authorized to perform an action on the device. The process is done by using the capacities of the application of each user. Generally, IoT systems are designed with two management architectures, including time-based and event-driven architectures. The event-driven architecture consists of sensors transmitting data when activity is sensed, the same as when an alarm is activated once a gate is opened [52]. However, for the time-based architecture, the components of the system transmit data continuously at a specified interval of time [53]. Additionally, it works recurrently after a break to be separately adjusted for each device or setup in a central management system sending queries to endpoint devices and sensors [54].

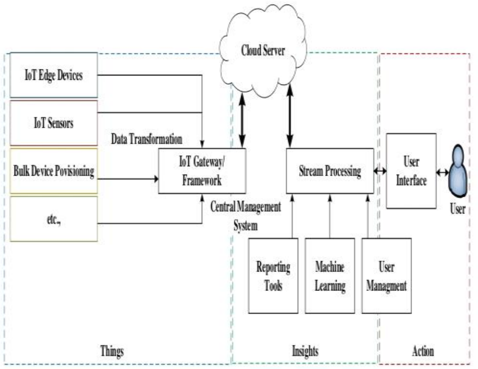

Figure 2. Internet of Things (IoT) architecture.

Various protocols have been used to enable data transmission for the IoT network [55]. It consists of a syntactic and semantic set of regulations determining the operating activity block of the computer network during data transmission [56]. The role of the utilized protocol is to determine the behavior of an entity during data transmission [57]. The traditional Internet Protocols (IPs) are unfortunately not appropriate for ensuring proper data exchange. It is very challenging to design an IoT network, as it comprises several sensors that cannot be added to the general address schema, affecting the possibility of obtaining a fully-fledged node. Besides, these nodes are strongly dependent on a constant energy source, the channel throughput capacity, and the storage parameters, requiring advanced management of the resources. Concerning Wireless Sensor Networks (WSNs), it is necessary to add a data sink to the network [58]. The process consists of first storing the data collected in the sink, before reaching to the other nodes and repeating the process [59]. The proper selection of a strategy for transferring data has a significant impact, as the sensor and sink disposition may enhance the IoT network bandwidth. It ensures security and privacy through the prevention of sending and receiving the same data from multiple sensors, which reduces the energy costs [60–62]. Moreover, several messaging protocols are being developed to support the use of IoT and make it easy to employ. These messages are essential for ensuring a connection between devices. The Constrained Application Protocol (CoAP) and Message Queue Telemetry Transport (MQTT) are the most used messaging protocols; however, some other famous protocols, including the

Extensible Messaging and Presence Protocol (XMPP) and Advanced Message Queuing Protocol (AMQP), result in an efficient overall network performance [63]. The application of these four protocols is as follows and is simplified in Table 1 below: CoAP: This is used in an IoT communication load susceptible to performance deprivation that occurs from traffic congestion. It is a web transfer protocol mainly developed for limited devices with a restricted processing memory and power, usually operating in low bit rate environments [64]. This Hypertext Transfer Protocol (HTTP) is similar to a web transfer protocol that is capable of extending the Representational State Transfer (RST) architecture to Low-Power Wireless Personal Area Networks (LoWPANs) [65]. Furthermore, the Low-Power Wide-Area Network (LoRaWAN) protocol provides the Medium Access Control (MAC) mechanism, which helps to enable communication between various devices and network gateways [66]. This protocol is based on a star topology and has several advantages in IoT applications, such as its low cost, low power, secure nature, and ease of deployment [67]. It follows the RST architecture and comprises a 4-byte header-only, including the User Datagram Protocol (UDP), as a default fundamental transport protocol. Moreover, it provides reliability through the retransmission timeout mechanism [68]. As CoAP works on top of UDP, it presumes possible end-to-end trustworthiness and primary control of congestion. This protocol operates in the application layer and is in charge of formatting the data formatting handshaking connection [69]. To communicate data, COAP provied , four type of messages including confirmable message , the known comfortable message the Acknowledgement message, and the Reset message. All in all, CoAP operates following a request/response approach [70]; • MQTT: This is used for lightweight M2M communications. It acts as an asynchronous protocol that follows the publish/subscribe protocol. The main goal of this protocol is to connect implanted devices and networks to middleware and applications. The advantages of MQTT are its ability to ensure routing in small cases, the fact that it is economical, its low memory, and its low power devices for susceptible and low bandwidth networks [71]. This protocol is extremely lightweight, which makes it suitable for M2M, WSN, and IoT [72]. It allows the transfer of telemetry-style data from devices to the server as messages, along with high latency or constrained networks [73]; • XMPP: This is mostly used for message exchange. It follows the publish/subscribe approach, which is more appropriate for IoT, contrary to the architecture of the CoAP request/response. Moreover, it represents an early protocol endorsed across the internet, regardless of relatively newer protocols, i.e., MQTT [74]. It is based on the Instant Messaging/Presence Protocol (IETF standards) that is used for multi-party chatting, voice and video calling, and telepresence [75]. The main benefits of XMPP consist of it being a secure protocol and the fact that it permits the addition of new applications on top of the core protocols [76]; • AMQP: This was developed for the financial industry. It is characterized by its capability in orientating messages, queuing, switching, security, reliability, and privacy [77]. Similar to XMPP, the AMQP protocol follows the same architecture of the publish/subscribe approach. The principal benefit of using AMQP consists of the store-and-forward element that guarantees reliability and trustworthiness, although it can involve possible network disruptions [78]. This protocol maintains reliable communication through message delivery and ensures delivery primitives involving at-most-once, at-least-once, and exactly once. It needs a trustworthy transport protocol that explains its use of the Transmission Control Protocol (TCP) for message exchange [79].,

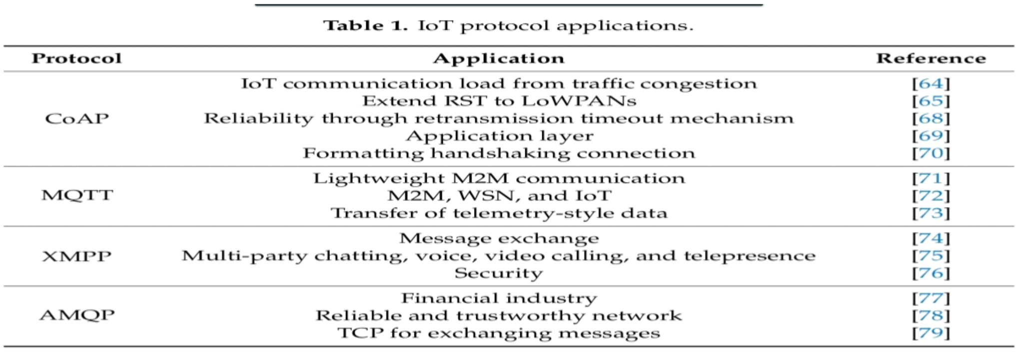

Table 1. IoT protocol applications.

Protocol	Application	Reference
CoAP	IoT communication load from traffic congestion	[64]
	Extend RST to LoWPANs	[65]
	Reliability through retransmission timeout mechanism	[68]
	Application layer	[69]
	Formatting handshaking connection	[70]
MQTT	Lightweight M2M communication	[71]
	M2M, WSN, and IoT	[72]
	Transfer of telemetry-style data	[73]
XMPP	Message exchange	[74]
	Multi-party chatting, voice, video calling, and telepresence	[75]
	Security	[76]
AMQP	Financial industry	[77]
	Reliable and trustworthy network	[78]
	TCP for exchanging messages	[79]

4. Related Work

Several studies and reviews have been conducted regarding IoT applications. This section gives a global and general overview of the main topics discussed in related studies regarding IoT applications. Asghari et al. [80] conducted a systematic review regarding IoT applications and focused on analytically and statistically categorizing the latest studies on IoT. This study is unique in that it uses the Systematic Literature Review (SLR) method as a selection and comparison review technique. In another review presented in [81], the current IoT services were investigated and the article focused on explaining how quality of service (QoS) needs and essentials might be satisfied to guarantee a smart ecosystem. The study presented a detailed analysis regarding the various applications and the threat that the shortage of cross-domain integration may pose. The research summarized the interoperability and explained QoS necessities, including the reliability, security, privacy, scalability, and availability. However, the study lacks statistics concerning the reported results. Another study presented in [82], focusing on IoT, discusses work related to the environment and agriculture. This study mainly focuses on four domains, including logistics, control, monitoring, and prediction. Two main points are discussed, starting with the significant technological attempts used in IoT applications to address environmental and agro-industrial problems. This work discusses the storage approach, communication technique, visualization approach, power sources, edge computing technology, sensing variables, and actuators. Another review presented by Han et al. [83] discusses the Internet protocol employed for smart objects, target applications, service modeling, service composition structures, and target platforms. The factors include the scalability, response period, accessibility, and expenditure. The main IoT techniques have been investigated in [84].

5. IoT Applications

This section of the paper mainly focuses on reporting IoT applications discussed in recent studies. Figure 3 represents a complete taxonomy of IoT in the significant fields of application. The principal areas of application are focused on health care, the environment, smart cities, commercial, industrial, and infrastructural fields [85,86].

The applications and use of IoT in the different domains are what drive and explain the development of this new trend, leading to the acceptance of IoT by the new world [87]. The study of IoT applications improves the understanding and enhancement of IoT technology, and thus, the design of new systems for newly developed cases [88]. The concept of IoT can be summarized as generating daily information from an object and transferring it to another one. Therefore, enabling communication between objects makes the range of IoT applications extensive, variable, and unlimited [89,90]

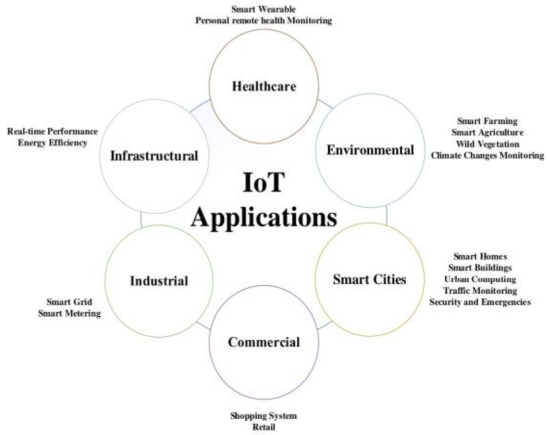

Figure 3. Taxonomy of IoT applications.

6. IoT and Next Generation Protocol

The IPv6 suite primary protocol is neighbor discovery protocol (NDP), and is considered a replacement for the address resolution protocol (ARP) function in IPv4 [165]. The IPv6 protocol considers an extremely auspicious protocol for complicated and dispersed network applications in the era of IoT and Industry 4.0. However, its industrial implementation is slowly increasing in smart manufacturing methods [166]. As the number of devices in the network grows, the received data becomes complex and complicated, which requires more efficient approaches to be collected, sorted, and processed to achieve higher QoS values [167]. This has led researchers and developers to focus on designing various smart network protocols with self-organizing, self-management, and self-configure features, which can able full 3GPP standards and establish an uninterrupted network [168]. Moreover, the IoT6, which is the research project of the future IoT, is progressing positively, yet the unification of IPv6 and IoT is struggling with some challenges. The aim is to exploit the potential of IPv6 and related standards to overcome current shortcomings and fragmentation of the IoT [169]. Currently, the prime issue is the need to integrate the IPv6 and corresponding protocol with IoT, which can help to offer various applications such as automation, smart homes, and smart cities. However, due to wish to design an efficient protocol, some of the significant issues, such as the integration, complexity, scalability, security, reliability, flexibility, and homogeneity, need to be investigated for more IoT applications.

7. Conclusions

The objective of this paper was to explain and describe new trends in IoT applications. This paper presents a survey of the latest studies conducted regarding IoT applications in the most important fields, including healthcare, the environment, smart cities, commercial, and industrial application domains. This study aimed to survey and review the various and most famous IoT application areas, in order to understand the diverse methodologies. The study has summarized the various challenges, such as data privacy and scalability for the healthcare applications, authorization and cost issues for environmental applications, mobility and architecture challenges for smart city applications, cost and implementation difficulties for commercial applications, hardware and production problems for industrial applications, and standardization and trust issues for infrastructural applications. It has stated that various IoT applications still need to be exploited, such as blockchain technology, in order to maintain transaction information, enhance the existing structure performance, or develop next-generation systems. This can help to achieve extra safety, automatic business management, distributed platforms, offline-to-online information authentication, and so on. Moreover, the security and privacy characteristics of IoT are the key factors that can lead to its ability to be developed into a universally implemented technology in the future. However, the self-organizing and accessible nature of IoT makes it susceptible to numerous insider and outsider attackers. This may compromise the users' security and privacy, enabling access to a user's private data, financial damage, and eavesdropping. Therefore, more advanced optimized algorithms and protocols are required to secure data privacy. It can be concluded that by designing an energy- and cost-efficient intelligent network with potential business growth for IoT systems, the next generation of development technology can be produced. Author Contributions: Conceptualization, F.Q. and R.H.; visualization, F.Q. and M.K.H.; writing—original draft preparation, R.H. and F.Q.; writing—review and editing, F.Q., M.K.H., A.H.M.A., and A.S.A.; funding acquisition, R.H.; supervision, R.H. and A.H.M.A.;

project administration, F.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is supported under the Dana Impak Perdana UKM DIP-2018-040 and Fundamental Research Grant Scheme FRGS/1/2018/TK04/UKM/02/07.

Acknowledgments: The authors would like to acknowledge the support provided by the Network and Communication Technology (NCT) Research Groups, FTSM, UKM, in providing facilities throughout this research. The authors would also like to thank the editor and the anonymous reviewers for their valuable comments and suggestions.

References

Internet of Things and Its Applications: A Comprehensive Survey Rosilah Hassan 1 , Faizan Qamar 2,* ,1 Mohammad Kamrul Hasan , 2 Azana Hafizah Mohd Aman and 3 Amjed Sid Ahmed

Received: 27 August 2020; Accepted: 16 September 2020; Published: 14 October 2020

1. Holma, H.; Toskala, A.; Nakamura, T. 5G Technology: 3GPP New Radio; John Wiley & Sons: Hoboken, NJ,

USA, 2020.

2. Faizan, Q. Enhancing QOS Performance of the 5G Network by Characterizing Mm-Wave Channel and

Optimizing Interference Cancellation Scheme/Faizan Qamar. Ph.D. Thesis, University of Malaya, Kuala

Lumpur, Malaysia, 2019.

3. Polese, M.; Giordani, M.; Zugno, T.; Roy, A.; Goyal, S.; Castor, D.; Zorzi, M. Integrated Access and Backhaul

in 5G mmWave Networks: Potential and Challenges. IEEE Commun. Mag. 2020, 58, 62–68. [CrossRef]

4. Qamar, F.; Siddiqui, M.H.S.; Hindia, M.N.; Dimyati, K.; Abd Rahman, T.; Talip, M.S.A. Propagation Channel

Measurement at 38 GHz for 5G mm-wave communication Network. In Proceedings of the 2018 IEEE Student

Conference on Research and Development (SCOReD), Selangor, Malaysia, 26–28 November 2018; pp. 1–6.

5. Hindia, M.N.; Qamar, F.; Ojukwu, H.; Dimyati, K.; Al-Samman, A.M.; Amiri, I.S. On Platform to Enable the

Cognitive Radio Over 5G Networks. In Wireless Personal Communications; Springer: New York, NY, USA,

2020; pp. 1241–1262.

6. Bogale, T.E.; Le, L.B. Massive MIMO and mmWave for 5G wireless HetNet: Potential benefits and challenges.

IEEE Veh. Technol. Mag. 2016, 11, 64–75. [CrossRef]

7. Mohamed, E.M.; Elhalawany, B.M.; Khallaf, H.S.; Zareei, M.; Zeb, A.; Abdelghany, M.A. Relay Probing for

Millimeter Wave Multi-Hop D2D Networks. IEEE Access 2020, 8, 30560–30574. [CrossRef]

8. Hindia, M.N.; Qamar, F.; Abbas, T.; Dimyati, K.; Abu Talip, M.S.; Amiri, I.S. Interference cancelation

for high-density fifth-generation relaying network using stochastic geometrical approach. Int. J. Distrib.

Sens. Netw. 2019, 15, 1550147719855879. [CrossRef]

9. Dahnil, D.P.; Hassan, R. Wireless Sensor Networks: A framework for community and educational gardens.

Adv. Sci. Lett. 2018, 24, 1153–1157. [CrossRef]

10. Tilwari, V.; Hindia, M.N.; Dimyati, K.; Qamar, F.; Talip, A.; Sofian, M. Contention Window and Residual

Battery Aware Multipath Routing Schemes in Mobile Ad-hoc Networks. Int. J. Technol. 2019, 10, 1376–1384.

[CrossRef]

11. Amiri, I.; Dong, D.S.; Pokhrel, Y.M.; Gachhadar, A.; Maharjan, R.K.; Qamar, F. Resource Tuned Optimal

Random Network Coding for Single Hop Multicast future 5G Networks. Int. J. Electron. Telecommun. 2019,

65, 463–469.

12. Li, J.; Lei, G.; Manogaran, G.; Mastorakis, G.; Mavromoustakis, C.X. D2D communication mode selection and

resource optimization algorithm with optimal throughput in 5G network. IEEE Access 2019, 7, 25263–25273.

[CrossRef]

13. Qamar, F.; Dimyati, K.; Hindia, M.N.; Noordin, K.A.; Amiri, I.S. A stochastically geometrical poisson

point process approach for the future 5G D2D enabled cooperative cellular network. IEEE Access 2019, 7,

60465–60485. [CrossRef]

14. Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An Overview of Internet of Things (IoT) and

Data Analytics in Agriculture: Benefits and Challenges. IEEE Internet Things J. 2018, 5, 3758–3773. [CrossRef]

15. Aman, A.H.M.; Yadegaridehkordi, E.; Attarbashi, Z.S.; Hassan, R.; Park, Y.J. A Survey on Trend and

Classification of Internet of Things Reviews. IEEE Access 2020, 8, 111763–111782. [CrossRef]

16. Udeshi, D.; Qamar, F. Quality Analysis Of Epon Network For Uplink and Downlink Design. Asian J. Eng.

Sci. Technol. 2014, 4, 78–83.

17. Gachhadar, A.; Qamar, F.; Dong, D.S.; Majed, M.B.; Hanafi, E.; Amiri, I.S. Traffic Offloading in 5G

Heterogeneous Networks using Rank based Network Selection. J. Eng. Sci. Technol. Rev. 2019, 12, 9–16. [CrossRef]

18. Hashem, I.A.T.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Khan, S.U. The rise of “big data” on cloud computing: Review and open research issues. Inf. Syst. 2015, 47, 98–115. [CrossRef]

19. Gachhadar, A.; Hindia, M.N.; Qamar, F.; Siddiqui, M.H.S.; Noordin, K.A.; Amiri, I.S. Modified genetic algorithm based power allocation scheme for amplify-and-forward cooperative relay network. Comput. Electr. Eng. 2018, 69, 628–641. [CrossRef]

20. Hassan, R.; Aman, A.H.M.; Latiff, L.A. Framework for Handover process using Visible Light Communications in 5G. In Proceedings of the 2019 Symposium on Future Telecommunication Technologies (SOFTT), Kuala Lumpur, Malaysia, 18–19 November 2019; pp. 1–4.

21. Le, A.T.; Huang, X.; Guo, Y.J. Beam-Based Analog Self-Interference Cancellation in Full-Duplex MIMO Systems. IEEE Trans. Wirel. Commun. 2020, 19, 2460–2471. [CrossRef]

22. Saizan, Z.; Singh, D. Cyber security awareness among social media users: Case study in German-Malaysian Institute (GMI). Asia Pac. J. Inf. Technol. Multimed. 2018, 7, 111–127. [CrossRef]

23. Muniyandi, R.C.; Qamar, F.; Jasim, A.N. Genetic Optimized Location Aided Routing Protocol for VANET Based on Rectangular Estimation of Position. Appl. Sci. 2020, 10, 5759. [CrossRef]

24. Mamode, M.I.S.; Fowdur, T.P. Survey of Scheduling Schemes in 5G Mobile Communication Systems. J. Electr. Eng. Electron. Control Comput. Sci. 2020, 6, 21–30.

25. Giordani, M.; Zorzi, M. Satellite communication at millimeter waves: A key enabler of the 6G era. In Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 17–20 February 2020; pp. 383–388.

26. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.J.A. The roadmap to 6G: AI empowered wireless networks. IEEE Commun. Mag. 2019, 57, 84–90. [CrossRef]

27. Jameel, F.; Sharma, N.; Khan, M.A.; Khan, I.; Alam, M.M.; Mastorakis, G.; Mavromoustakis, C.X. Machine learning techniques for wireless-powered ambient backscatter communications: Enabling intelligent IoT

networks in 6G era. In Convergence of Artificial Intelligence and the Internet of Things; Springer: Cham,

Switzerland, 2020; pp. 187–211.

28. Kato, N.; Mao, B.; Tang, F.; Kawamoto, Y.; Liu, J. Ten Challenges in Advancing Machine Learning Technologies

toward 6G. IEEE Wirel. Commun. 2020, 27, 96–103. Available online: https://ieeexplore.ieee.org/document/

9061001 (accessed on 1 September 2020). [CrossRef]

29. Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges,

Opportunities and Research Directions. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT),

Levi, Finland, 17–20 March 2020; pp. 1–5.

30. Liu, Y.; Yuan, X.; Xiong, Z.; Kang, J.; Wang, X.; Niyato, D. Federated Learning for 6G Communications:

Challenges, Methods, and Future Directions. arXiv 2020, arXiv:2006.02931.

31. Hindia, M.N.; Qamar, F.; Majed, M.B.; Rahman, T.A.; Amiri, I.S. Enabling remote-control for the power

sub-stations over LTE-A networks. Telecommun. Syst. 2019, 70, 37–53. [CrossRef]

32. Qamar, F.; Siddiqui, M.U.A.; Hindia, M.; Hassan, R.; Nguyen, Q.N. Issues, Challenges, and Research Trends

in Spectrum Management: A Comprehensive Overview and New Vision for Designing 6G Networks.

Electronics 2020, 9, 1416. [CrossRef]

33. Mahmood, N.H.; Alves, H.; López, O.A.; Shehab, M.; Osorio, D.P.M.; Latva-Aho, M. Six key features of

machine type communication in 6G. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT),

Levi, Finland, 17–20 March 2020; pp. 1–5.

34. Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136.

[CrossRef]

35. Mohd Zaki, I.; Rosilah, H. The Implementation of Internet of Things using Test Bed in the UKMnet

Environment. Asia Pac. J. Inf. Technol. Multimed. 2019, 8, 1–17.

Symmetry 2020, 12, 1674 24 of 29

36. Hassan, R.; Nori, S.S.; Othman, N.E. The improvement of the protection for 6LoWPAN in IoT through

non-causal hash function scheme. In Proceedings of the 2018 15th International Conference on

Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON),

Chiang Rai, Thailand, 18–21 July 2018; pp. 600–603.

37. Whitmore, A.; Agarwal, A.; Da Xu, L. The Internet of Things—A survey of topics and trends. Inf. Syst. Front.

2015, 17, 261–274. [CrossRef]

38. Ali, Z.M.; Arshad, M.A.B.M.; Bakar, M.A. POLIoT: Internet Of Things Framework In Managing Network

Threats At Metro Polytechnic Tasek Gelugor. In Proceedings of the 2018 Cyber Resilience Conference (CRC),

Putrajaya, Malaysia, 13–15 November 2018; pp. 1–4.

39. Jain, P.; Adrangi, F.; Venkatachalam, M. Cellular IoT Network Architecture. Google Patents US 10,623,942 B2,

14 April 2020.

40. Korade, S.; Kotak, V.; Durafe, A. A review paper on internet of things (IoT) and its applications. Int. Res. J.

Eng. Technol. 2019, 6, 1623–1630.

41. Wu, F.; Wu, T.; Yuce, M.R. An internet-of-things (IoT) network system for connected safety and health

monitoring applications. Sensors 2019, 19, 21. [CrossRef]

42. Pungus, S.R.; Yahaya, J.; Deraman, A.; Bakar, N.H.B. A data modeling conceptual framework for ubiquitous

computing based on context awareness. Int. J. Electr. Comput. Eng. 2019, 9, 5495–5501. [CrossRef]

43. Alsharif, M.H.; Nordin, R.; Abdullah, N.F.; Kelechi, A.H. How to make key 5G wireless technologies

environmental friendly: A review. Trans. Emerg. Telecommun. Technol. 2018, 29, e3254. [CrossRef]

44. Zhang, H.; Lu, X. Vehicle communication network in intelligent transportation system based on internet of

things. Comput. Commun. 2020, 160, 799–806. [CrossRef]

45. Udoh, I.S.; Kotonya, G. Developing IoT applications: Challenges and frameworks. IET Cyber Phys. Syst.

Theory Appl. 2018, 3, 65–72. [CrossRef]

46. Afzal, B.; Umair, M.; Shah, G.A.; Ahmed, E. Enabling IoT platforms for social IoT applications: Vision,

feature mapping, and challenges. Future Gener. Comput. Syst. 2019, 92, 718–731. [CrossRef]

47. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express 2019, 5, 1–7. [CrossRef]

48. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.

49. Raeespour, A.K.; Patel, A.M. Design and Evaluation of a Virtual Private Network Architecture for Collaborating Specialist Users. Asia Pac. J. Inf. Technol. Multimed. 2016, 5, 13–50. [CrossRef]

50. Stackowiak, R. Azure IoT Solutions Overview. In Azure Internet of Things Revealed; Springer: Berkeley, CA, USA, 2019; pp. 29–54.

51. Mojib, G.; Aman, A.H.M.; Khalaf, M.; Hassan, R. Simulation analysis for QoS in Internet Of Things wireless network. 3C Tecnol. 2019, 2019, 77–83. [CrossRef]

52. Almeida, R.B.; Junes, V.R.C.; da Silva Machado, R.; da Rosa, D.Y.L.; Donato, L.M.; Yamin, A.C.; Pernas, A.M. A distributed event-driven architectural model based on situational awareness applied on Internet of Things. Inf. Softw. Technol. 2019, 111, 144–158. [CrossRef]

53. Hu, B.; Guan, Z.H.; Chen, G.; Shen, X. A distributed hybrid event-time-driven scheme for optimization over sensor networks. IEEE Trans. Ind. Electron. 2018, 66, 7199–7208. [CrossRef]

54. Windley, P.J. API Access Control with OAuth: Coordinating interactions with the Internet of Things. IEEE Consum. Electron. Mag. 2015, 4, 52–58. [CrossRef]

55. Johnson, D.; Ketel, M. IoT: Application Protocols and Security. Int. J. Comput. Netw. Inf. Secur. 2019, 11, 1–8. [CrossRef]

56. Kambourakis, G.; Kolias, C.; Geneiatakis, D.; Karopoulos, G.; Makrakis, G.M.; Kounelis, I. A State-of-the-Art Review on the Security of Mainstream IoT Wireless PAN Protocol Stacks. Symmetry 2020, 12, 579. [CrossRef]

57. Sudarshan, A.; Dirisam, S.; Shetty, J.; NS, G.R.S. Review of Protocols used in Enterprise Networks. Int. J. Eng.

Res. Technol. 2019, 8, 53–56.

58. Deebak, B.D.; Al-Turjman, F. A hybrid secure routing and monitoring mechanism in IoT-based wireless

sensor networks. Ad Hoc Netw. 2020, 97, 102022.

59. Malathy, S.; Porkodi, V.; Sampathkumar, A.; Hindia, M.N.; Dimyati, K.; Tilwari, V.; Qamar, F.; Amiri, I.S.

An optimal network coding based backpressure routing approach for massive IoT network. Wirel. Netw.

2020, 1–18. [CrossRef]

Symmetry 2020, 12, 1674 25 of 29

60. Dohare, A.; Tulika; Mallikarjuna, B. Data Collection in Wireless Sensor Networks Using Prediction Method.

J. Adv. Res. Dyn. Control Syst. 2019, 11, 815–820. [CrossRef]

61. Martin, T.; Geneiatakis, D.; Kounelis, I.; Kerckhof, S.; Fovino, I.N. Towards a Formal IoT Security Model.

Symmetry 2020, 12, 1305. [CrossRef]

62. Popescu, C.R.G.; Popescu, G.N. Risks of cyber attacks on financial audit activity. Audit Financ. J. 2018, 16,

140–147. [CrossRef]

63. Bahashwan, A.A.O.; Manickam, S. A brief review of messaging protocol standards for internet of things

(IoT). J. Cyber Secur. Mobil. 2019, 8, 1–14. [CrossRef]

64. Hassan, R.; Jubair, A.M.; Azmi, K.; Bakar, A. Adaptive congestion control mechanism in CoAP application

protocol for internet of things (IoT). In Proceedings of the 2016 International Conference on Signal Processing

and Communication (ICSC), Noida, India, 26–28 December 2016; pp. 121–125.

65. Tukade, T.M.; Banakar, R. Data transfer protocols in IoT—An overview. Int. J. Pure Appl. Math. 2018, 118,

121–138.

66. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A survey of LoRaWAN for IoT: From technology to

application. Sensors 2018, 18, 3995. [CrossRef] [PubMed]

67. Khutsoane, O.; Isong, B.; Abu-Mahfouz, A.M. IoT devices and applications based on LoRa/LoRaWAN.

In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017; pp. 6107–6112.

68. Järvinen, I.; Daniel, L.; Kojo, M. Experimental evaluation of alternative congestion control algorithms for Constrained Application Protocol (CoAP). In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 453–458.

69. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X. CoAP—Application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In Digital Twin Technologies and Smart Cities; Springer: Cham, Switzerland, 2020; pp. 151–175.

70. Akpakwu, G.A.; Hancke, G.P.; Abu-Mahfouz, A.M. CACC: Context-aware congestion control approach for lightweight CoAP/UDP-based Internet of Things traffic. Trans. Emerg. Telecommun. Technol. 2020, 31, e3822. [CrossRef]

71. Soni, D.; Makwana, A. A survey on mqtt: A protocol of internet of things (iot). In Proceedings of the International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017), Chennai, India, 4–8 April 2017.

72. Luzuriaga, J.E.; Cano, J.C.; Calafate, C.; Manzoni, P.; Perez, M.; Boronat, P. Handling mobility in IoT applications using the MQTT protocol. In Proceedings of the 2015 Internet Technologies and Applications (ITA), Wales, UK, 8–11 September 2015; pp. 245–250.

73. Hwang, H.C.; Park, J.; Shon, J.G. Design and implementation of a reliable message transmission system based on MQTT protocol in IoT. Wirel. Pers. Commun. 2016, 91, 1765–1777. [CrossRef]

74. Chien, H.Y.; Chen, Y.J.; Qiu, G.H.; Liao, J.F.; Hung, R.W.; Lin, P.C.; Kou, X.A.; Chiang, M.L.; Su, C. A MQTT-API-compatible IoT security-enhanced platform. Int. J. Sens. Netw. 2020, 32, 54–68. [CrossRef]

75. Chen, Y.; Kunz, T. Performance evaluation of IoT protocols under a constrained wireless access network.

In Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking

(MoWNeT), Cairo, Egypt, 11–13 April 2016; pp. 1–7.

76. Joe, M.M.; Ramakrishnan, B. Review of vehicular ad hoc network communication models including WVANET

(Web VANET) model and WVANET future research directions. Wirel. Netw. 2016, 22, 2369–2386. [CrossRef]

77. Yassein, M.B.; Shatnawi, M.Q. Application layer protocols for the Internet of Things: A survey. In Proceedings

of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September

2016; pp. 1–4.

78. Karagiannis, V.; Chatzimisios, P.; Vazquez-Gallego, F.; Alonso-Zarate, J. A survey on application layer

protocols for the internet of things. Trans. IoT Cloud Comput. 2015, 3, 11–17.

79. Dizdarevi´c, J.; Carpio, F.; Jukan, A.; Masip-Bruin, X. A survey of communication protocols for internet of

things and related challenges of fog and cloud computing integration. ACM Comput. Surv. 2019, 51, 116.

[CrossRef]

80. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Internet of Things applications: A systematic review. Comput. Netw.

2019, 148, 241–261. [CrossRef]

Symmetry 2020, 12, 1674 26 of 29

81. Bello, O.; Zeadally, S. Toward efficient smartification of the Internet of Things (IoT) services. Future Gener.

Comput. Syst. 2019, 92, 663–673. [CrossRef]

82. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.;

Garreta, L.E. Review of IoT applications in agro-industrial and environmental fields. Comput. Electron. Agric.

2017, 142, 283–297. [CrossRef]

83. Han, S.N.; Khan, I.; Lee, G.M.; Crespi, N.; Glitho, R.H. Service composition for IP smart object using realtime

Web protocols: Concept and research challenges. Comput. Stand. Interfaces 2016, 43, 79–90. [CrossRef]

84. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. Inf. Syst. Front. 2015, 17, 243–259. [CrossRef]

85. Souri, A.; Asghari, P.; Rezaei, R. Software as a service based CRM providers in the cloud computing:

Challenges and technical issues. J. Serv. Sci. Res. 2017, 9, 219–237. [CrossRef]

86. Souri, A.; Rahmani, A.M.; Jafari Navimipour, N. Formal verification approaches in the web service

composition: A comprehensive analysis of the current challenges for future research. Int. J. Commun. Syst.

2018, 31, e3808. [CrossRef]

87. Chettri, L.; Bera, R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems.

IEEE Internet Things J. 2019, 7, 16–32. [CrossRef]

88. Tun, S.Y.Y.; Madanian, S.; Mirza, F. Internet of things (IoT) applications for elderly care: A reflective review.

Aging Clin. Exp. Res. 2020. [CrossRef]

89. Redhu, S.; Maheshwari, M.; Yeotikar, K.; Hegde, R.M. Joint Data Latency and Packet Loss Optimization

for Relay-Node Selection in Time-Varying IoT Networks. In Proceedings of the 24th Annual International

Conference on Mobile Computing and Networking, New Delhi, India, 29 October–2 November 2018;

pp. 711–713.

90. De Almeida, I.B.F.; Mendes, L.L.; Rodrigues, J.J.; da Cruz, M.A. 5G waveforms for IoT applications.

IEEE Commun. Surv. Tutor. 2019, 21, 2554–2567. [CrossRef]166. Feldner, B.; Herber, P. A qualitative evaluation of IPv6 for the Industrial Internet of Things. Procedia Comput. Sci.

2018, 134, 377–384. [CrossRef]

167. Sinche, S.; Raposo, D.; Armando, N.; Rodrigues, A.; Boavida, F.; Pereira, V.; Silva, J.S. A Survey of IoT

Management Protocols and Frameworks. IEEE Commun. Surv. Tutor. 2019, 22, 1168–1190. [CrossRef]

168. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks.

IEEE Commun. Surv. Tutor. 2019, 22, 170–195. [CrossRef]

169. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nilashi, M.; Alizadeh, M. The application of internet of

things in healthcare: A systematic literature review and classification. Univers. Access Inf. Soc. 2019, 18,

837–869. [CrossRef]