A Survey on the Challenges and Opportunities of the Internet of Things (IoT)

Laith Farhan
School of Engineering
Manchester Metropolitan University, UK
& University of Diyala, Iraq
l.al-bayati@mmu.ac.uk

Sinan T. Shukur
Faculty of Medicine and Health Sciences
Macquarie University, Australia
sinantalib@yahoo.co.uk

Ali E. Alissa
School of Computer Science
University of Plymouth, UK
ali.alissa@plymouth.ac.uk

Mohmad Alrweg
School of Engineering
Manchester Metropolitan
University, UK
mohmad.s.alrweg@mmu.ac.uk

Umar Raza
School of Engineering
Manchester Metropolitan
University, UK
u.raza@mmu.ac.uk

Rupak Kharel
School of Engineering
Manchester Metropolitan
University, UK
r.kharel@mmu.ac.uk

***Abstract*—Internet of Things (IoT) is a rapidly growing technology with a wide range of applications in various fields. It has unified a plethora of devices and infrastructure under the same umbrella and is considered by many technologies leaders as the network of the future (NoF). IoT connects heterogeneous devices that provide sensing, control, actuation, and monitoring activities for smarter environments. Smart IoT devices or objects are characterized with a unique identifier to transfer data over the network without human intervention. IoT is expected to further extend the boundaries of the autonomous world with advanced connectivity of physical entities, systems, services. However, there are some serious obstacles and challenges, which must be resolved before the full potential of IoT is realized. The focus of this study is to discuss the key drivers of change, challenges that may slow the adoption of IoT and the potential of the internet of things technology.**

***Index Terms*—Internet of Things (IoT); Wireless Sensor Network (WSN); Future Network; Future Challenges.**

I. Introduction

During the last decade, Internet of Things (IoT) has attracted intensive attention due to a wide range of applications in industrial, biomedical observation, agriculture, smart cities, environmental monitoring and other fields (Fig. 1) [1]. IoT is the internetworking of physical devices used in our daily lives that use standard communications architectures to provide new services to end users [2]. From a conceptual standpoint, the elements of IoT summarized into a simple equation below:

$$IoT = Human + PhysicalObjects(sensors, controllers, devices, storages) + Internet$$

It is envisioned that by 2020 the future Internet will include tens of billions of smart objects/devices [3]. IoT technology provides better services to end users via real-time data processing, communications and visualization. IoT can be extended to almost everything from refrigerator to washing machine, wristwatches to smartphones, home security to alarm system, etc [4]. For example, smart refrigerators can tell us the end of the validity of food using bar-codes or which items to buy during our shopping in the market. On the other hand, imagine that we can control our house from anywhere. By using smart phones or tablets with just simple touch we can set a desired temperature or turn lights on or off before getting home. These are examples of just a few applications out of thousands being currently developed every day in the field of IoT.

The massive growth in the number of devices connected to the internet (up to 100 billion devices) , poses a huge range of challenges. In the future IoT will not be islands of isolated systems, but will be an integration of many islands of connected systems, applications, services and underlying devices. At the moment, each of these devices and services work on their own architectures, data format, and own existing protocol stacks. They are all still at early stages of development. Hence, the communication between these objects is insecure, suffers from interoperability and integration issues. Furthermore, the sources of energy required to power these devices are very precious due to the fact that most of them are powered by battery or by means harvested energy. Therefore, there is a need for comprehensive review of existing unconstrained and constrained devices protocols with the view of developing unified, dynamic, standardized, energy efficient and intelligent protocol stacks with recourse to node identity (both capacity and capability). So far, most of these new challenges and concerns have started to attract the attention of academic researchers and companies. The organization of the paper is as follows: Section 2 presents briefly IoT applications challenges and summarizes the related works. We conclude the paper in section 3.

II. IoT Applications and Research Challenges

Many researchers and early adopters have come up with promising solutions to overcome the problems and challenges in realizing IoT applications. However, IoT opens up new

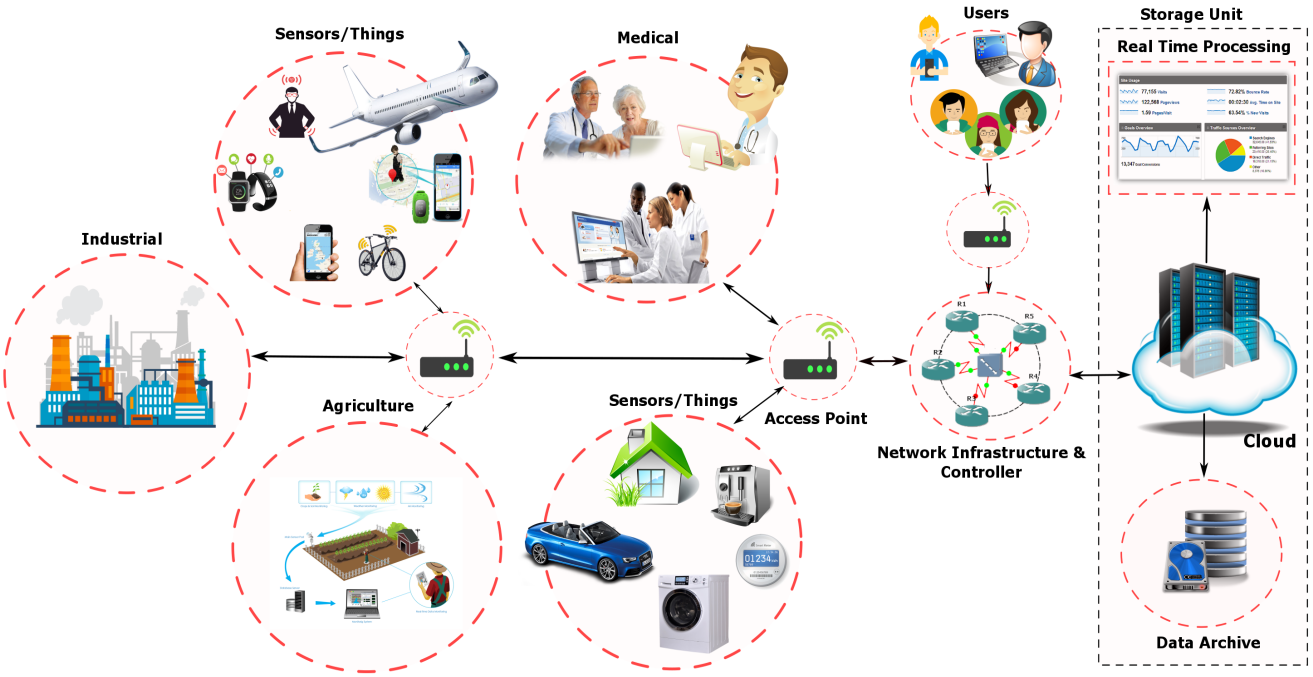

Fig. 1: Internet of things (IoT) architecture.

horizontal challenges that demand latest research and capacities to address them. In this section, we briefly highlight the key challenges for the future IoT systems (see Fig. 2.). Wireless Sensor Networks (WSN) are considered as one of the fundamental underlying technologies for IoT. Therefore, the study has also considered some previous works in the WSN field.

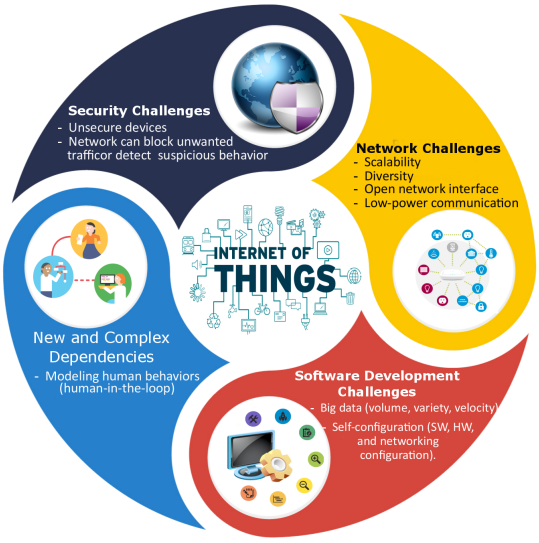

Fig. 2: IoT Challenges and Opportunities.

A. Network Challenges

- **Scalability and Diversity:** IoT combines a plethora of devices/objects and infrastructures under the same umbrella. Thus, each of these objects and systems operate using their architectures, protocol stacks, and data formats. This has created a complex interoperability and integration challenge to realize large-scale heterogeneous IoT ecosystems. The communications between these heterogeneous devices need to be adaptive to allow dynamic interconnectivity and support decentralized nature (plug and play). Trillions of objects will be connected by the internet. The questions that can be asked are, how to protect, authenticate, authorize, and name these devices? Will 6LowPAN and IPv6, CoAP, MQTT, protocols play the roles [5]? The study by [6] [6] enhanced the scale of IoT-cloud by Name Data Networking (NDN) based on publish and subscribe (pub/sub) method. NDN offered three crucial features in terms of the sub/pub scalability: 1) Enabling QoS by distance vector routing. 2) Enabling the efficient message reduction by multicast data delivery. 3) Hierarchical routing for building a scalable overlay topology. M. Amoretti et al. [7] implemented a novel naming scheme and efficient services discovery protocol for WSN called DIstributed NAming Service (DINAS). The proposed scheme is based on three categories: i) Bloom filters, to produce especial name from nodes and services. ii) Advertising name addresses and queries in the network. iii) Caches, to store name addresses between nodes in the network instead of concentrating them at the gateway router. DINAS outperforms the centralized solution. Secure DNS name auto-configuration (SDNSNA) for IoT networks was carried out by K. Lee et al. SDNSNA intended to assign automatic domain names for IPv6 IoT applications into a DNS system. The proposed

system has also supported the security functionality by authentication process solution [8]. The work in [9] [9] implemented smart IoT gateway that allows interoperability and interconnection between heterogeneous objects in IoT networks. The proposed model enabled connectivity of different communications technologies (e.g. Ethernet, Bluetooth, Zigbee, Wi-Fi). It uses a flexible protocol that allows gathering data from different objects in a uniform format. In addition, it presents a lightweight and optimal protocol for IoT devices that equipped with limited resources to forward their information and supports local data storage for analysis purposes.

- **Energy Requirement:** IoT paradigm must deal with energy consumption due to the fact that most of IoT devices are powered by batteries. This means that it is not reasonable to waste the energy by unnecessary data transmissions, protocol overheads, or running the radio all the time (listening and transmitting). IoT technology will soon enable the realization of self-sustainable wireless communication. It is still limited understanding of the properties of various energy sources and their impact on energy harvesting adaptive algorithms. Energy resource can compose wind solar, thermal energy, kinetic energy, hydroelectric harvesting, etc. Therefore, it is important to optimize the energy consumption of a system.
  A centralized traffic aware scheduling algorithm (TASA) has been introduced recently [10]. The proposed scheme allows to set up Time Synchronized Channel Hopping (TSCH) schedule based on traffic load and network topology. It uses the information related to the traffic load e.g. average traffic produced by each node and related to paths coming from the routing protocol e.g. low-power and lossy networks (LLN). TASA respected low duty cycle and latency at the same time. The work in [4] introduced self-organizing and adaptive Dynamic Clustering (DCMDC) solution to maintain mobile data collectors-relay networks. The proposed scheme divided the network into sub-groups based on Service Zones (SZs). Localizing mobility management traffic to a SZ reduces bandwidth, route setup delay, and signaling overhead. Moreover, network clustering helps to achieve load balancing and scalability. S. Sundar et al. [11] target the challenge of implementing an energy efficient and reliable protocol for IoT networks. The idea is that some nodes go to sleep mode after an area is covered by other neighboring nodes. In addition, they suggested two primary and secondary servers. When there were large number of data coming from sensors, the second server automatically starts to operate. In [12], the authors propose a greedy cluster formation algorithm to generate clusters and calculate clusters diameters. It reduces the number of cluster diameters and delay of the network, moreover enhance lifetime of network by deploying multiple sinks in multi-hop. The approach proposed in [13] implements low power CoAP to achieve high energy efficiency. This approach focuses on power management through radio duty cycling as well as removed the complexity from application layer. In another study, M. Al-Jemeli et al. implemented a cross-layer protocol to minimize energy consumption and improve throughput and QoS for mobile WSN (MWSN). The technique employs two major concepts: i) Minimize packets broadcasting to neighbor nodes; ii) Control transmission power that depends on close distance between mobile node and others. Experimental results shows 10% reduction in end-to-end delay and relatively packet delivery ratio [14].

B. Security Challenges

Security and privacy are intrinsic parts of IoT networks. It is very important to ensure privacy protection and security in various activities, such as transportations, personal activities, business processes, and information protection [15] [16]. Access control guarantees that only authorized entities allow to access and modify the information. IoT systems are also desired to be self-healing (detect, diagnose, and countermeasures the attack). Hence, IoT security can be applied at: a) Application Layer. b) Network Layer. c) Physical Layer. There is a wealth of literature on securing IoT systems, but networks are still suffering from threats and are being hacked frequently. Most IoT data is available and stored on the Internet, therefore researchers need to focus on new web based security level techniques and solutions. S. Raza et al. [17] demonstrated an end-to-end (E2E) secure communication in 6LowPAN protocol. The proposed scheme supported both encapsulation security payload and IPsec protocol authentication header. E2E communications are able to check, authentication, encryption of packets and established IPv6 mechanisms. Security Analysis of IoT (IoTSAT) by M. Mohsin et al. [18] models the network-level dependencies, policy-level behavior, device-level interactions, and IoT-specific threats in predicate logic. The proposed work is highly beneficial and scalable for uncovering complex attack vectors of IoT networks. A. Capossele et al. [19] implemented Datagram Transport Layer Security (DTLS) over CoAP protocol for IoT applications. The results were shown minimizing ROM occupancy and computation overhead. Another study by M. Singh et al. [20] suggested secure MQTT for IoT applications. The proposed model enabled security using CP/KPABE for MQTT-SN and MQTT. Also, they implement, and design performance analysis of SMQTT-SN and SMQTT protocols for IoT devices.

C. Fault Tolerance

It is one of the most important issues in the area of WSN and IoT applications. Both technologies involve large number of heterogeneous sensor nodes spread over a large geographic area to perform a specific task. The explosive growth of the connected devices demand higher reliability and performance for modern networks. Some sensor nodes may be blocked or fail due to environment interference, physical damage, or lack of power. The failure of sensor nodes should not affect the overall task of the sensor network. Most of WSN and IoT routing protocols have the ability to recover from the failure

of a sensor node. The sensor node is reported as a failure node when a sensor node cannot receive messages from neighbor nodes for a specific period of time and thus, excluded from the routing path. The problem becomes worse when two or more sensor nodes fail in the same area. The network might cripple because other nodes might not find a route to the ultimate receiver. Therefore, a routing protocol must follow new links dynamically to deliver the data collected by other devices to the intended destination. Also, multi levels of redundancy may be needed in a fault tolerant sensor networks.

Many design goals are related to routing policy such as energy consumption, small delay, high throughput, limited variance of the connection quality. Authors in [21] presented that expected transmission count (ETX) algorithm performs up to two times better than minimal hop-count for long links in terms of throughput. The ETX strategy is to find high throughput paths on multihop wireless communication. It minimizes the expected total number of packet transmission (including retransmissions) required to successfully deliver data to the final destination. Another study [22] implements new routing technique called balanced energy adaptive routing (BEAR) for IoT networks. The proposed method operates in three phases: i) Sensor nodes share the information related to their location and residual energy ii) BEAR protocol elects neighbor nodes and selects the facilitator and successor nodes based on the node locations. iii) Data transmission - The results of BEAR showed improved network lifetime by upto 55%. In [23], authors investigated a novel context-aware routing (CAR) method for IoT applications. The proposed scheme improved the current request response model, during the exchange in peer to peer fashion. The simulation results of CAR showed reduced total wasted time in network delay and improve network service and bandwidth.

D. Software Development Challenges

The ”5V” (volume, velocity, value, variety, and veracity) are important challenges in IoT networks (Fig. 3). Every two years, data is doubling in size and it is expected to reach 44 Zettabytes in the next four years [24]. The ”5V” of data is difficult to be analyzed, processed, stored through traditional technologies. Thus, researchers trend to implement more intelligent algorithms can deal with a vast amount of data that can lead to minimize the problems.

M. Rizwan et al. [25] presents a new framework IoT Big Data Analysis (IBDA) and storage for real-time data generation from IoT devices. The key contribution of IBDA is the ”5V” of information collects from sensors and complex integration of big data analytics in the IoT domain. IBDA indicates is fit for the purpose and seems suitable for IoT applications. M. Mazhar et al. [26] address big data analytics of IoT devices for smart cities. The proposed system used Hadoop ecosystem in a real environment and data processing performed using spark over Hadoop. The results revealed that the proposed work is efficient and scalable. Y. Kang et al. [27] showed data repository implementation model using MongoDB for IoT integrated RFID sensor. They devise a data

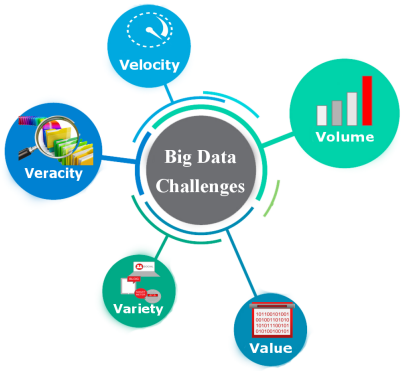

Fig. 3: Big Data Challenges.

repository schema that allows to store big data of IoT e.g. GPS, Sensor, and RFID data. The proposed model generates shared key to uniform data distribution over data servers and increase query speed. The result is acceptable, efficient, and effective for IoT-Big data.

E. New and Complex Dependencies Challenges

In recent years, IoT applications proliferate and become more sophisticated. Many of these smart applications are used by humans, i.e., things and humans will operate synergistically [5]. It offers new opportunities to a broad range of applications such as, healthcare [28], low cost price of devices [29], transportation [30], etc. There are few previous works have considered human in the loop for IoT applications. For example, in intelligent transport systems, vehicles talk with each other via the wireless technologies and take the decision of the speed, braking or crossing in the junction that will improve the traffic flow in real-time without any human intervention. However, in emergency situations or when something abnormal happens, the (system administrator or driver) immediately intervene to resolve any problem that occurs in the system. This is one of the most important issues of human-in-the-loop systems.

III. Conclusion

In summary, with the emergence of IoT, new regulatory approaches to ensure its energy, scalability, security and privacy, human-in-the-loop, big data, etc. become necessary. The IoT revolution is expanding connectivity via the internet and a wide range of applications (e.g. actuators, sensors and other embedded systems). This will have an effect on the quality, different life styles and the way we behave and interact with humans, machines and devices in the future. Therefore, new research challenges and problems will emerge due to the large-scale device proliferation and their inter-communication. This paper gives an overview of the key issues related to the IoT services and technologies. A number of researcher challenges have been described, which are expected to become a major research trends in the next decade. A number of previous works have been analysed, and most relevant WSN and IoT applications were presented.

IV. Acknowledgment

The authors would like to thank Ministry of Higher Education and Scientific Research (Iraq) and University of Diyala for the funding to conduct the research. Also, many thanks to Manchester Metropolitan University for their help and support.

References

[1] X. L. D. a. Li, Shancang and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, April 2015.

[2] W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley Professional, 2015.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[4] A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur, and H. Al-Bashar, "Dynamic clustering and management of mobile wireless sensor networks," *Comput. Netw.*, vol. 117, no. C, pp. 62–75, Apr 2017.

[5] J. A. Stankovic and L. Fellow, "Research Directions for the Internet of Things," pp. 1–7, 2014.

[6] S. Han and H. Woo, "NDN-based Pub / Sub System for Scalable IoT Cloud," *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 488–491, Dec 2016.

[7] M. Amoretti, O. Alphand, G. Ferrari, S. Member, F. Rousseau, and A. Duda, "DINAS : a Lightweight and Efficient Distributed Naming Service for All-IP Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 4662, no. c, pp. 1–14, 2016.

[8] K. Lee, H. Kang, J. P. Jeong, H. Kim, and J.-s. Park, "Secure DNS Name Autoconfiguration for IPv6 Internet-of-Things Devices," *Information and Communication Technology Convergence (ICTC), 2016 International Conference on*, pp. 564–569, 2016.

[9] D. C. Yacchirema and S. Member, "Smart IoT Gateway For Heterogeneous Devices Interoperability," *IEEE Latin America Transactions*, vol. 14, no. 8, pp. 3900–3906, 2016.

[10] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, "On Optimal Scheduling in Duty-Cycled Industrial IoT Applications Using IEEE802.15.4e TSCH," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3655–3666, Oct 2013.

[11] Shyam Sundar Prasad and C. Kumar, "An energy efficient and reliable internet of things," in *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*. IEEE, oct 2012, pp. 1–4.

[12] D. R. Dandekar and P. Deshmukh, "Energy balancing multiple sink optimal deployment in multi-hop wireless sensor networks," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*. IEEE, 2013, pp. 408–412.

[13] M. Kovatsch, S. Duquennoy, and A. Dunkels, "A Low-Power CoAP for Contiki," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*. IEEE, oct 2011, pp. 855–860.

[14] M. Al-Jemeli and F. A. Hussin, "An Energy Efficient Cross-Layer Network Operation Model for IEEE 802.15.4-Based Mobile Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 684–692, feb 2015.

[15] M. Hammoudeh, F. Al-fayez, H. Lloyd, R. Newman, and B. Adebisi, "System : Deployment Issues and Routing Protocols," *IEEE SENSORS*, vol. 17, no. 8, pp. 2572–2582, 2017.

[16] S. Pirbhulal, H. Zhang, E. E. Alahi, S. Mukhopadhyay, and H. Ghayvat, "A Novel Secure IoT-Based Smart Home Automation," pp. 1–19, 2017.

[17] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing Communication in 6LoWPAN with Compressed IPsec," *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*, 2011.

[18] M. Mohsin, Z. Anwar, G. Husari, E. Al-shaer, and M. A. Rahman, "IoTSAT : A Formal Framework for Security Analysis of the Internet of Things (IoT)," *Communications and Network Security (CNS), 2016 IEEE Conference on*, 2016.

[19] A. Capossele, V. Cervo, G. D. Cicco, and C. Petrioli, "Security as a CoAP resource : an optimized DTLS implementation for the IoT," *Communications (ICC), 2015 IEEE International Conference on*, pp. 549–554, 2015.

[20] M. Singh, R. Ma, S. Vl, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*, 2015.

[21] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless networks*, vol. 11, no. 4, pp. 419–434, 2005.

[22] N. Javaid, S. Cheema, M. Akbar, N. Alrajeh, M. S. Alabed, and N. Guizani, "Balanced energy consumption based adaptive routing for iot enabling underwater wsns," *IEEE Access*, vol. 5, pp. 10 040–10 051, 2017.

[23] F. Al-Turjman and M. Gunay, "Car approach for the internet of things," *Canadian Journal of Electrical and Computer Engineering*, vol. 39, no. 1, pp. 11–18, 2016.

[24] Z. Yaoxue, R. E. N. Ju, L. I. U. Jiagang, X. U. Chugui, G. U. O. Hui, and L. I. U. Yaping, "A Survey on Emerging Computing Paradigms for Big Data ," vol. 26, no. 1, 2017.

[25] M. R. Bashir and A. Q. Gill, "Towards an iot big data analytics framework: Smart buildings systems," *2016 IEEE 18th International Conference on High Performance Computing and Communications*, pp. 1325–1332, Dec 2016.

[26] M. M. Rathore, S. Member, A. Ahmad, and A. Paul, "IoT-Based Smart City Development using Big Data Analytical Approach," *(ICA-ACCA), IEEE International Conference on*, 2016.

[27] Y.-s. Kang, I.-h. Park, J. Rhee, and Y.-h. Lee, "MongoDB-Based Repository Design for IoT-Generated RFID / Sensor Big Data," *IEEE Sensors Journal*, vol. 16, no. 2, pp. 485–497, 2016.

[28] S.-y. Ge, S.-M. Chun, H.-S. Kim, and J.-T. Park, "Design and implementation of interoperable IoT healthcare system based on international standards," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, jan 2016, pp. 119–124.

[29] B. Moatamed, F. Shahmohammadi, and R. Ramezani, "Low-cost Indoor Health Monitoring System," *Wearable and Implantable Body Sensor Networks (BSN), 2016 IEEE 13th International Conference on*, pp. 159–164, 2016.

[30] S. H. Sutar, R. Koul, and R. Suryavanshi, "Integration of Smart Phone and IOT for development of Smart Public Transportation System," *Internet of Things and Applications (IOTA), International Conference on*, pp. 73–78, 2016.