Internet of Things (IoT) and its Applications: A Survey

Article *in* International Journal of Computer Applications · September 2020

DOI: 10.5120/ijca2020919916

1 author:

Afrah Salman Dawood
University of Technology, Iraq
6 PUBLICATIONS **10** CITATIONS

SEE PROFILE

Internet of Things (IoT) and its Applications: A Survey

Afrah Salman Dawood
University of Technology
Iraq, Baghdad

ABSTRACT
Internet of Things (IoT) is the concept of connecting different devices to each other and to the internet to transmit thousands of bits of data and information. IoT is changing a great part of the world relevant; from the manner in which we drive to how we make buys and even how we get vitality to our homes. Complex sensors and chips are embedded around us. How these devices share data and information and how we make use of them. The common platform of IoT is personal health. In this paper, an overview of different platforms and architecture, applications and challenges

Keywords
Internet-of-Things (IoT), IoT platforms, IoT applications, sensors, personal health, IoT challenges

1. INTRODUCTION
The expression "Internet of Things" was formally presented in 1998–1999 by Kevin Ashton of Automatic Identification center (Auto-Id) at Massachusetts Institute of Technology (MIT). Kevin recommended widely Web-associated RFID advancements can be utilized in supply chains to monitor things without human contribution [18]. Internet of Things (IoT) is the concept of connecting different devices to each other and to the internet to transmit thousands of bits of data and information. IoT is changing a great part of the world significantly; from the manner in which we drive to how we make buys, what is more, even how we get vitality to our homes. Complex sensors and chips are implanted around us. How these devices share data and information and how we make use of them. The common platform of IoT is personal health.

different devices contact the IoT stage which arranges the data from various devices and offers assessment to bestow the most significant data to applications that address explicit industry needs. The diagnostic bus gathers data from all these sensors then passes it to a passage in the vehicle which coordinates sorts the information from sensors. Along these lines, most important demonstrative data will be transmitted to the maker's stage yet before sending; a secure connection must be established.

Creating applications for the IoT could be a difficult undertaking because of a few reasons; (I) the high multifaceted nature of circulated registering, (ii) the absence of general rules or systems that handle low level correspondence and improve high level execution, (iii) different programming languages, and (iv) different communication protocols. It includes designers to deal with the framework and handle both programming and equipment layers alongside protecting all practical and non-useful programming prerequisites. This multifaceted nature has prompted a snappy development regarding presenting IoT programming structures that handle the previously mentioned difficulties [1].

After some time, the IoT is depended upon to have colossal home and business applications, to add to the individual fulfillment and to build up the world's economy. For example, smart homes will enable their occupants to normally open their garage while arriving at home, set up their espresso, control environment control systems, televisions and various machines. So as to comprehend this potential improvement, rising advances and progressions, and organization applications need to grow moderately to facilitate showcase solicitations and customer needs. Besides, devices ought to be made to fit customer essentials regarding openness wherever and at whatever point. Moreover, new shows are required for correspondence likeness between heterogeneous things (vehicles, living things, products, telephones, apparatuses, and so forth.) [2], see Fig.1.

The devices conduct with the IoT stage which incorporates the information from huge gadgets and gives dissection in order to pick up extremely worthy information to apps which address specific industry requirements. The diagnostic bus gathers data and information from all these sensors and after that passes it to a gateway in the car which integrates sorts the data from sensors. In this manner, most related diagnostic data will be transferred to the manufacturer's rostrum, however, a secure connection must be established before sending.

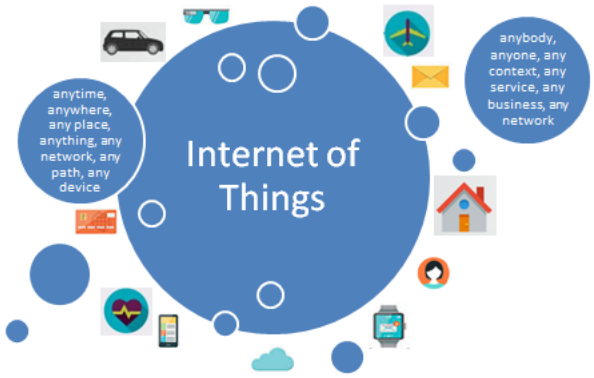

Fig.1: Internet of Things

As the complexity of Internet of Things (IoT) systems increases, a large variety of tools and technologies for IoT management are making their way into both research setups and the market. IoT management arrangements must consider the asset confinements of implanted gadgets, as well as their heterogeneity and network dynamics. With these in mind, the Internet Engineering Task Force developed several standards targeting the joining and inter-operation of heterogeneous gadgets, for example, the Representational State Transfer Configuration Protocol (RESTCONF) or the Constrained Application Protocol (CoAP) Management Interface. Concurrently, the Open Mobile Alliance developed the Lightweight Machine-to-Machine protocol, for IoT device management. This paper provides a comprehensive, up-to-

date overview of IoT management technologies, frameworks and protocols. Also, it proposes a taxonomy for IoT devices management. In addition to presenting the various solutions, the paper provides comparative views, standardization timeline, and market analysis. The exhibited analysis ranges from customary network the management protocols, for example, Straightforward System The board Convention, to the most up to date IoT the executives and setup conventions, for example, CoAP Management Interface and Lightweight Machine-to-Machine protocols. Moreover, this survey identifies remaining challenges and solutions offered by recent management protocols, not covered by previous surveys [1].

Besides, design institutionalization can be viewed as a spine for the IoT to make an aggressive situation for organizations to convey quality items. Likewise, conventional Web engineering should be overhauled to coordinate the IoT challenges. For instance, the colossal number of articles ready to interface with the Web ought to be considered in numerous basic conventions. In 2010, the quantity of Web associated objects had outperformed the world's human populace [11]. Accordingly, using an enormous tending to space (e.g., IPv6) gets important to fulfill client needs for brilliant items. Security and protection are other significant necessities with regard to the IoT on account of the innate heterogeneity of the Web related objects and the capacity to screen and control physical articles. Over and above, the executives and observing of the IoT should occur to guarantee the conveyance of top notch administrations to clients at a productive expense. The rest of the sections in this paper is organized as follows: section II details related work and research directions; section III explains the architecture and platform of the IoT; section IV is the applications of IoT; section V details the challenges of IoT; and finally, section VI is about the discussion of IoT.

2. RELATED WORK AND RESEARCH DIRECTIONS

Several survey papers and researches on IoT have been published. The authors in reference [1] surveyed the security of the primary IoT structures, an aggregate of 8 systems are considered. For every structure, we explain the proposed design, the basics of growing outsider shrewd applications, the good equipment, and the security highlights. Reference [2] studied the IoT all in all, referencing different IoT designs, showcase openings, IoT components, correspondence advances, standard application conventions, fundamental difficulties and open research issues in the IoT territory. Reference [3] displayed various business IoT structures and gave a relative investigation dependent on used methodologies, bolstered conventions, use in industry, equipment prerequisites, and applications improvement. In [4], the creators studied the security and protection issues in IoT from four alternate points of view. To begin with, they feature on the impediments of applying security in IoT gadgets (for example battery lifetime, processing power) and the proposed answers for them (for example lightweight encryption conspire intended for installed frameworks). Second, they abridge the characterizations of IoT assaults (for example physical, remote, nearby, and so forth.). Third, they center around the components and structures planned and executed for verification and approval purposes. Last, they break down the security issues at various layers (for example physical, arrange, and so forth.). A concise outline of the current IETF models for the Web of things is given in [5]. Creators in [6] quickly examined about the definition of IoT, the means by which IoT delegates different advances, concerning its engineering, qualities and applications, IoT applicable concept and what are the future difficulties for The research in [7] presents a comprehensive overview of IoT and survey of existing architectures, enabling technologies, applications and research challenges for IoT. In [8], the paper condenses the best in class in associated vehicles from the requirement for vehicle information and applications thereof, to empowering advances, challenges, and distinguished chances. the paper in [9] conducts a far reaching diagram of IoT concerning framework engineering, empowering innovations, security and protection issues, and presents the coordination of haze/edge registering and IoT, and applications. Particularly, this work initially investigates the conduction among Cyber-Physical Systems(CPS) and IoT, both of them suppose considerable labors in realizing an insightful cyber-physical world. The paper in [10] provides an overview of the Industrial Internet with the emphasis on the architecture, enabling technologies, applications, and existing challenges.

3. IOT PLATFORM ARCHITECTURE

IoT is implemented in different platforms for a wide range of applications; thus, the architecture differs according to the platform. To work with all the various operators affecting IoT architecture, it's easier and progressively compelling to locate a dependable supplier of IoT arrangements. This choice will altogether lessen the quantity of assets spent in transit. Basically, there are three IoT architecture layers which are: a) Client side (IoT Device Layer) b) Administrators on the server side (IoT Gateway Layer) and finally, c) A pathway for associating customers and administrators (IoT Platform Layer) [12]. Truth be told, tending to the requirements of every one of these layers is vital on every one of the phases of IoT engineering. Being the premise of attainability basis, this consistency makes the outcome planned truly work. Likewise, the major highlights of manageable IoT engineering incorporate usefulness, adaptability, accessibility, and practicality. Without tending to these situations, the aftereffect of IoT design is a disappointment. Subsequently, all the previously mentioned necessities are tended to in 4steps as follows (see Fig.2) [12]:

- **Networked things (wireless sensors and actuators)**

Detecting and activating stage covers and modifies everything required in the physical world to pick up the vital bits of knowledge for additional investigation. The fundamental element of a sensor is the capacity to change over data got in the external world into information for investigation (for example it is essential to begin with the incorporation of sensors in the four phases of an IoT design system to get data in an appearance that can be really prepared. The actuators can mediate the physical reality (for example they can turn off the light and change the temperature in a room).

- **Internet getaways and Data Acquisition Systems (Sensor data aggregation systems and analog-to-digital data conversion)**

The paths of digitized amassed information. In spite of the way that this period of IoT designing still strategies working in a closeness with sensors and actuators, Internet getaways and Data Acquirement Structures (DAS) appear here too. Specifically, the later interface with the sensor framework and absolute yield, while Internet gets away from work through Wi-Fi, wired LANs and perform further taking care of. The rule importance of this stage is to process the huge proportion

of information assembled on the past stage and press it to the perfect size for extra examination. Besides, the fundamental change to the extent that planning and structure happens here.

- **The appearance of edge IT systems**

The prepared data is moved to the IT world. In particular, edge IT structures perform upgraded assessment and pre-dealing with here (for instance it insinuates AI and observation propels). Simultaneously, some additional dealing with may happen here, going before the period of entering the server ranch. In like way, Stage 3 is immovably associated with the past stages in the structure of a building of IoT. In like manner, the territory of edge IT systems is close to the one where sensors and actuators are organized, making a wiring closet. All the while, the residence in remote work environments is also probable.

- **Data center and cloud (Analysis, management, and storage of data)**

The guideline frames on the last step of IoT configuration happen in server homestead or cloud. Completely, it enables start to finish preparing, nearby a consequent update for criticism. Here, the capacities of both IT and OT (operational advancement) specialists are required (for instance the phase starting at now fuses the scientific capacities of the most essential position, both in electronic and human universes). Along these lines, the data from various sources may be consolidated here to ensure an all-around assessment. In the wake of satisfying all the quality rules and necessities, the information is reclaimed to the physical world — yet in a readied and conclusively examined appearance formerly.

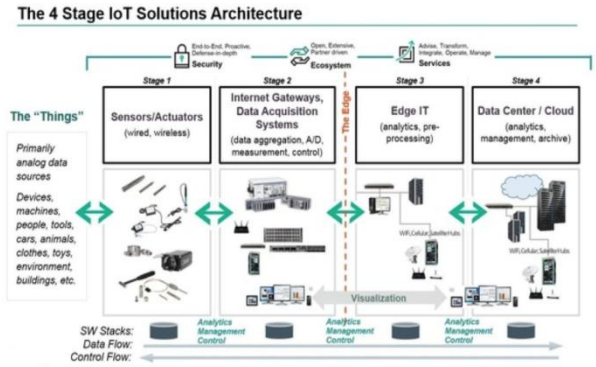

Fig.2: Stages of IoT Architecture [12]

In fact, there is an alternative to expand the way toward building a maintainable IoT design by presenting an additional phase in it. It alludes to starting a client's power over the structure — if just your outcome does exclude full computerization, obviously. The fundamental errands here are perception and the board. In the wake of including Stage 5, the framework transforms into a circle where a client sends directions to sensors/actuators (Stage 1) to play out certain activities. Furthermore, the procedure starts from the very beginning once more.

An IoT stage is a multi-layer innovation that empowers direct provisioning, the executives, and robotization of associated gadgets inside the IoT universe. It essentially interfaces your equipment to the cloud by utilizing adaptable network alternatives, endeavor level security instruments, and expansive information preparing powers. Generally, IoT steps can vary according to needs. It is usually alluded to as middleware when explaining how it associates remote gadgets to client applications (or different gadgets) and deals with each of the collaborations among the equipment and the application layers [13]. Different IoT platforms can be classified and described in Table 1.

Table 1. Fields of IoT platforms

General Field	IoT Platform
Generic IoT Platforms for analytics [17]	Agricultural environment,
	smart home, etc.
Cloud platforms for IoT [14]	Thingworx 8 IoT Platform
	Microsoft Azure IoT Suite
	Google Cloud's IoT Platform
	IBM Watson IoT Platform
	AWS IoT Platform
	Cisco IoT Cloud Connect
	Salesforce IoT Cloud
	Kaa IoT Platform
	Oracle IoT Platform
	Thingspeak IoT Platform
	GE Predix IoT Platform
Industrial IoT platform (IIoT) [15]	Predictive maintenance [16]
	Remote Monitoring
	Process automation
	Remote management

4. IoT APPLICATIONS

Various applications have been implemented with IoT using different types of sensors, smart devices, servers, etc. Fig.3 lists different applications that make use of IoT concepts and platforms.

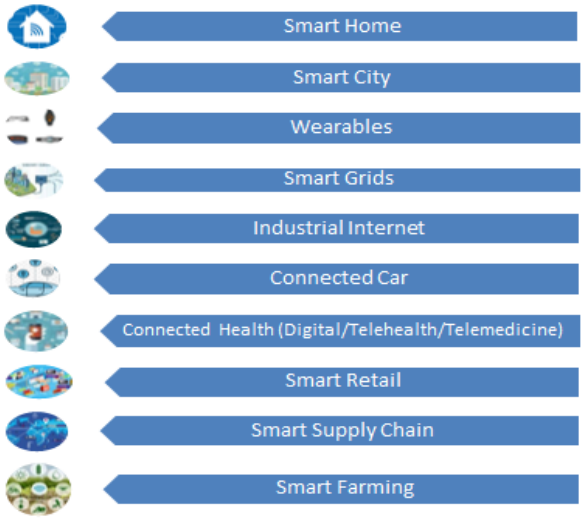

Fig.3: IoT applications

The most important and efficient application that stands out is the smart home and similar applications in the field. The plurality of the present surveys on IoT smart home agendas concentrates on operation provided by more intelligent connected devices besides to privacy concerns related to IoT (see table 2) [18]. Just like smart homes, wearable remains an important topic among potential IoT applications that make life easier. Smart cities, as the name indicates, is a big technology and spreads a broad difference of use cases, from water distribution and traffic administration to waste administration and environmental observations. The reason why it is so public is that it attempts to take off the inconvenience and troubles of people who live in cities. On the other hand, smart networks essentially promise to extract data on the practices of buyers and power providers in a robotized design to improve the effectiveness, financial matters, and unwavering quality of power circulation. [26] One tactic is to think about the Industrial Internet by taking a glimpse at related gadgets in ventures, for instance, power age, oil, gas, and social insurance. It also uses circumstances where improvised personal time and architecture disappointments can bring about dangerous circumstances. A framework inserted with the IoT will in general combine gadgets like wellness groups for heart checking machines.

Table 2: IoT applications

Industry	Use case
Smart City	Smart bin offers smart waste monitoring through smart sensors and route improvement technologies [19].
Transport	Spanish train administrator RENFE utilizes Siemens' high-speed train and monitors trains creating strange examples and sends them back for investigation to stop fail on the route [20].
Agriculture	Semios utilizes sensors and machine vision innovation to follow bug populaces in garden, and other farming settings [21]
Financial Sector	Dynamic Insurance utilizes Snapshot to decide Insurance premium for vehicle drivers [22].
Healthcare	Abilify MyCite (aripiprazole tablets with sensor) has an ingestible sensor inserted in the pill that records that the medicine was taken [23].
Government	US region has actualized smart meter checking for the whole town's private and business water meters [24].
Utility	US oil and gas organizations are advancing oilfield generation with the IoT. In this IoT model, the organization is utilizing sensors to gauge oil extraction rates, temperatures, well pressure, and so on. [24].
Environment	Self-ruling boats and watercraft are formerly watching the oceans conveying advanced sensor instruments, gathering information on changes in Arctic ice [25].

Connected cars, connected health and other technologies are huge and broad systems of various sensors, radio wires, installed programming, and advancements that aid correspondence to explore in our perplexing world. They have the duty of settling on choices with consistency (remote checking), precision, and speed. they additionally must be dependable. These prerequisites will turn out to be considerably progressively basic when people surrender control of the directing haggle to the independent vehicles that are being tried on our parkways at this moment.

5. IOT CHALLENGES

In general, any technology has many challenges including security, difficulty of implementation in the real world and other points to consider while implementing the topology. The Internet of Things (IoT) is perhaps the most smoking innovation in the period of computerized change, associating everything to the Internet. It is simply the center innovation behind brilliant homes, driving vehicles, savvy utility meters, and keen urban areas. However, there are nine fundamental security challenges for the eventual fate of the web of things (IoT). The quantity of IoT gadgets is quickly expanding in the course of the most recent couple of years. As indicated by an expert firm Gartner, there will be in excess of 26 billion associated gadgets around the globe by 2020, up from only 6 billion in 2016. While IoT gadgets bring powerful correspondence between gadgets, mechanize things, spare time and cost and have various advantages, there is one thing as yet concerning the clients—IoT security. There have been explicit episodes which have made the IoT gadgets testing to trust. Below are basic nine challenges for the future of IoT [27]:

- **Outdated equipment and programming**

Since the IoT gadgets are being utilized progressively, the producers of these gadgets are concentrating on building new ones and not giving enough consideration to security. A larger part of these gadgets doesn't get enough updates, though some of them never get a solitary one. This means these items are secure at the hour of procurement however gets helpless against assaults when the programmers discover a few bugs or security issues. When these issues are not fixed by discharging ordinary updates for equipment and programming, the gadgets stay powerless against assaults. For each seemingly insignificant detail associated with the Internet, the standard updates are an absolute necessity. Not having updates can prompt information break of clients as well as of the organizations that assemble them.

- **Use of weak and default certifications**

Many IoT organizations are selling gadgets and furnishing shoppers default accreditations with them — like an administrator username. Programmers need only the username and secret word to assault the gadget. At the point when they know the username, they complete savage power assaults to contaminate the gadgets.

- **Malware and ransomware**

The quick ascent in the advancement of IoT items will make cyberattack changes eccentric. Cybercriminals have become propelled today — and they lock out the buyers from utilizing their very own gadget.

Predicting and forestalling assaults: Cybercriminals are proactively discovering new strategies for security dangers. In such a situation, there is a requirement for not just finding the vulnerabilities and fixing them as they happen yet additionally figuring out how to foresee and forestall new dangers. The

test of security is by all accounts a long-haul challenge for the security of associated gadgets. Present day cloud administrations utilize risk knowledge for foreseeing security issues. Other such methods incorporate AI-fueled checking and investigation instruments. Be that as it may, it is unpredictable to adjust these methods in IoT in light of the fact that the associated gadgets need preparing of information in a split second.

- **Difficult to discover if a gadget is influenced**

Although it isn't generally conceivable to ensure 100% security from security dangers and ruptures, the thing with IoT gadgets is that a large portion of the clients don't become more acquainted if their gadget is hacked. When there is an enormous size of IoT gadgets, it gets hard to screen every one of them in any event, for the specialist co-ops. It is on the grounds that an IoT gadget needs applications, administrations, and conventions for correspondence. Since the quantity of gadgets is expanding fundamentally, the quantity of things to be overseen is expanding much more. Thus, numerous gadgets continue working without the clients realizing that they have been hacked.

- **Data assurance and security challenges**

In this interconnected world, the insurance of information has become extremely troublesome in light of the fact that it gets moved between numerous gadgets inside a couple of moments. One minute, it is put away in versatile, the following moment it is on the web, and afterward the cloud. This information is moved or transmitted over the web, which can prompt information spill. Not every one of the gadgets through which information is being transmitted or got are secure. When the information gets spilled, programmers can offer it to different organizations that disregard the rights for information protection and security. Besides, regardless of whether the information doesn't get spilled from the customer side, the specialist co-ops probably won't be consistent with guidelines and laws. This can likewise prompt security episodes.

- **Use of self-ruling frameworks for information the board**

From information assortment and systems administration perspective, the measure of information created from associated gadgets will be too high to even consider handling. It will without a doubt need the utilization of AI devices and mechanization. IoT administrators and system specialists should set new principles with the goal that traffic examples can be distinguished effectively. Be that as it may, utilization of such apparatuses will be somewhat hazardous on the grounds that even a smallest of slip-ups while designing can cause a blackout. This is basic for huge ventures in social insurance, monetary administrations, force, and transportation businesses.

- **Home security**

Today, an ever-increasing number of homes and workplaces are getting keen with IoT availability. The huge manufacturers and engineers are fueling the condos and the whole structure with IoT gadgets. While home robotization is something to be thankful for, however, not every person knows about the prescribed procedures that ought to be dealt with for IoT security. Regardless of whether the IP addresses get uncovered, this can prompt presentation of private location and other contact subtleties of the purchaser. Assailants or invested individuals can utilize this data for underhanded purposes. This leaves shrewd homes at potential hazard.

- **Security of autonomous vehicles**

Just like homes, oneself driving vehicles or the ones that utilize IoT administrations, are additionally in danger. Shrewd vehicles can be commandeered by gifted programmers from remote areas. When they get to, they can control the vehicle, which can be dangerous for travelers.

6. DISCUSSION

The developing thought of the Internet of Things (IoT), where the Internet meets the physical world, is quickly discovering its way all through our cutting-edge life, meaning to improve the personal satisfaction by associating many shrewd gadgets, advancements, and applications. By and large, the IoT would take into consideration the computerization of everything around us. This paper recorded and studied various stages and applications. This, thus, ought to give a decent establishment to scientists and specialists who are intrigued to increase a knowledge into the IoT advances and conventions to comprehend the general engineering and job of the various segments and conventions that comprise the IoT. Besides, different challenges related to different IoT platforms and environments have been discussed.

7. REFERENCES

[1] M. Ammar, G. Russello, B. Crispo, “Interent of Things: A Survey on the Security of IoT Framework”, Journal of Information Security and Applications 38 (2018) 8–27.

[2] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surveys Tutorials 2015;17(4):2347–76.

[3] Derhamy H, Eliasson J, Delsing J, Priller P. A survey of commercial frame- works for the internet of things. In: 2015 IEEE 20th conference on emerging technologies & factory automation (ETFA). IEEE; 2015. p. 1–8.

[4] Yang Y, Wu L , Yin G , Li L , Zhao H . A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 2017.

[5] Sheng Z, Yang S , Yu Y , Vasilakos AV , McCann JA , Leung KK . A survey on the ietf protocol suite for the internet of things: standards, challenges, and op- portunities. IEEE Wireless Commun 2013;20(6):91–8.

[6] K. K. Patel, S. M. Patel, P. G. Scholar, C. Salazar, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”, DOI 10.4010/2016.1482, ISSN 2321 3361 © 2016 IJESC.

[7] Giri, S. Dutta, S. Neogy, Z. Pervez, K. P. Dahal, Z. Pervez, “Internet of things (IoT): a survey on architecture, enabling technologies, applications and challenges”, October 2017, DOI: 10.1145/3109761.3109768, the 1st International Conference.

[8] J. Siegel, D. C. Erb, S. E. Sarma, A Survey of the Connected Vehicle Landscape--Architectures, Enabling Technologies, Applications, and Development Areas, October 2017IEEE Transactions on Intelligent Transportation Systems, DOI: 10.1109/TITS.2017.2749459.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A Survey on Internet of Things: Architecture, Enabling

Technologies, Security and Privacy, and Applications, March 2017, DOI: 10.1109/JIOT.2017.2683200.

[10] J. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, Q. Yan, Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges, April 2017, IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2017.2691349.

[11] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," CISCO White Paper, 2011.

[12] [Internet], Available from: https://medium.com/datadriveninvestor/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f [Accessed: 2019-12-15].

[13] [Internet], Available from: https://www.kaaproject.org/what-is-iot-platform [Accessed: 2019-12-15].

[14] [Internet], Available from: https://dzone.com/articles/10-cloud-platforms-for-internet-of-things-iot [Accessed: 2019-12-20].

[15] [Internet], Available from: https://www.iotworldtoday.com/2019/08/07/top-10-iiot-platforms/ [Accessed: 2019-12-20].

[16] [Internet], Available from: https://www.digi.com/blog/post/about-the-industrial-iot-definition-use-cases-and [Accessed: 2019-12-20].

[17] Pradeep B. and Balasubramani R, "Generic IoT Platform for Analytics", IOP Conf. Series: Materials Science and Engineering 594 (2019) 012046, IOP Publishing, DOI:10.1088/1757-899X/594/1/012046.

[18] Dasgupta, A. Q. Gill and F. Hussain, "Privacy of IoT-Enabled Smart Home Systems", Open access peer-reviewed chapter, February 20th 2019, DOI: 10.5772/intechopen.84338.

[19] N. Sharma, N. Singha and T. Dutta, "Smart bin implementation for smart cities", International Journal of Scientific and Engineering Research, 2015;6(9):787-79.

[20] [Internet]. Available from: https://www.rcrwireless.com/20160912/big-data-analytics/siemens-train-teradata-tag31-tag99 [Accessed: 2020-1-5].

[21] N. Kshetri, "The economics of the internet of things in the global south", 2016; doi:10.1080/01436597.2016.1191942.

[22] P. Handel, I. Skog, J. Wahlstrom, F. Bonawiede, R. Welch, J. Ohlsson and M. Ohlsson, "Insurance telematics: Opportunities and challenges with the smartphone solution", IEEE Intelligent Transportation Systems Magazine, 2014;6(4):57-70.

[23] [Internet]. Available from: https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication [Accessed: 2020-1-5].

[24] [Internet]. Available from: https://www.sas.com/en_us/insights/articles/big-data/3-internet-of-things-examples.html [Accessed: 2020-1-5].

[25] R. B. Hughes, "The autonomous vehicle revolution and the global commons", SAIS Review of International Affairs, ISSN: 1945-4724, 2016;36(2):41-56

[26] [Internet]. Available from: https://dzone.com/articles/top-10-uses-of-the-internet-of-things [Accessed: 2020-1-5].

[27] [Internet]. Available from: https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/ [Accessed: 2020-1-5].