International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 8, August-2018

Study on Internet of Things: Applications

Fida Hussain#, Dr. Ashish Oberoi*

[#]MTech CSE, RIMT University, Mandi ,Gobindgrah ,Punjab, India.
[*]HOD CSE, RIMT University, Mandi ,Gobindgrah ,Punjab, India.

Abstract— **IoT (Internet of Things) can be defined as the integration of real-worlddevices with the internet as it helps in creating the connection between the existingdevices and Internet. IoT is the novel technology to make the computing devices sensory which otherwise are senseless .IoT provides the means to ensure communication among devices using the internet from different cohorts which require to use IP (Internet Protocol) addresses assigned to each device. The growth of the IoT is increasing at the greater pace with the advancement in the technology. The development of the IoTin anumber of fields has led to the development of various applications which include ITS (Intelligent Transportation Systems), smart home systems, intelligent shopping systems,etc. The primary idea of the IoT is to connect the previous and the new physical objects to the Internet. It can be estimated that by the year 2050, the total number of devices connected to the internetwill be around five times more than its users.Along with such advancements, this paper presents the review of major applications of IoT along with challenges, findings of previous researches and future work that can be carried based on the results that are achieved till now.**

Keywords— **IoT, Bluetooth, IP based IoT, Non-IP based IoT,IoT network, Security.**

I. INTRODUCTION

IoT (Internet of Things) is described as the group of devices, sensors and various objects, which are interconnected to each other through the internet. These all communicate[12] with each other for some specific purposes toprovide various services to their consumers. It is the form of a networkcontaining devices, which are connected together for collecting and sharing data.

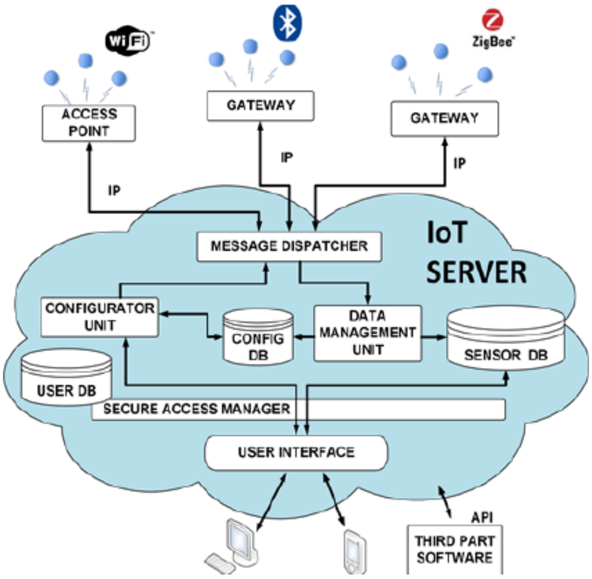


Fig.1: Block Diagram of IoT [11]

History of IoT

The Arpanet came into existence in 1969; this is also known as the older version of the internet. The first internet "device" was created by John Romkey in 1990 [13]. It was the toaster, which is turned on and off with the help of internet. After this, the toaster was connected to the computer system with the TCP/IP networking. It used the SNMP (Simple Network Management Protocol)management information base (MIB) for power on the system. After this, in 1999, the IoT term was coined by Kevin Ashton. It was considered as the big year for the IoT. In the year2008, the group of companies started the IPSO Alliances, which helps in promoting the IP (Internet Protocol). In 2009, the IoT was born. In this, various objects and things were connected to the internet. There were around 12.5 billion devices connected to the internet in 2010.

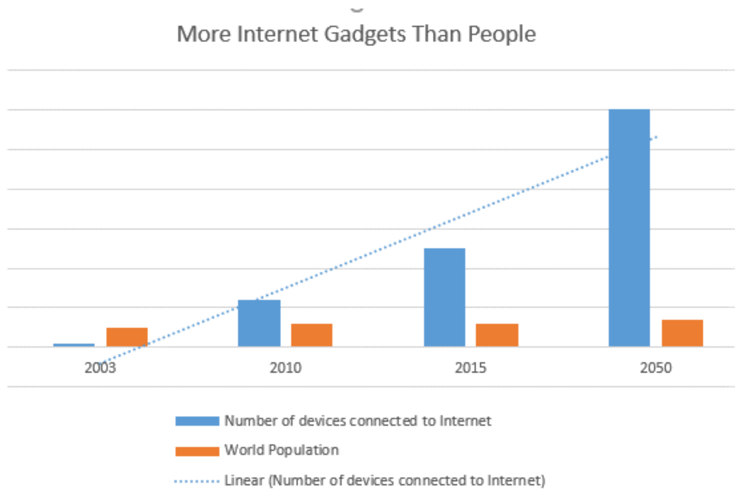


Fig.2: Total devices vs. World population [13]

Fig. 2 represents the total number of the devices that are connected to the internet, are more than the totalnumber of users [13].

The IoT can be broadly classified [1] into three categories. These are as below:

a) IOT systems to acquire and share the contextual information.
b) IOT systems to process the contextual information
c) To improve the overall quality of the IoT systems

From the above categories, only the first two categories can be taken as the primary functional block of IoT. Itorobong S. Udoh and Gerald Kotonya [1] presented the IoT technology stack and described the requirements of the IoT applications that are normally used. There were many challenges while developing the IoT that need to be identified. Vijay Sivaraman et al., [2]examined the security implications of the IoT devices. The research developed the open network for the usage of the households IoT. The testing of the vulnerabilities of the various devices was done. These devices are subjected to be targeted under the laboratory conditions. After this, the IoT suppliers, insurers, and consumers were invited for the evaluation of the results. After the examination process, various possible approaches were also proposed, which helped in mitigating the risks.

Irina-IoanaPătru et al., [4] presented the solution, which helps in connecting various devices into the single entity that can be accessed at any time. The proposed work helps in integrating the functionalities of the various home automation devices. The implemented model presented the connection of the home appliances like Lightbulb and Thermostat in one system that can be accessed remotely. The advantage of these systems is that all the configurations can be done on only one device. The proposed solution helps in presenting the modular implementation of the new smart home application systems.

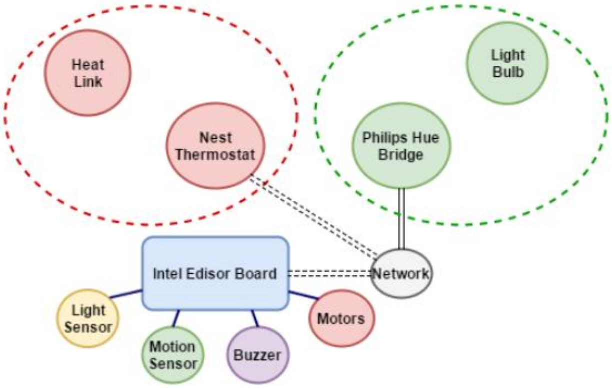


Fig.3: Communication system [4]

GianlucaBarbona et al., [5] presented the ASIP (Arduino Service Interface Programming) model, which helps in providing the services and add new capabilities to the microcontroller. The model is an infrastructure, which comprises the software architecture and helps in managing the micro-controllers of higher-level languages. The proposed network architecture was based on the USB links and TCP Sockets.

KashifSaleem et al., [7] proposed the BSCoP (Bioinspired secure Ipv6 Communication Protocol) for the IoT. Routing protocol for the Lossy as well as for the Low power networks was also enhanced to provide more reliable services. This was implemented with the help of a classification algorithm, which is inspired by the AIS (Artificial Immune System). This system works by detecting the behavior of the nodes. The proposed model was able to detect the excessive amount of the broadcasts and can isolate them with the help of a classification algorithm. These help in improving the power as well as the transmission rates.

Romeo Giuliano et al., [8]tackled the various security issues for the non-IP devices. This helped to make the connection with the mediator gateway by the short range. They have proposed the security algorithm for the Unidirectional as well as bi-directional terminals based on the capabilities of the terminals. The time-based solution was proposed that helps in a secure transaction. The method does not require the server for the management of various devices.

Gartner's Emerging Technologies

The Gartner's Emerging Technologies helps the businesses in understanding the emerging trends that they need to be included for the competitive advantages. The phones are becoming smarter, the mobile payments options are included but to make it widespread, the technology should be developed with the help of the hype cycle. There are various new emerging technologies which are connected to the internet and works in the more intelligent way. These include Mobile Robots, Big Data, IoT (Internet of Things), Autonomous Vehicles, Internet TV, Wireless Power, Machine-to-machine communication, Home Health Monitoring, and Complex Event Processing.

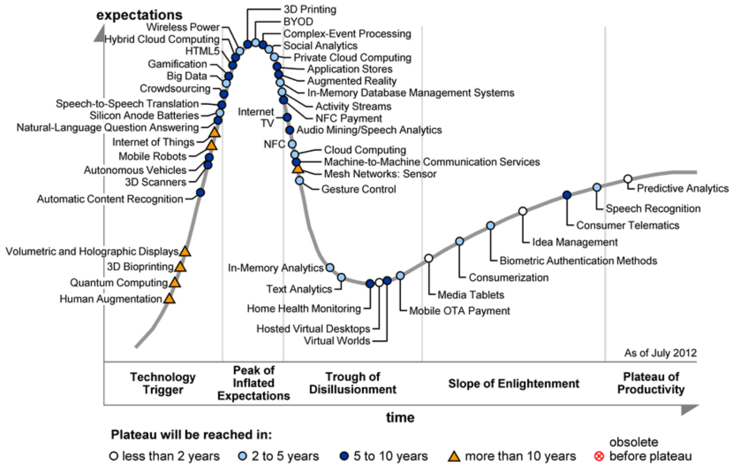


Fig. 4: Gartner's Hype Cycle for Emerging Technologies 2012 [20]

To make the system possible for the massive connection of devices, the industry must have to find out the correct balance for the power consumption, bandwidth, and cost. The other wireless protocols include 3G, 4g, Bluetooth, and Wi-Fi that need to be complemented by the wireless networks for the better designing of things. All the technologies, which are included in the Hype Cycle, are because of their high levels of Hype [20].

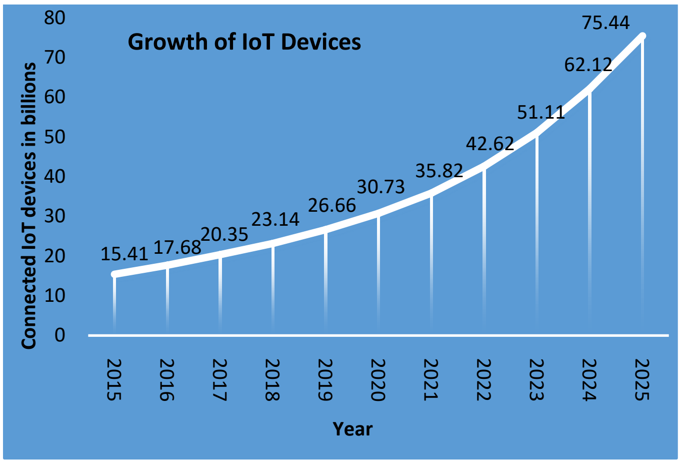


Fig. 5: Growth of IoT Devices [21]

In the past few years, the number of IoT devices are increasing

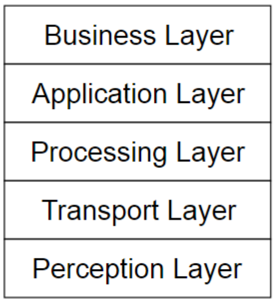
ata faster pace. Fig. 5 shows the number of IoT devices in billions that were connected from 2015 and the expected number of total devices that will be connected tothe year 2025. It can be seen that by the year 2020, there will be 30.73 billion installed IoT devices and this number will be almost double in the year 2024 [21]. Thus, there is a needfor more advancements and features so that the IoT can provide more security and required features to its users along with the performance efficiency.

II. Architecture of IOT

The overall architecture of IOT is divided into five layers that have different functions to perform. These layers are responsible for the overall functioning of the IoT system. The architecture is as shown in Fig. 6.

1) Business Layer

This layer helps in managing the applications, business, and the relevant models. This layer also researches the profit, and the business models and IoT cannot be effective without the research on the business model. This layer also equally manages the privacy of the user's data.



Business Layer
Application Layer
Processing Layer
Transport Layer
Perception Layer

Fig.6: Architecture of IOT [14]

2) Application Layer

The main purpose of this layer is usually based on the data processed in the Process Layer and helps in developing the applications of the IoT (Internet of things). These include logistics management, intelligent transportation, LBS (Location Based Service) and Identify Authentication. The major function of the application layer is to provide the applications. This layer is considered as the main layer, which leads to the large-scale development of the IoT.

3) Processing Layer

The processing layer helps in storing, analyzing, and processing all the information of the devices, which is received from the transport layer. This layer is used to carry a large amount of data and helps in processing large datasets. The main techniques, which are included in this, are cloud computing, database, ubiquitous computing, and intelligent processing.

4) Transport Layer

The transport layer is also known as Network Layer and plays the major role in transmitting the data, which is received from the Perception Layer to the processing part. The transmission occurs with the help of LAN (Local Area Network). Other techniques, which are utilized in this layer, are 3G, FTTx, Bluetooth, Wi-Fi, ZigBee, and IR.

5) Perception Layer

The perception Layer is used to perceive all the physical properties of the devices. The physical properties include the temperature and the location. All these can be retrieved with the help of sensors like Infrared Sensors, 2-D barcode, and RFID. The major role of this layer is to gather all the required information and convert it to the digital signals. This also needs to implant a microchip to sense the temperature, speed and other parameters of the devices. The usage of the nanotechnology can be seen in this; it helps in making the chip small enough so that it can be implanted easily into the objects.

III. FINDINGS

IP based and non-IP basedIoTs

IoT ensures the communication among various types of devices using the unique IP addresses assigned to each device through internet [7]. In addition, different IP based IoT were used in the pastlike IPv4, which were having some limitations that have been documented regarding depleting the address space. Because of the IPv4 limitations, the IPv6 is being used currently for the Internet of Things (IoT). The devices related to the Internet of Things come in different quality and sizes and therefore contains various manufacturing cost. The IoT nodes contain various communication capabilities and packet forwarding and routing due to the reduction in the size of the IP stack. However, having the same IP backbone, the IoT networks regarding layered security are not compared with the traditional networks. Further, for real-time IPv6 routing based IoT devices, the RPL (Routing Protocols for low power) and Lossy networks communicate directly through the Internet without using the packet translation. The IPv6 also uses Bio-inspired Secure IPv6 Communication protocol for providing an edge-to-edge communication for the IPv6 based communication [7].

Many times, the protocol implementation on some of the devices make use of network stack which implies that such devices should contain processors, memory, operating system and so on which ultimately leads to the increase of cost andcomplexity of the network. In addition, such devices [8] become the means for hacking or misconfiguration and therefore start requiring management and updating. Due to this, such devices are referred to as non-IP, and according to the principle, these devices cannot directly use the addressed IP network by the service platform that is running on remote servers. For securing the non-IP based IoT devices, architecture is considered that make the use of a mediator in the network. This mediator represents all the IP terminals that are inside the network to allow the applications which are running on the service application platform, to provide communication and addressing with them as if considering them as IP devices. The mediator uses the secure connection to communicate through being places at one hop along with the non-IP devices. Non-IP based IoT devices are used to communicate with the gateways by the standard protocol which is, in general, cannot adopt the IP stack to communicate with the gateway, and therefore these non-IP devices are represented over the network using the mediator.

Bluetooth based IoT Applications

With the Internet of Things getting popular and making the homes smarter by the wireless technologies, Bluetooth low energy (BLE) is becoming [9] an essential technology for using the IoT in small devices with low power, and low cost. This BLE is being used for a number of devices and portable medical devices by the healthcare industry.

The BLE or the Bluetooth 4.0 is implemented using an entirely new protocol stack with the help of new applications and profiles, and its core objective is to run on a coin-cell battery for a very long time. Using the BLE, it enables the devices to connect to the internet in an efficient way using the client-server architecture.

The Bluetooth Low Energy is operated using 40 channels in the 2.4 GHz ISM band consisting a space of 2MHz and can transmit at a rate of 1 Mbit/s with the help of GFSK modulation. In addition, it makes use of frequency hopping like the classic Bluetooth but uses the adaptive frequency hopping at a slow rate. The BLE from among the 40 channels uses only 3 to advertise that is used for the device discovery and after the device is connected and discovered, uses the remaining channels (37 channels) for data transmission.

Master device mode, advertising mode, slave device mode and scanning mode are the four primary modes with the help of which the BLE device operates. Among these four modes, the device uses the advertising mode for advertising period information to establish a link and to respond to another device that makes additional queries. Further, the BLE Data packet uses 8-bit preamble with 32-bit access codes, which are defined using the radio frequency channel and a variable PDU (Protocol data unit) which ranges from 2 to 39 bytes and 24 bit CRC. This provides the information that the transmission time ranges from 80 µs to 0.3ms and the advertise packets consist of the protocol data unit which contains up to 31 bytes of data and 16-bit header. In addition, the device, which starts in the advertising mode, is assumed as the slave device mode, and similarly, the scanning mode is assumed as the master device mode.

Embedded Systems

Embedded systems are integrated into the IoT network using the existing IoT architecture that is of two existing technologies namely UID (ubiquitous ID) architecture and ConstrainedApplicationProtocol (CoAP). With the help of the existing IoT network architecture, a new software framework is created which appends the functionalities of IoT on of the existing embedded systems. This framework provides consistent, intuitive and easy to use API that is used by the programmers of the embedded systems to reduce the cost of added IoT functionalities to the products [15].

Various Wireless Communications Used

Among the various wireless communications, Wi-Fi is considered as the most powerful technique for indoor localization based on its signal strength. The radios primarily used for the communication through Wi-Fi are considered similar to the radios of the walkie-talkie and other devices, and such wireless communication that can help in transmitting the frequencies of 5GHz or 2.4 GHz[17]. The wireless communication GPRS is an established technology considered better than the other mobile technologies, and because of this, the coverage of GPRS is higher than its other counterparts, and the vast majority of the areas are monitored for gaining precision where the 3G/4G is not always available [18]. The wireless packet based communication is known as GPRS, which is designed for replacing the switched service that is available on the second generation for the mobile communications and TDMA networks using a packet of data from various terminals across different channels in the systems and making efficient usage of the bandwidth available.

Various Applications

The IoT system can be utilized in numerous organizations [10], which includes education systems, Bus Stands, Railway stations, and Airports. These help on displaying the information and provides the notifications. The areas where the IoT services can be seen are explained below:

Smart Cities

- IoT helps in monitoring the parking slots in the urban areas. It also monitors the vehicles and their pedestrian levels, which helps in optimizing the driving.
- It detects the Android devices, iPhones, and all the smart devices, which has the Bluetooth as well as the Wi-Fi interfaces.
- The IoT is used in detecting the garbage levels within the containers. This further helps in optimizing the trash collection routes.
- IoT also predicts the traffic jams on the Highways with the warning messages. These vary as per the climatic conditions.

Smart Agriculture

- The moisture of the soil, as well as the crops in the yards, can be monitored with the help of IoT. This helps in controlling the total amount of sugar in the grapevines and grapes.
- The selective irrigation can be performed in the dry zones with the help of IoT, which further helps in reducing the water resources required.
- The overall study of the weather forecasting conditions helps in getting the information related to the rain, snow, drought and the wind changes.

Medical field

- IoT helps in monitoring and controlling the various conditions inside the freezers, which stores medicines, organic elements,and other medical products.
- It is used in measuring the ultraviolet radiations. This helps in generating the warning for the people.

Home Automation

- The IoT can be used in homes for remotely monitoring and managing the home appliances. This helps in reducing the monthly bills.
- It automatically switches on and off the remote appliances, which help in avoiding accidents and saving energy.

IV. Challenges

Various challenges, which are related to the technology, include security, privacy, and interoperability of the IoT devices are explained below:

Security: All the IoT devices are connected to the network, and they are most likely to be vulnerable. The security seems to be the dominant part in case ofthe safety of the IoT connected devices. Hence, the security is the major challenge for the IoT.

Privacy: The IoT devices help in collecting data from homes, streets, and data related to people. These data must be having the privacy issues. The data shared by the users is of the confidential nature. Therefore, the privacy of the data must be the major part in IoT. It must be addressed as it is connected directly to the personal data of the individual.

Interoperability: In the interoperable nature, the IoT devices are connected, and they exchange information with the help of sensors. There should be proper standardization for all the IoT system providers such that the device can be connected easily and the information can be exchanged.

V. Future Scope

With the development in the technologies, there are many more areas where the IoT can be used to optimize the services and to collect informative data for many purposes. Some of the things that can be considered in future work include the following [16]:

1. The connection of more devices to IoT can be made using the Arduino and required modules to operate the devices through mobile phones. These devices can be home appliances or related devices. To achieve this, Arduino can be used that provides the capabilities to integrate the hardware with a software program to manipulate the devices. Using both IP and non IP based networks.

2. IoT will be of the main focus of researchers in the coming years after the announcement of Microsoft to invest $5 billion globally for the Internet of Things. The major areas that will be focused include automobile sector, prediction in manufacturing industries, agriculture, IoT based street lightning, a measure of water quality and many more areas as well [22].

3. Management of the IoT devices is required to access the network for which the network should support the plug and play mechanism for the devices. Moreover, the users should not configure the IoT devices manually, and such devices should be automatically configured and to make use of this feature, the plug and play mechanism is a necessity for the IoT networks.

4. Connection management is required as the different device may contain various communication protocol and this connection management support various standards for the nodes belonging to the user.

VI. CONCLUSION

IoT becomes an important part of the network and is facilitating many users to provide a number of services. In this paper, various technologies of the IoT and previous researches based on that were reviewed. This paper also discussed the various challenges and future work based on the IoT devices and its improvements. With the increase in the technological advancements, it is required to connect number of devices with the internet to collect accurate and relevant information that can further help in various decision making based on collected data.Data security is considered as a crucial issue in the area ofinformation sharing, and the confidentiality of the data related to IoT may not disclose because of the data, like containing humidity, temperature, and others. However, the data security is essential to protect the data from malicious attackers and hackers.Along with providing more security features, Advancement in home automation can be further extended using IoT so that users can manipulate the electronic devices through mobile phones. This will provide huge benefits to the users who are not capable of frequently moving from one place to another due to some physical disability or to people who want to manipulate the devices from anywhere through the internet.

REFERENCES

1. Udoh, I. S., &Kotonya, G. (2018). Developing IoT applications: Challenges and frameworks. IET Cyber-Physical Systems: Theory & Applications, 3(2), 65-72. doi:10.1049/iet-cps.2017.0068.
2. Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., &Karliychuk, T. (2018). Smart IoT Devices in the Home: Security and Privacy Implications. IEEE Technology and Society Magazine, 37(2), 71-79. doi:10.1109/mts.2018.2826079
3. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2016). A Privacy-Preserving Communication Protocol for IoT Applications in Smart Homes. 2016 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI). doi:10.1109/iiki.2016.3
4. Patru, I., Carabas, M., Barbulescu, M., & Gheorghe, L. (2016). Smart home IoT system. 2016 15th RoEduNet Conference: Networking in Education and Research. doi:10.1109/roedunet.2016.7753232
5. Barbon, G., Margolis, M., Palumbo, F., Raimondi, F., &Weldin, N. (2016). Taking Arduino to the Internet of Things: The ASIP programming model. Computer Communications, 89-90, 128-140. doi:10.1016/j.comcom.2016.03.016
6. Hui, T. K., Sherratt, R. S., & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. Future Generation Computer Systems, 76, 358-369. doi:10.1016/j.future.2016.10.026
7. Saleem, K., Chaudhry, J., Orgun, M. A., & Al-Muhtadi, J. (2017). A bio-inspired secure IPv6 communication protocol for the Internet of Things. 2017 Eleventh International Conference on Sensing Technology (ICST). doi:10.1109/icsenst.2017.8304428
8. Giuliano, R., Mazzenga, F., Neri, A., &Vegni, A. M. (2014). Security Access Protocols in IoT Networks with Heterogenous Non-IP Terminals. 2014 IEEE International Conference on Distributed Computing in Sensor Systems. doi:10.1109/dcoss.2014.50
9. Collotta, M., & Pau, G. (2015). Bluetooth for the Internet of Things: A fuzzy approach to improve power management in smart homes. Computers & Electrical Engineering, 44, 137-152. doi:10.1016/j.compeleceng.2015.01.005
10. Sharma, V., & Tiwari, R. (2016). A review paper on "IOT" & Its Smart Applications. International Journal of Science, Engineering, and Technology Research (IJSETR), 5(2), 472-476.
11. Spano, E., Pascoli, S. D., &Iannaccone, G. (2013). An intragrid implementation embedded in an Internet of Things platform. 2013 IEEE 18th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). doi:10.1109/camad.2013.6708104
12. Al-Shargabi, B., &Sabri, O. (2017). Internet of Things: An exploratory study of opportunities and challenges. 2017 International Conference on Engineering & MIS (ICEMIS). doi:10.1109/icemis.2017.8273047
13. M., K., M., S., &Banakar, R. (2015). Evolution of IoT in smart vehicles: An overview. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). doi:10.1109/icgciot.2015.7380573
14. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of the Internet of things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 5, 484-487.
15. Lee, S., Bae, M., & Kim, H. (2017). Future of IoT Networks: A Survey. Applied Sciences, 7(10), 1072. doi:10.3390/app7101072

16. Yashiro, T., Kobayashi, S., Koshizuka, N., &Sakamura, K. (2013). An Internet of Things (IoT) architecture for embedded appliances. 2013 IEEE Region 10 Humanitarian Technology Conference. doi:10.1109/r10-htc.2013.6669062
17. Chen, Z., Zou, H., Jiang, H., Zhu, Q., Soh, Y., &Xie, L. (2015). Fusion of WiFi, Smartphone Sensors, and Landmarks Using the Kalman Filter for Indoor Localization. Sensors, 15(1), 715-732. doi:10.3390/s150100715
18. Navarro-Hellín, H., Torres-Sánchez, R., Soto-Valles, F., Albaladejo-Pérez, C., López-Riquelme, J., & Domingo-Miguel, R. (2015). A wireless sensors architecture for efficient irrigation water management. Agricultural Water Management, 151, 64-74. doi:10.1016/j.agwat.2014.10.022
19. Soursos, S., Zarko, I. P., Zwickl, P., Gojmerac, I., Bianchi, G., &Carrozzo, G. (2016). Towards the cross-domain interoperability of IoT platforms. 2016 European Conference on Networks and Communications (EuCNC). doi:10.1109/eucnc.2016.7561070
20. LeHong H. and Fenn J. (2012, September 18). Key Trends to Watch in Gartner 2012 Emerging Technologies Hype Cycle.https://www.forbes.com/sites/gartnergroup/2012/09/18/key-trends-to-watch-in-gartner-2012-emerging-technologies-hype-cycle-2/#26afb6477036 last Accessed 24 July, 2018
21. Statista. (2016). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ last Accessed 24 July, 2018.
22. SwapnilJaiswal. (2018,5). Microsoft will invest $5 billion in IoT over the next 4 years globally – Microsoft News Center India.https://news.microsoft.com/en-in/microsoft-will-invest-5-billion-in-iot-over-the-next-4-years-globally/ Last Accessed 24 July, 2018