Computing, Information Systems & Development Informatics Journal
Vol. 13 No. 1, March 2022 - www.cisdijournal.net

Internet of Things: Technologies, Applications and Challenges

[1]Abdulsalami B.A., [2]Atoba M. A., [3]Murainah A.O. & [4]Bello J.
[1,2,3,4]Department of Mathematical and Computer Science
Fountain University
Osogbo, Osun State, Nigeria.
E-mails: abdulsalami.baseerat@fuo.edu.ng., atobamubaraq@gmail.com.

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 make a diverse number 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, as it represents an enabler of new communication possibilities between people and things. The main aim of this study is to investigate the applications of IoT, its related technologies, and associated challenges. This study explains the concept of IoT, and defines and summarizes its main technologies and uses, offering a next-generation protocol as a solution to IoT challenges. The key features required for employing a large-scale IoT, and its challenges are revealed, to enhance research and development in this field.

Keywords*:* Bluetooth, GPRS, Internet of Things, IoT, RFID, Sensors, Wi-Fi, ZigBee, Actuators, Fog computing

CISDI Journal Reference Format
Abdulsalami B.A., Atoba M. A., Murainah A.O. & Bello J. (2022): Internet of Things: Technologies, Applications and Challenges Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 1, Pp 43-50
Available online at www.isteams.net/cisdijournal
dx.doi.org/1022624/AIMS/CISDI/V13N1P5

1. INTRODUCTION

The Internet of Things (IoT) is an emerging field of data communication. It is a network of interconnected gadgets connected to the internet to transfer and receive data from one to the other. It is known to be a system of interconnected objects which are embedded with sensors, software, and control systems. According to Atzori *et al*., (2010), it is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The sensors use various types of wireless technologies such as Radio-Frequency Identification (RFID), Wi-Fi, Bluetooth, General Packet Radio Service (GPRS), and ZigBee.

In recent times, IoT technology has turned out to be a significant boon for individuals and businesses, because it enables the autonomous exchange of useful information between different uniquely identifiable real-world devices that are invisibly embedded around us. Until recently, internet access was confined to devices like desktops, tablets, and smartphones but now, with IoT technology, virtually any equipment can be connected to the internet and monitored remotely. IoT is on the verge of reshaping the current form of the internet into a modified and integrated version due to its limitless imagination. The number of devices that use the internet is growing daily, and having all of them connected via wired or wireless medium will provide people with a powerful source of information at their fingertips.

Some of the important applications of IoT include smart healthcare systems, agriculture, education, traffic management, spatiotemporal predicting energy, Water quality analytics, bee colony status monitoring, waste management and monitoring, grid, transportation, etc. These are shown in Figure 1. Several types of research are currently being studied on IoT technologies in order to sustain their importance in platform development.

Figure 1: Application areas of IoT
(Source: Mishra, 2021)

2. ARCHITECTURE OF IoT

According to Sethi & Sarangi, (2017), different IoT architectures have been proposed by different researchers. A three-key level architecture was first described, followed by a four-key level architecture, then a five-layered architecture based on Transmission Control Protocol or Internet protocol (TCP/IP), and Telecommunication Management Network (TMN) was proposed, and finally, a six-layered architecture based on the network hierarchical structure However, there is no single consensus on architecture for IoT, which is agreed universally (Sethi & Sarangi, 2017). Below is Figure 2 showing the six layers architecture.

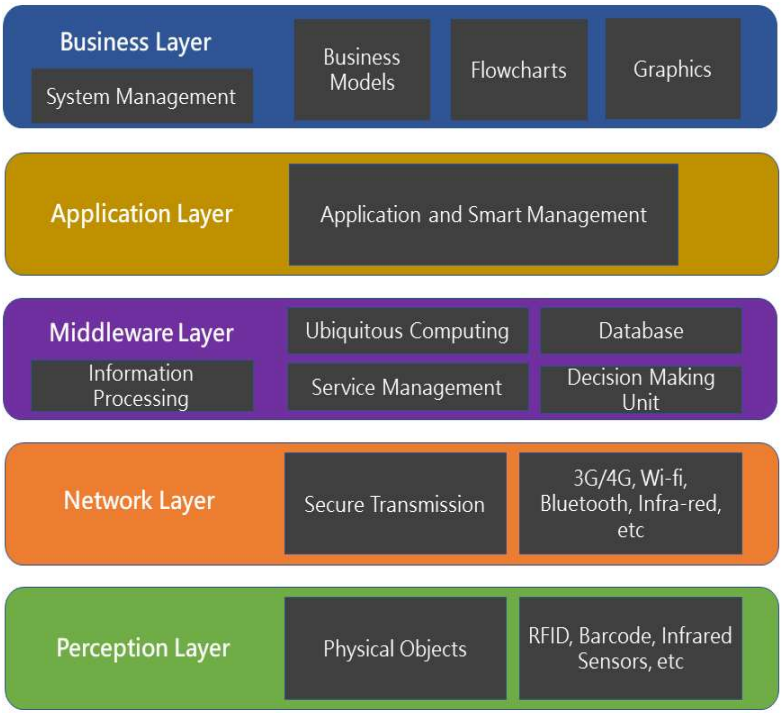

Figure 2: IoT Layered Architecture
(Source: dos Santos & Canedo, 2019**)**

Coding layer: According to dos Santos & Canedo, (2019) and Dhoot (2020), this layer is the foundation of IoT technology. It is the coding layer that allows the objects of interest to be identified. Each object is given a unique identification (ID) in this layer, making it easy to distinguish between them (Dhoot, 2020).

Perception layer: This is the IoT device layer, which gives each object a physical meaning. It is made up of data sensors in various forms, such as RFID tags, infrared sensors, and other sensor networks which could detect the objects' temperature, humidity, speed, and location, among other things. This layer collects useful information about objects from the sensor devices that are connected to them and converts the information into digital signals, which are then sent to the Network Layer to be processed further (Bansal & Rana, 2017).

Network layer: This layer's job is to receive useful information from the Perception Layer in the form of digital signals and transmit it to the middleware Layer's processing systems, via transmission mediums such as Wi-Fi, Bluetooth, WiMaX, Zigbee, Global system of mobile communication (GSM), 3G, and protocols such as IPv4, IPv6, MQTT, and DDS (Bansal & Rana, 2017).

Middle layer: The data from the sensor devices are processed by this layer. Cloud computing, for example, is one of the technologies included. Ubiquitous computing ensures direct access to the database, allowing it to store all necessary data. The information is processed with the help of intelligent processing equipment, and a fully automated action is taken based on the information's processed results (Bansal & Rana, 2017).

Application layer: Based on the processed data, this layer realizes IoT applications for all types of industries. Because applications promote IoT development, this layer is extremely beneficial in the large-scale development of IoT networks. Smart homes, smart transportation, smart planet, and other IoT-related applications are possible (Dhoot, 2020).

Business layer: This layer is in charge of managing IoT applications and services, as well as all IoT research. It provides many business models that can be used to develop efficient business strategies (Dhoot, 2020).

3. IoT TECHNOLOGIES

Many new and existing technologies are associated with IoT which are responsible for the connection of several subsystems, and enable them to operate under a controlled and unified platform that is managed smartly. It entails, in addition to advanced computer and communication network technology, an external communication network, many new IoT supporting technologies, such as collecting information technology, remote communication technology, remote information transmission technology, sea measures information intelligence analyses and controlling technology, and so on, which are still being developed (Siraj *et al*., 2017). Some of these technologies are described in the section below.

a. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is one of the technologies that allows objects to be uniquely identified. It's a form of transmitter microchip that looks like an adhesive sticker and can be active or passive depending on the application. Active tags have a battery attached to them, which keeps them active all of the time and allows them to continuously produce data signals, whereas passive tags are only active when they are triggered. The RFID system is made up of readers and RFID tags that emit information such as identity and position, or any other information about the object when triggered by the development of a suitable signal. The produced object-related data signals are sent to the Readers through radio frequencies where they are later analyzed by the processors.

b. Wireless Sensor Network (WSN)

A wireless sensor network (WSN) is a network of spatially distributed autonomous devices that use sensors to collaboratively monitor physical or environmental variables, temperature, sound, vibration, pressure, motion, or pollution, for example, in various sites (Alcaraz *et al*., 2018). A WSN is a key component of the IoT paradigm (Siraj *et al*., 2017; Alcaraz *et al*., 2018). There are vast number of sensors available for example, sensors can be attached to a patient's body to track how the patient reacts to the medication, allowing doctors to assess the medication's effectiveness.

c. Cloud Computing

Cloud computing is a type of intelligent computing in which a large number of servers are consolidated onto a single cloud platform to enable sharing of resources that may be accessed at any point in time and from any location. Both Cloud computing and IoT have seen a rapid and independent evolution, and both of their characteristics are often complementary. According to Farooq *et al*., (2015), the cloud appears to be the only technology capable of adequately analyzing and storing all of the data. IoT has benefited from the virtually unlimited capabilities and resources of the cloud in terms of storage, processing, and communication. Cloud can offer an effective and efficient solution for IoT service management, and for implementing applications and services that exploit the things or the data produced by them. It facilitates IoT application by enabling the collection and processing of these data, in addition to rapid setup and integration of new things, while maintaining low costs for deployment and for complex data processing (Khan & Sawant, 2016). On the other hand, the cloud can also benefit from IoT by extending its scope and services to real-world things in a more distributed and dynamic manner (Sayed *et al*., 2017).

d. Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to the science of building machines that imitates human intelligence. AI-based systems are evolving, and machines are increasingly becoming capable of performing human-related tasks. Integrating AI into IoT will enable more efficient IoT operations, improve human-machine interactions, and enhance data management and analytics. For example, implementing AI algorithms and data analytics techniques can help transform IoT data into useful information for improved decision-making. Machines can become smarter over time and decision-making can be refined to increase accuracy. This development will in turn accelerate the digital transformation of businesses and industrial organizations, and enable them to make smarter decisions, thus making the world an autonomous place.

e. Optical Technologies

Optical technologies such as optical communication systems, Light Fidelity (Li-Fi), and Cisco's Bi-Directional (BiDi) optical technology already play a significant role in modern networks, and are still evolving to meet up with the requirements of modern applications. Li-Fi, a game-changing visible light communication (VLC) technology, offers excellent connectivity on a higher bandwidth for things interconnected under the IoT concept while Bi-Directional (BiDi) technology, on the other hand, provides a 40G ethernet for huge data from a variety of IoT devices (Bansal & Rana, 2017). Optical technologies have the potential to greatly help in realizing future smart infrastructures and systems. Hence, they could represent a huge step forward in the development of a global, high-performance, and highly reliable IoT. According to Aleksic, (2020), optical technologies provide fundamental components and functions at both device and network layers of the IoT layered model such as a variety of practical sensor implementations, and high-performance communication and network capabilities.

f. Nano Technologies

Nanotechnology is science, engineering, and technology conducted at the nanoscale, which is about 1 to 100 nanometres (National Nanotechnology Initiative). Nanotechnology allows for the creation of smaller and better versions of interconnected objects. It can reduce a system's consumption by enabling the development of nanometer-scale devices that can function as sensors and actuators in the same way that conventional devices do (Rajinder, 2017). Nanotechnology intersects with IoT systems in different ways, from the manufacturing of reliable sensors that form an IoT system to the nano-processors that compute and process data collected by IoT sensors. There is an explosion of data resulting from IoT systems, from consumer level to industrial and commercial levels, massive amounts of IoT data are often created by interconnected nanodevices. Nanotechnology can also be used to create powerful processors and supercomputers that collect, analyse and report on the data IoT devices create.

Integrating nanotechnology into IoT will also impact IoT systems. According to the National Nanotechnology Initiative, Nanotechnology will revolutionize the IoT. It can improve IoT in the areas of data accuracy, sustainability of less power consumption and carbon emission reduction, affordability of IoT technologies, improve battery energy efficiencies, among others benefits.

g. Actuators

An actuator is a device that turns energy into motion, hence they are used to drive motions in mechanical systems (Madakam *et al*., 2015). It requires hydraulic fluid, electricity, or some other form of power. A linear motion, rotational motion, or oscillatory motion can be created using actuators. Cover short distances of up to 30 feet and communicate at speeds of less than 1 Mbps (Madakam *et al.,* 2015). Actuators are commonly utilized in manufacturing and industrial settings. According to Madakam *et al*., (2015), there are three categories of actuators which are widely used nowadays. Electric actuators are the most prevalent type among them. Hydraulic and pneumatic systems allow smaller motors to produce more force and torque.

h. Big Data Analytics

In recent times, the number of devices and sensors in networks have increased in the physical environments due to the explosion of the Internet which has also led to the rapid expansion of the networks. This will lead to significant change in the information communication networks, services and applications in various domains (Sayed *et al*., 2017). Large volumes of heterogenous data are being generated from many IoT applications and services, and are stored on big data systems on a large scale. These sensory data when collected can be analyzed and turned into real information to give us a better understanding about our physical world and to create more valuable products and services. These IoT produced data strongly depends on the 3V's factor of big data, which are volume, velocity and variety. Big data advanced tools like Hadoop, Spark, etc. are also employed in interpreting and examining the accumulated IoT data.

4. APPLICATIONS OF IoT

Below are some of the different application areas where IoT is growing its roots.

a. Healthcare

The importance of healthcare in one's life cannot be overemphasized. People especially in a densely populated area lack access to quality healthcare. IoT has the capabilities to alleviate strain on healthcare systems. Different sensors are mounted on the patient's body, and the data obtained can be sent to nearby or far away doctors. Through consultation, patients received treatments and are healed. This could be stored in the cloud for prospective use. According to Goel *et al*., (2021), IoT can be used for a variety of medical applications, such as workout routines, real-time health monitoring, and aged care. Hence, it is critical to research the current status in IoT-based healthcare systems and review relevant research questions that need to be addressed in order to advance IoT in healthcare.

b. Smart Cities

A smart city is an urban system that makes infrastructure more interactive, accessible, and efficient by making use of information and communication technology (Goel *et al*., 2021). The smart city contains smart devices with IoT technology such as surveillance camera, smart water distribution, smart healthcare systems, automated transportation, smart energy management, etc., and this technology is able to solve issues like shortage of water and energy supplies, traffic jams, pollution, ad other major problems faced by human. According to Sayed *et al*., (2017), implementing smart cities require careful planning in every stage, with support of agreement from governments and citizens. By IoT technologies, cities can be improved at many levels, making human life easier, safer and smart.

c. Agriculture

Agriculture is vital to our well-being. With continuous and significant increase in population, the demand for food is increasing tremendously. With IoT, a smart agriculture can be achieved by using sensors networks, and scientific research databases. With this development, growing of plants and other agriculture productions needed by humans like fruits and vegetables can be monitored. IoT could also revolutionize the way farmers work. Their production processes based on managing many resources such as weather, water and sunlight etc. can be stored in the cloud for prospective use (Sayed *et al*., 2017). This in turn provides data and insight to farmers on how they can yield a better return on investment. Several types of sensors can be used to examine various critical elements associated with farming, such as sensing for soil moisture and nutrients, and controlling water usage for plant growth. These data can be used to make improvements.

d. Industry Automation

Nowadays, one of the most developed technologies is the industries and manufacturing revolution. Industrial internet termed as Industrial Internet of things (IIoT) is a new buzz in the industrial sector where intelligent machines are packed with different sensors, software and big data analytics to make them smarter. These sensors and software collect data and IoT interpret these data making the machines smarter and accurate. This makes it communicates easily with humans.

e. Smart Vehicles

The vehicles in this implementation area are equipped with sensors that allow communication with several other devices inside the vehicle, as well as with other similar vehicles and fixed infrastructure. A new paradigm, V2X (vehicle to everything), is introduced, designed primarily for highly mobile devices, wherein a vehicle is connected to everything. The vehicles that are interconnected and share a variety of data are referred to as a Vehicular Ad hoc network (VANET) based on Dedicated Short-range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE).

f. Smart Homes

In smart homes, multiple gadgets are seamlessly integrated via wired and wireless technologies, resulting in a highly personalized and safe home environment. Smart appliances, smart meters, and home electricity generation are all essential components of a smart house. The home area network (HAN) is a network within a home that allows for remote access and control of equipment and systems.

g. Activity Monitoring

Human physical activities can be tracked by placing wearable sensors. It is very beneficial in terms of enhancing the quality of care and protecting humanity. It is also successful in providing continuous monitoring support. Various sensors like accelerometer, Gyroscope, GPS, Cameras, etc. can be utilized to attain activity monitoring.

h. Smart Grids

As per the definition given by NIST, a Smart grid is a modernized grid that uses two-way communication and control capabilities to enable a bidirectional flow of energy using leading to an array of new functionalities and applications. The deployment of smart grids enables load forecasting and self-healing. Different networks associated with smart grids are HAN, Neighborhood Area Network (NAN), Wide Area Network (WAN), IP network, Sensor and Actuator Network (SANET).

5. CHALLENGES OF IoT

As previously described, the implementation of an IoT application necessitates the integration of a variety of information and communication technologies in the form of hardware and software. Some of the most significant challenges that IoT innovators are currently facing in this context include device-level energy supply, identification and addressing, Internet scalability, security and personal privacy, and standardization and harmonization. In terms of IoT platforms, the selection of an IoT platform will undoubtedly be the first significant challenge for companies providing connected products or product systems, as the respective market is young and highly fragmented.

The platform providers' ability to create active ecosystems around their platforms, and also provide professional and timely support to their partners and development communities, will undoubtedly be a key factor. Finally, supporting the most recent and constantly evolving standards, as well as integrating appropriate end-to-end toolchains even in the embedded software domain to improve developer productivity, are major challenges in the development of IoT platforms.

The following are some of the potential IoT-related issues:

i. **Unauthorized Access to RFID**
Unauthorized access to tags containing identification data is a major issue in IoT that can expose any type of sensitive information about the user and must be addressed (Farooq, 2015). Not only can a rogue reader read the tag, but it can also be modified or even destroyed. In this context, some of the real-world RFID threats are summarized, including RFID Virus, Side Channel attack with a cell phone, and SpeedPass Hack (Farooq, 2015).

ii. **Sensor-Nodes Security Breach**
WSNs are vulnerable to a variety of attacks because sensor nodes are part of a bi-directional sensor network, which means that in addition to transmitting data, they can also acquire data. Jamming, tampering, Sybil, Flooding, and other types of attacks are some of the potential attacks.

iii. **Cloud Computing Abuse**
Cloud Computing is a big network of converged servers which allow sharing of resources between each other (Aamir *et al.,* 2014). These shared resources are vulnerable to a variety of security concerns, including Man-in-the-middle (MITM) attacks, phishing, and so on (Aamir *et al.,* 2014), Measures must be taken to assure the clouding platform's complete security. The Cloud Security Alliance (CSA) proposed certain potential dangers, including malicious insider, data loss, account hijacking, and abnormal use of shared computers, among others.

6. FUTURE DIRECTIONS

As IoT technology enables devices to transmit information over a network to other local or remote devices, the privacy of data being transmitted cannot be compromised. To curb this menace, data should be stored and accessed by the authorized nodes only. As the number of devices being connected to internet is growing day by day, so a new addressing scheme should also be considered as this is an area where utmost care is needed to name and identify devices. The various and different technologies like RFID, IEEE 802.15.4, ZigBee, 6LoWPAN should be integrated together with other IoT technologies to enable them work together. For example, the time-sensitive data should be analyzed on a priority basis for faster decision making so the fog computing should be integrated in a more effective and efficient manner. A new research and novel paradigm for managing the huge big IoT data coming from the objects should be proposed.

7. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the concept of IoT will soon be inexorably developing on a very large scale. By embedding intelligence into the devices around us, this growing networking paradigm will influence every aspect of our lives, from automated homes to smart health and environment monitoring. Research is being conducted in order to broaden its use, but without solving the issues in its development and ensuring the user's privacy and security, it's quite unlikely that it will become an all-pervasive technology. It's quite unlikely that it will become an all-pervasive technology. The implementation of IoT necessitates concerted efforts to address and propose answers to its security and privacy issues.

REFERENCES

1. Alcaraz, C., Najera, P., Lopez, J., & Roman, R. (2018). *Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?*
2. Aleksic, S. (2020). *A Survey on Optical Technologies for IoT , Smart Industry , and Smart A Survey on Optical Technologies for IoT , Smart Industry , and Smart Infrastructures*. *September 2019*. https://doi.org/10.3390/jsan8030047
3. Aamir, M., Hong, X., Wagan, A.A. Tahir, M., & Asif, M. (2014). "Cloud Computing Security Challenges and their Compromised Attributes," in *International Journal of Scientific Engineering and Technology*, Volume 3, Issue 4, pp. 395-399
4. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/J.COMNET.2010.05.010
5. Bansal, B., & Rana, S. (2017). Internet of Things: Vision, Applications and Challenges. *International Journal of Engineering Trends and Technology*, *47*(7), 380–384. https://doi.org/10.14445/22315381/IJETT-V47P263
6. Dhoot, A. (2020). A Survey of Internet of Things. *SYNCHROINFO JOURNAL*, *6*(5), 25–32. https://doi.org/10.36724/2664-066X-2020-6-2-25-32
7. dos Santos, Y. L., & Canedo, E. D. (2019). On the Design and Implementation of an IoT based Architecture for Reading Ultra High Frequency Tags. *Information 2019, Vol. 10, Page 41*, *10*(2), 41. https://doi.org/10.3390/INFO10020041
8. Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A Review on Internet of Things (IoT). *International Journal of Computer Applications*, *113*(1).
9. Goel, S. S., Goel, A., Kumar, M., & Moltó, G. (2021). A review of Internet of Things: qualifying technologies and boundless horizon. *Journal of Reliable Intelligent Environments 2021 7:1*, *7*(1), 23–33. https://doi.org/10.1007/S40860-020-00127-W
10. Healthcare Paradigms in the Internet of Things Ecosystem. (2021). *Healthcare Paradigms in the Internet of Things Ecosystem*. https://doi.org/10.1016/C2019-0-00358-5. Accessed 12th, December, 2021.
11. Khan, I. & Sawant, S.D. (2016). A Review on Integration of Cloud Computing and Internet of Things. *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 5, Issue 4.
12. Madakam, S., Ramaswamy, R., Tripathi, S., Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, *3*(5), 164–173. https://doi.org/10.4236/JCC.2015.35021.
13. Mishra, N. (2021). *Internet of Things Applications , Security Challenges , Attacks , Intrusion Detection , and Future Visions : A Systematic Review*. 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408
14. Rajinder, T. (2017). An Overview of Internet of Things (IoT): From Literature Survey to Application Implementation Perspective. https://www.researchgate.net/publication/322083410_An_Overview_of_Internet_of_Things_IoT_From_Literature_Survey_to_Application_Implementation_Perspective.

15. Sayed, E., Ahmed, A., & Kamal, Z. (2017). *Internet of Things Applications , Challenges and Related Future Technologies*. *January*.
16. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2017/9324035
17. Siraj, S., Janhavi, M., & Scholar, P. G. (2017). A Survey on IoT: Identity Management in Internet of Things. *International Journal for Technological Research In Engineering*, *4*(9). www.ijtre.com