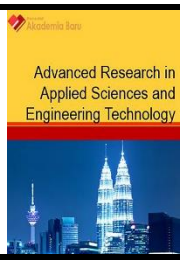
Penerbit Akademia Baru

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
www.akademiabaru.com/ submit/index.php/araset/index
ISSN: 2462-1943



The Internet of Things Vision: A Comprehensive Review of Architecture, Enabling Technologies, Adoption Challenges, Research Open Issues and Contemporary Applications

Rashidah Funke Olanrewaju[1], Burhan Ul Islam Khan[1,*], Aisha Hassan Abdalla Hashim[1], Khairul Azami Sidek[1], Zuhani Ismail Khan[2], Hamdan Daniyal[3]

[1] Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia
[2] Microwave Research Institute, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia
[3] Faculty of Electrical and Electronic Engineering Technology, Universiti Malaysia Pahang (UMP), Pekan, Pahang, Malaysia

ABSTRACT

With the improvements in machine-to-machine (M2M) communication, ubiquitous computing, and wireless sensor networks, the Internet of Things (IoT) has become a notion that is constantly rising in importance. Using uniquely addressable IDs, the Internet of Things links diverse physical items and allows them to communicate with one another through the Internet. A general overview of the IoT in the context of the architecture and associated technologies is provided in this article. On the other hand, the Internet of Things does not follow a standardised architecture model. This is accomplished by describing widely recognised architectural concepts that are subsequently refined with the associated technology in various tiers. Also included are some solutions that have been developed and future directions for addressing the obstacles faced by the IoT paradigm. Finally, the article discusses several Internet of Things applications to demonstrate the viability of the IoT idea in real-world settings.

Keywords:
Internet of Things, IoT Architecture, IoT Working, IoT Applications, IoT Challenges

Received: 21 February 2022 **Revised: 2 March 2022** **Accepted: 3 March 2022** **Published: 5 March 2022**

1. Introduction

The Internet of Things (IoT) is a novel paradigm that allows for the communication of sensors and electrical devices over the Internet to serve a better purpose. The IoT is a technology that uses smart devices and the Internet to bring ground-breaking solutions to several difficulties and challenges connected to a wide range of industries throughout the world, including consumers, industry, government, and public and private sectors [1]. The IoT is increasingly becoming an essential part of people's lives, and its presence can be seen everywhere. In general, the Internet of Things (IoT) is a technological innovation bringing together a huge variety of frameworks, smart systems, sensors and smart objects (Figure 1). Furthermore, it utilises nanotechnology and quantum in aspects of

* *Corresponding author.*
E-mail address: burhankhan@iium.edu.my

https://doi.org/10.37934/araset.26.1.5177

sensitivity, processing speed, and storage capabilities that were previously unimaginable [2]. Numerous studies have been undertaken. to illustrate the prospective use and application of IoT developments. The results are accessible in scholarly publications, press reports, and other written materials, both online and offline. It might be implemented as a preparation effort before developing fresh creative business ideas while contemplating interoperability, assurance and security.

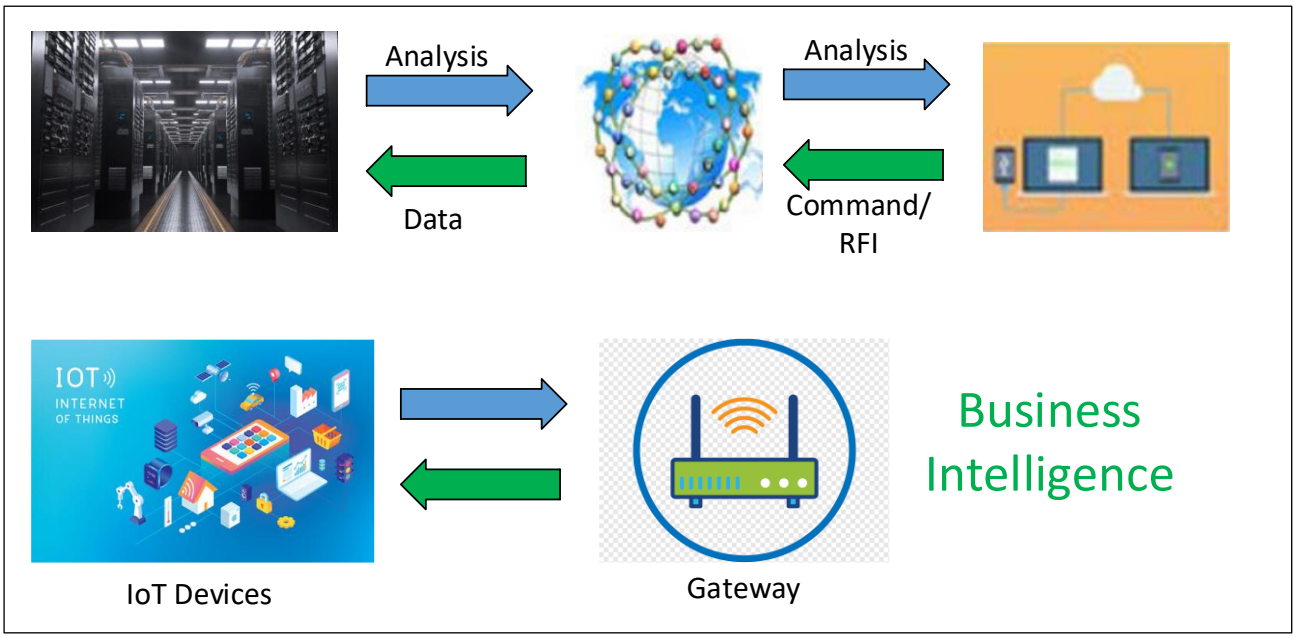


Fig. 1. General architecture of IoT

1.1 IoT Definition

The Internet of Things (IoT) has generated considerable attention in both the industrial and academic sectors, with the main motives for this interest stemming from the capabilities that IoT delivers [3]. It also ensures the establishment of a future in which all intelligent things and devices are interconnected and can interact with one another with the least amount of interference from humans [4]. The ultimate goal of IoT is to improve the lives of people by having all smart objects in our surroundings comprehend all we need and desire, and acting in our best interests without our direct orders [4-5]. The IoT encompasses many technologies that contribute to its vision, but research in this subject is still very much in its early phases. As a result, the term "Internet of Things" does not have a universal definition; instead, the following definitions have been supplied by various academics.

- Definition 1: Things have virtual identities and personalities, in which they are integrated with smart interfaces which facilitate interaction and connect with users' surroundings and social situations [6], and they can communicate and connect with one another.
- Definition 2: Things that are interconnected and play an essential part in what could be referred to as the "Internet of the future" [7].
- Definition 3: This term is made up of two words: The Internet is defined as a global network made of an extraordinarily diverse array of networks that operate according to established communication protocols; meanwhile, the term "Things" refers to every linked device that utilises the same communication protocols as the Internet [7].
- Definition 4: An IoT network's environment is composed of both real and virtual things, which transform into virtual things when they are placed inside a cyber world. Such objects can

sense, analyse, and process data and self-manage, relying on integrated specialised requirements and communication protocols. These smart things should have distinct virtual personalities and identities [8] and communicate through interoperable communication protocols.

- Definition 5: The Internet of Things (IoT) concept signifies "anything that can be reached from anywhere at any time by anyone for any service over any network". As a result, the Internet of Things can be referred to as 6Anys [9].

1.2 Internet of Things Future Vision

The IoT is still in its early phases of development, and numerous stakeholders may be involved depending on their usage and interests. It is still in its initial phases, and everyone is seeking to comprehend the Internet of Things from the perspective of their own requirements. The modern concept comprises a sensor-based collection of data, data administration, processing of data, and the World Wide Web, among other technical elements. It needs to be noted that sensor-based hardware is used. This concept, as defined by an introductory and broad definition [10-11], is defined as the wide usage around us of a range of objects or things (like sensors, actuators, Radio Frequency Identification (RFID) tags, mobile phones, etc.) that, through determines schemes, are capable of interfacing with each other working collaboratively with their neighbours to achieve a common goal. Figure 2 offers an overview of three specific concepts presented by [12]. These are their names:

- Things Oriented Vision
- Internet Oriented Vision
- Semantic Oriented Vision

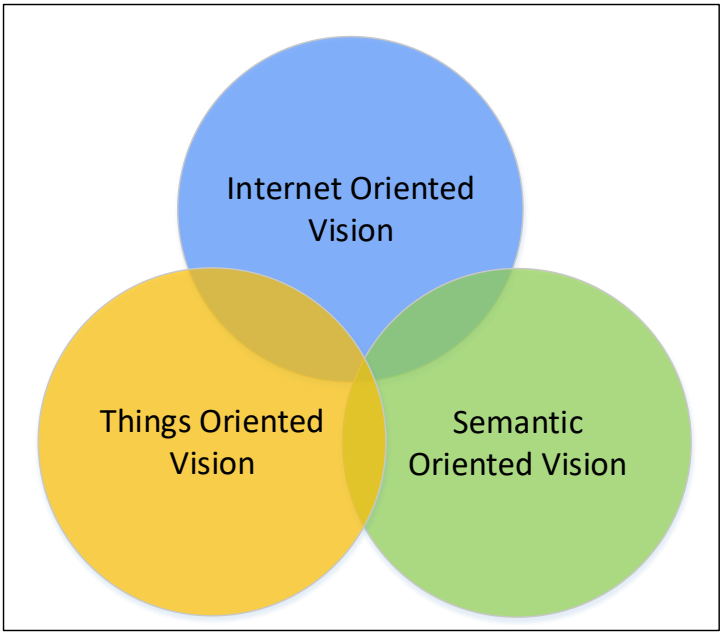


Fig. 2. Three major Internet of Things perspectives

1.2.1 Things oriented vision

The founding principle is the adoption of Electronic Product Code (EPC) regulations to identify the individual item. Sensors have been included in this strategy. It is crucial to remember that long-term vision will rely on sensors and their competencies to fulfil the "things"-oriented vision. Using sensors and sensor-type embedded systems, users can produce data on a large scale as a collective effort. Sensor networks and RFID-based sensor networks will be used to manage the collaboration of RFI-based technologies. We can produce data collectively using sensor-type embedded devices and sensors. In the future, sensor networks will integrate RFID-based technologies with high tech computing and sensing equipment, along with global connectivity.

This claim is supported by the fact that sensors and ubiquitous technologies like RFID [13] allow us to control everything.

1.2.2 Internet oriented vision

The Internet oriented vision has stressed the necessity for connected smart gadgets. Since IP is the most extensively used Internet protocol, the objects must contain IP protocol capabilities. The sensor-based devices or objects attributes can be tracked in real-time. This is the basis for embedded computing objects that are fundamentally microcomputers with computational power.

1.2.3 Semantic oriented vision

The realisation that we would have a large number of sensors and a huge amount of data collected by those sensors is the driving force behind this idea. As a result, we'll have a vast amount of data to sort through, most of which will duplicate previous data. Therefore, it is necessary to understand raw data to achieve better representations and comprehension of the information presented. Suppose we can convert data sets into heterogeneous and homogeneous forms. In that case, we will rely on technology to analyse the data, which will alleviate the interoperability problems associated with interpreting the data. In this case, a solid comprehension of raw data analysis is required.

2. Architecture of IoT

In the world of the Internet of Things, no one can agree on the best design. Different scholars have recommended various architectural designs.

2.1 Three- and Five-Layer Architectures

A three-layer architecture is the most basic form [14-15], as in Figure 3. In this field of study, it was first used during the preliminary stages of the investigation. The perception, network, and application layers comprise this system's three layers.

1) Perception layer: Sensors in the perception layer (also known as the physical layer) are responsible for gathering and interpreting data about the immediate environment. It identifies physical properties or intelligent objects in the surroundings.
2) Network layer: The network layer connects servers, smart objects, and network devices to the network. Its features are also employed in sensor data processing and transmission.

3) Application layer: The application layer offers users with application-specific services. For example, a smart home application can turn on a coffee maker by simply pressing a button.

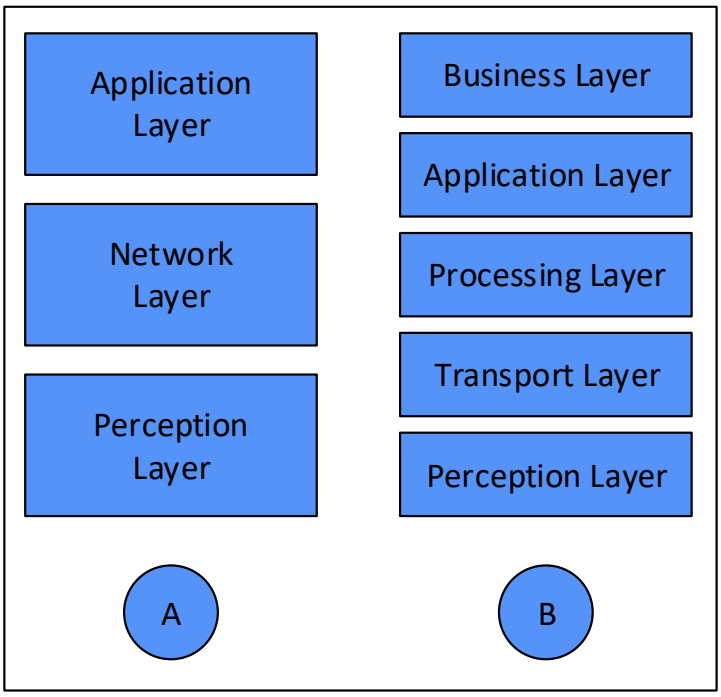


Fig. 3. Three layer Internet of Things architecture

The three-layer architecture illustrates the underlying concept of the Internet of Things; nevertheless, it is not appropriate for IoT research because most of it emphasizes on the more delicate components of the Internet of Things rather than on the general concept. Consequently, the literature has various innovative layered architectures. One such design is the five-layer architecture [14–16], including the business and processing levels. Layers 1 through 5 are "perception," "transport," "processing," "application," and "business." (see Figure 3). The perception and application layers function in the same way as the three-layered architecture does. We will go through the utility of the last three layers in detail.

1) The transport layer communicates sensor data between the processing and perception layers and conversely over networks like 3G, WiFi, RFID, Bluetooth, NFC, and Local Area Network (LAN).
2) Processing layers are also called "middleware layers" since they contain middleware functions. Thousands of gigabytes of data are processed, stored, and analysed by this layer connected to the Internet. It can administer and offer a broad collection of services to the bottom layers. It uses cloud computing, Big Data processing analysis module and databases.
3) The business layer is responsible for the overall management of the IoT system, including business, revenue models, privacy protection, and applications. In this paper, we will not discuss the business layer in detail. As a reason, we will not be discussing it further. Similarly, the processing level in the human brain is the inspiration for another design presented by Ning and Wang [17]. Much of it is inspired by the human mind and ability to feel and think, make judgments and recall, and respond to their external world. A total of three pieces comprises this structure. The first being the human brain, that may be compared to the data centre or data management and processing unit in terms of functionality. The second structure is the spinal cord, representing a dispersed network of smart gateways and data

processing nodes. Lastly, there is the network of nerves composed of components like sensors and networking.

2.2 Cloud and Fog Based Architectures

Cloud-Fog computing architectures are new frameworks designed to improve existing Internet of Things architectures (IoT) [18]. It is important to note that this classification differs from Section 2.1, which was based on protocol requirements.

We have been particularly ambiguous regarding the kind of data created by IoT devices and the data processing nature. Cloud computers may carry data processing out in an extensive, centralised manner depending on the system architecture. Cloud computing is placed at the centre in a cloud-centric architecture, with applications placed above it and a network of smart things underneath it. Part of the reason is the cloud's incredible flexibility and scalability. It offers services including the core infrastructure, the storage, the software, and the platform to its customers. Developers can make software, machine learning, storage, data mining, and visualisation tools available on the cloud.

Several researchers have recently proposed the use of fog computing [19-21], a system architecture wherein network gateways and sensors do some of the data processing and analysis. An example of a fog architecture [22] is presented in Figure 4, which uses a tiered approach to insert pre-processing, monitoring, security, and storage layers between the transport and physical levels, as illustrated in the diagram below. It monitors resource utilisation, response times, power usage, and service availability. This layer processes, filters, and analyses sensor data. The temporary storage layer handles dissemination of data, archiving, and replication. The security layer ensures data confidentiality and integrity in addition to decryption and encryption. Pre-processing and network edge monitoring are required prior to transferring data to the cloud.

The terms "edge computing" and "fog computing" are frequently employed alternatively in the same context. In contrast, the latter is considered more general. Cisco used the phrase fog computing to describe sensors and smart gateways; however, edge computing is more pervasive. Devices like pumps, lights, and motors might be equipped with smart data pre-processing capabilities. The goal is to pre-process data in these edge devices as much as feasible. The architectural diagram is similar to Figure 3 in terms of the arrangement in terms of system architecture. Consequently, we will not discuss edge computing in detail.

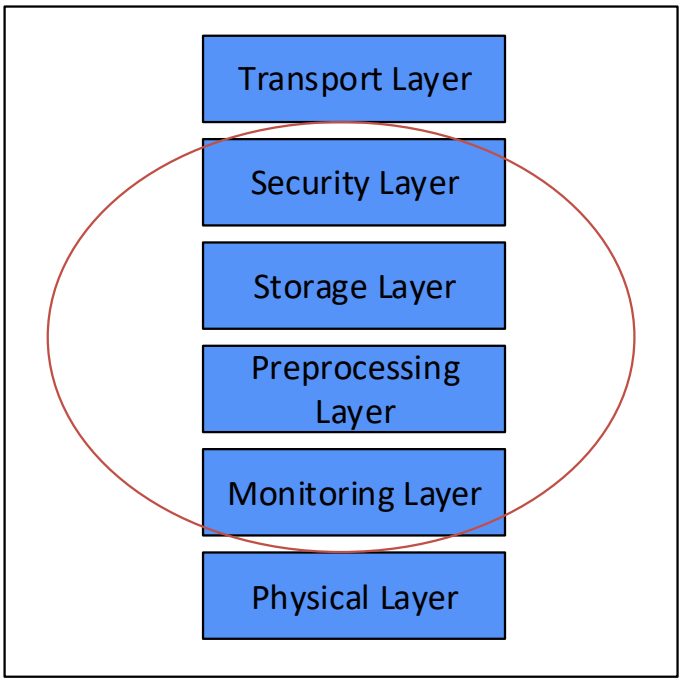


Fig. 4. Fog architecture of a smart IoT gateway

Finally, there isn't a clear boundary between protocol architectures and architectural system designs. Frequently, the system and the protocols are designed in tandem. Both for fog and cloud architectures, we will use the general 5-layer Internet of Things protocol stack (as depicted in the architectural schematic in Figure 3).

2.3 Social IoT

The IoT in a social context. Let us consider a new paradigm: the Social Internet of Things (SIoT). In this section, we analyse social ties among things in the same manner that humans create social relationships (see [23]). The following are the three most important aspects of a SIoT system:

It is feasible to navigate the Internet of Things. We might begin with one device and progress through all connected devices. Employing such an IoT device social network, it is easy to discover new services and devices.

A requirement for trustworthiness (the strength of the link) exists between gadgets analogous to Facebook friends.

To analyse the social networks of IoT devices, we can use models similar to those used for researching human social networks.

2.3.1 Basic components

We regard services and devices as bots in a standard social IoT scenario, which allows them to establish interactions between themselves and adjust those relationships over time. This will allow us to effortlessly integrate the gadgets and have them work together to complete a complex task. For a model to function correctly, it must have numerous interoperable components. Here are a few of the essential elements of such a system to consider:

- ID: We need a distinct way to identify objects. Any number of parameters can be used to assign an object an ID, including Media Access Control (MAC), universal product codes, IPv6, and others.

- Metainformation: We require metadata regarding the device's design and function in addition to an ID. To properly communicate with the item and place it within the IoT ecosystem.
- Security controls: Similar to Facebook's "friend list" options. A device's owner may restrict the devices that can join it. These are called owner controls.
- Service discovery: We require specialised directories to hold details about devices offering specific services like a service cloud. For devices to communicate, these directories must be kept current.
- Relationship management: This module handles network connectivity. It also keeps track of the devices to which a device should attempt to connect based on the services it provides. For example, if a light controller wishes to connect with a light sensor, this is quite reasonable.
- Service composition: This module elevates the social IoT paradigm. The purpose is to give users better integrated solutions. For instance, if a power sensor linked to an air conditioner connects to an analytics engine, the ensemble may provide a lot of data on the air conditioner's consumption trends. The ability to weigh data against the usage habits of other users and derive even more valuable information is made possible by a more extensive social model that includes more devices. Users may be alerted, among other things, that they are the most energy-intensive consumers in their neighbourhood, and possibly even among their Facebook friends.

2.3.2 Representative architecture

All proposed architectures for the Internet of Things include a server-side design. Because the server links to all associated components and combines (composes) the services, users can access it from any location.

There are three layers to the server-side architecture, on average. This is the first layer, which comprises a database of all devices, metainformation, relationships and their properties. The code on the second layer (the Component Layer) allows you to communicate with devices and provide a service. This is the topmost layer, and it is accountable for supplying services to the users.

In general, there are two levels on the device (object) side. A device can connect to other devices and communicate with them (using established protocols) through the object layer, which is the first of these layers. The object layer communicates with the social layer by passing information between the two. The social layer manages user apps, inquiries, and server-side application interaction.

3. Stages in the IoT Architecture

There are four key phases [24] in IoT architecture.

- Sensors and Actuators
- The advent of edge IT systems
- Internet Gateways
- Data Storage, Data Centres and Cloud

3.1 Sensors and Actuators

Sensors [25] are devices that collect data from the environment and provide it as analogue signals to the microcontroller to be processed. The sensors' main job is to convert data from the outside

world into something usable. Sensors must be used in the Internet of Things architecture to gather, analyse, and process information. It is possible to control physical reality with actuators. Among other things, they may be utilised to turn off and, on the lights, operate smart equipment, and alter the temperature of a space. Some Sensors are:

- Temperature Sensors: By its name, a temperature sensor measures the amount of heat energy present in the environment. This information can be utilised to detect climate changes that forecast the weather [26].
- Proximity Sensor: This sensor detects whether or not any tangible things are present in the vicinity of the sensor; if any of the devices or objects are located nearby the sensor, it indicates that object detected; otherwise, it indicates that the object not detected.
- Pressure Sensor: The presence of pressure is detected by this sensor, which then turns it into electrical energy [27].
- DHT11 Sensors: Temperature and humidity are measured with the help of these sensors. These sensors transmit the result displayed on the screen in digital format. It is equipped with an 8-bit microprocessor that creates serial data from temperature and humidity measurements and a Negative Temperature Coefficient (NTC) for temperature measurement.
- Ultrasonic Sensor: An ultrasonic sensor can determine the distance between two objects by using ultrasonic sound waves. Transducers are employed by ultrasonic sensors for sending and receiving ultrasonic pulses sent and received by the sensor.
- Infrared (IR) Sensors: Obstacle detection and transmission of an infrared signal are accomplished using an infrared sensor (also known as IR Sensor). It can detect and emit infrared radiation, making it a versatile device. In addition, this sensor can be utilised to build a robot that follows a blue line.
- Gas Sensor: A gas sensor detects the presence of gas in the surrounding environment. It is possible to detect oxygen, carbon dioxide, nitrogen, methane, and other gases with the help of this sensor.
- PIR Sensor: This sensor is responsible for detecting movement. These sensors are body detecting devices that identify the presence of humans and provide signals to the microcontroller, which then executes the appropriate operations.
- Water Quality Sensors: It is used to analyse water quality and measure the number of ions present in the water.
- Smoke Sensor: This is the most often used sensor for detecting smoke in the environment. As soon as smoke is detected in the surroundings, a signal is sent to the microcontroller, which, in turn, transmits a signal to the alarm system, resulting in the alarm system sounding.

3.2 The Advent of Edge IT System

The data prepared is delivered to the IT system using the IoT architecture. A more sophisticated method of pre-processing, visualising, and summarising the data is used in the IT system. This indicates that it has something to do with machine learning and visualisation technology. Before accessing the data centres, additional pre-processing is performed on the data. This stage is associated with the development of the IoT architecture, as were the previous phases, since the IT system is located extremely close to the actuators and sensors, making it necessary to create a wired network as close as possible.

3.3 Internet Gateways

Internet [28] gateways are software programs or hardware devices used to connect two devices, such as sensors, microcontrollers, smart devices, and the cloud when linking them together. The gateway sends all data generated by sensors or other smart devices to the cloud to be stored. The Internet gateway in the IoT is the conduit via which physical devices communicate with the cloud. The Internet gateway is indispensable to the operation of the Internet of Things, and as such, it is a critical component of the IoT architecture. Sensors can generate many data points per second; thus, the gateway helps pre-process the data nearby before transferring it to the cloud. The Internet gateway helps limit the quantity of data transferred to the cloud by evaluating, gathering, and summarising data at the edge. This is also responsible for network and data security.

3.4 Data Storage, Data Centres and Cloud

As the last step of the IoT architecture, it is essential to note that Deeper processing has been made possible by this. Professionals in the IoT and operational technologies are required. On the other hand, we may argue that this stage is associated with a greater level of analytical abilities available in digital as well as human realms. Consequently, a variety of data from various sources is available for in-depth investigation. It is now possible to return data to the physical world with the appearance that has been precisely evaluated and processed after all of the expectations and needs have been fulfilled.

4. Working of IoT

IoT comprises four components that work together to make IoT work.

1) Sensors: Sensors are devices that collect data from their surroundings. Sensors are present in numerous configurations (Proximity Sensors, Temperature Sensors, Gas Sensors, Light Sensors, etc.) These sensors are used in the construction of smart devices or systems such as tablets and smartphones, and they can also be used for predicting the weather and other intelligent applications. For example, smartphones make extensive use of sensors, so they are called smartphones.
2) Connectivity: A cloud-based storage system must store the data collected by sensors. Data storage in the cloud necessitates the creation of a channel from which the data is moved to the cloud. Consequently, either wirelessly or through the use of an Ethernet cable, the device must be connected directly to the Internet. A device connected to Bluetooth, satellite, WiFi, or a LAN can send data to the cloud, and this is known as cloud computing.
3) Data Processing: When the data has been uploaded to the cloud, the software can begin performing various operations and processing it. For example, this can determine whether the temperature is within a normal range or not. So, once the data has been uploaded to the cloud, it will be processed for the correct result to be viewed by the user or for the appropriate action.
4) User Interface: After all of the data has been processed, the final result will be provided to the user at this stage. This could happen if users are alerted via (text, notifications, email, etc.). For instance, if the temperature is too low, the user can receive a text message informing them that the temperature is too low, along with the temperature specifics. Users can also verify on the device via a user interface. The user interface is crucial when checking the temperature on a smartphone or online browser.

As a result, IoT devices such as sensors and smart gadgets collect data from their surroundings and interact with the cloud via numerous means. After the data is kept in the cloud, it is processed, and the final result is displayed using the user interface (email, text, notifications, etc.). This process is represented in Figure 5.

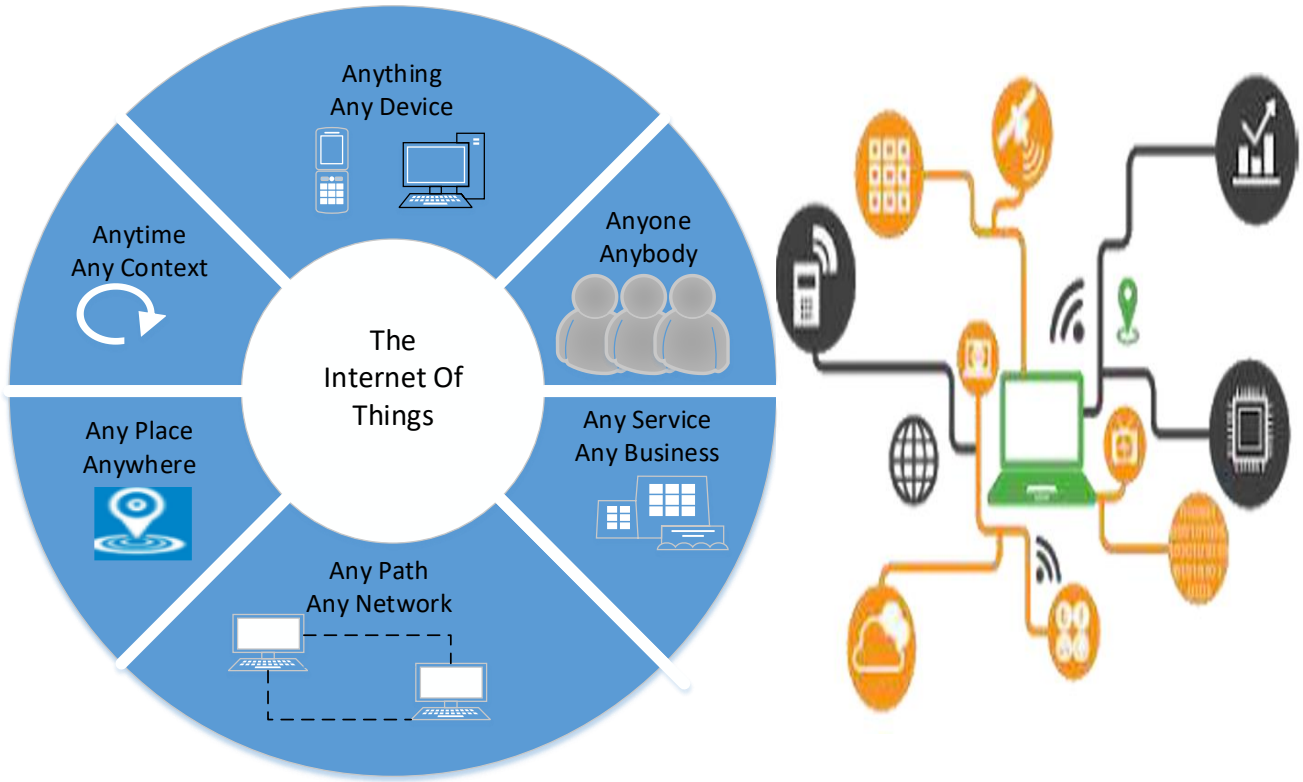


Fig. 5. Working of IoT [15]

5. Challenges and Technologies in Various Layers

As mentioned earlier, the IoT can be realised using various enabling technologies depending on the architecture. The four-layer Service-Oriented Architecture (SOA)-based Internet of Things architecture is given as an example in this section to show how the enabling technologies and difficulties at each layer are related.

5.1 Perception Layer

The primary function of the perception layer is to track and identify objects. The following technologies can be used to accomplish this goal:

5.1.1 Radio Frequency Identification (RFID)

RFID, a contactless communication system, tracks and identifies objects without physical contact. It allows for short-distance data transmission using radio signals [30-31]. The RFID-based system is comprised of three components: an antenna, an RFID reader, and an RFID tag [32]. A microchip attached to an antenna can be used to create an RFID tag. Each RFID tag is affixed to a certain object and has a unique identification number that can only be accessed by that object. By comparing the attached RFID tag with the right signals, an RFID reader may recognise an object and obtain the

essential information [34], which the reader transmits. The transmission of signals between an RFID reader and an RFID tag is accomplished by using an antenna. The following advantages of RFID are compared to those of other technologies [33-34]: Durability, fast scanning, noncontact reading, reusability, ample storage, low cost, security, small size, etc. As a result of these advantages, RFID can be used in the perception layer of the Internet of Things to track and identify objects and exchange information.

5.1.2 Wireless sensor networks

Wireless Sensor Networks (WSNs) have the potential to play a significant role in the Internet of Things [35-40]. WSNs can monitor and report on the status of devices, and send the information to a centralised hub or sink node across many hops [41-42]. As a result, WSN can be a new link between the real world and the cyber world [43]. WSN offers several advantages over other technologies, including low cost, dynamic reconfiguration, scalability, small size, reliability, and low energy consumption. These advantages contribute to WSN's ability to be integrated into various settings with various requirements. In the Internet of Things, both WSN and RFID can be used to collect data; the distinction is that RFID is primarily employed for object identification, whereas WSN is largely utilised for the interpretation of real-world physical qualities related with the external environment [44].

5.1.3 Others

A barcode, also known as a 1-D code, stores information that consists of many white spacings and black lines. Each of these lines and spacings is organised in a linear or 1-D direction, with different widths, and it is organised according to special encoding rules [45]. A device that scans the barcode with an infrared beam can read the information contained within the barcode [46].

A two-dimensional code uses black and white pixels spread out on a plane to store data. Each black pixel is a binary "1," while each white pixel is a binary "0." [47]. The black and white pixels on a computer screen can store a substantial amount of data encoded with special rules. A 2-D code has advantages over a barcode, including higher information content, excellent reliability, and increased ruggedness [44].

Further development is the RFID sensor network (RSN), a combination of a sensor network and an RFID system. When used in conjunction with an RFID system, a sensor network can be used to recognise and monitor the status of objects [48]. Small RFID-based sensing devices and an RFID reader are used to create an RSN, with the RFID reader acting as a sink node, generating data and supplying power to the network.

5.2 Network Layer

The network layer determines routing and supports data transfer across diverse networks. Several protocols for safe and dependable IoT communication are discussed below.

5.2.1 IEEE 802.15.4

IEEE 802.15.4 is a MAC and physical layer protocol for wireless personal area networks (WPANs) [49-50]. IEEE 802.15.4 focuses on low-rate WPANs, which allow low-rate connectivity for all devices in a private area also with low-cost and low energy consumption [51]. The IEEE 802.15.4 protocol

suite is centred on an Open System Interconnection module. Lower levels can serve top layers by implementing parts of transmission functions. IEEE 802.15.4 supports 2.4 GHz, 915 MHz, and 868 MHz bands with 250, 40, and 20 kB/s transmission rates [52]. Many wireless communication systems and protocols rely on IEEE 802.15.4, including ZigBee [53] and WirelessHART [54].

5.2.2 6LoWPAN

Low-power WPANs (LoWPANs) are made up of several low-cost devices connected wirelessly [44]. Compared to other networks, LoWPAN has a significant advantage (such as low bandwidth, small packet sizes, low-power consumption, and so on). This led to creating the 6LoWPAN protocol, which mixes IPv6 with LoWPAN. It is possible to transfer IPv6 packets across IEEE 802.15.4 networks by utilising the 6LoWPAN protocol [55]. Due to its less power consumption and inexpensive cost, 6LoWPAN is well suited for use in the Internet of Things, including many low-cost devices. In addition to having excellent compatibility and connectivity with legacy architectures, LoWPAN also has several advantages, such as ad hoc self-organisation, low energy consumption, and so on.

5.2.3 ZigBee

ZigBee is a low-power wireless network technology that was originally designed for short-range communication [56]. The ZigBee protocol is composed of five layers: physical, medium access control (MAC), transmission, network, and application [44]. In addition to low energy consumption and cost, ZigBee networks are also reliable and secure. The ZigBee network supports mesh, tree, and star topologies [57].

5.2.4 Z-Wave

Z-wave is a short-range wireless communication technique that offers the advantages of low cost, low energy consumption, and high reliability [56]. Reliable communication between a controller and one or more end devices is one of the primary goals of Z-wave, and it is particularly well suited for networks with limited available bandwidth. It is vital to note that a Z-wave network can support no more than 232 nodes (slaves) and that all nodes (slaves) would be monitored by the controller and would have routing capabilities [44][56]. Each slave in a Z-wave network has a route list stored in its memory, that is continually being updated by the controller [58].

5.2.5 Message Queue Telemetry Transport

Message Queue Telemetry Transport (MQTT) employs the publish/subscribe mechanism to collect data from distant sensors and send it to servers [48]. MQTT is a high-latency, low bandwidth protocol. It is also easy to implement. MQTT may be used on various platforms to link IoT devices to the Internet. The IoT will benefit significantly from MQTT's use as a message protocol between servers and sensors/actuators.

5.2.6 Constrained Application Protocol

The Constrained Application Protocol (CoAP) is a communications protocol based on the representational state transfer (REST) architecture [49][59], and [60]. It is not possible to use HTTP in IoT because of its complexity because the majority of devices in IoT have limited resources (i.e., limited computing capability and limited storage). CoAP was proposed to adapt specific HTTP

functionalities to fulfil IoT needs to solve this issue. In general, CoAP serves as the application layer protocol in the 6LoWPAN protocol stack, and it is designed to allow devices with limited resources to engage in RESTful interactions. For example, CoAP allows group communication and push notification but not broadcast communication. Additional characteristics provided by CoAP [61] include security, resource block-wise resource transmission, observation, resource discovery, and integration with the HTTP protocol, among others [61].

5.2.7 Extensible Messaging and Presence Protocol

It is built on XML streaming protocols [62] that the Extensible Messaging and Presence Protocol (XMPP) is used for instant messaging. Given that XMPP contains features of the XML protocol, it offers exceptional capabilities in scaling and addressing and security. Telepresence, audio and video streaming, and multiparty conversation are all possible with it. XMPP supports three roles: client, server, and gateway, with bidirectional interactive communication in each role. The server may handle links and messages while the gateway ensures stable connections across diverse systems. The client can connect to the server through TCP/IP and send the context via XML streaming. As a result, XMPP may provide object-to-object communication using XML-based text messages.

5.2.8 Data Distribution Service

To support high-performance device-to-device interaction, the Data Distribution Service (DDS) protocol, which is a publish/subscribe protocol, is used [63]. DDS is a data-centric protocol created by the object-management group [44]. It can support multicasting to achieve excellent service quality and dependability. Furthermore, DDS publish/subscribe architecture does not require a broker, making it suited for IoT applications with strict time constraints and device-to-device connections [49].

5.2.9 Advanced Message Queuing Protocol

Advanced Message Queuing Protocol (AMQP) is an open standard used to offer message service (routing, queuing, reliability, security, and so on) [49][64]. It is designed to function in message-oriented contexts and is a middleware protocol. The AMQP protocol allows clients to communicate reliably with message middleware, even if the clients and middleware are written in diverse languages. Apart from that, AMQP implements several different types of message-exchange architectures, such as the publish-and-subscribe models and store-and-forward, as well as message queuing, message distribution, point-to-point routing and context-based routing [65].

5.2.10 Others

There are a variety of protocols that can play essential roles in IoT, in addition to communication protocols, messaging protocols, and transmission protocols. [49][66] show that multicast Domain Name System (mDNS) may be utilised to provide name resolution in IoT applications. To identify needed services in a specific network, clients can employ DNS service discovery, which is performed through the usage of mDNS [49][67]. A link-independent routing protocol may be used to identify routes over lossy and low-power connections [49][68][69], among other things. These protocols can be integrated into the Internet of Things; however, more advanced protocols with higher security, interoperability, and reliability are essential to enhance the IoT development.

5.3. Service Layer

As previously mentioned, the service layer is positioned between the application layer and the network layer, and it is responsible for providing objects or applications with efficient and secure services. The service layer should contain service administration, interface, resource, middleware, and sharing technologies to guarantee effective service delivery.

5.3.1 Interface

Interactions between applications and devices require interface technologies at the service layer. The interface should also manage the devices linked to it, particularly device communication, device operation, device connection, and device disconnection [70]. It is possible to think of an interface profile (IFP) as a service standard for the IoT, as it may be used to make it easier for different applications and devices to interact. Play and Universal plug should be adopted to obtain an efficient IFP [70-71]. As the Internet of Things (IoT) has progressed, numerous efforts have improved the interface. For example, the SOCRADES integration architecture [72-73] might be employed to create effective interactions among services and applications [70][74]. As the development of SOA-IoT progresses, service provisioning processes have the capability of facilitating interactions with applications and services. Even though various interface technologies have been established for the Internet of Things, establishing more effective, scalable, and secure interface technologies at a cheap cost remains a significant problem in future research for supporting the IoT.

5.3.2 Service management

Service management can efficiently find applications and devices and plan efficient and dependable services to satisfy customer requirements dependably. A service can be thought of as behaviour that includes the storage, exchange, and collection of data or a combination of these behaviours used to accomplish a specific goal [75][76]. In the Internet of Things, some criteria can be addressed by a single service, while other requirements necessitate the integration of numerous services. As a result, services are classed as primary or secondary [70]. Application and primary device capabilities can be exposed through the primary service (also called the basic service). However, the secondary service might rely on the primary or secondary services to execute auxiliary functionality.

SOA has been used to integrate services to mask the implementation details of services and to ensure that these services may be deployed consistently across heterogeneous devices and applications. It is possible to ensure the dependability and consistency of services [78] and [70]. Examples include the OSGi platform created by a dynamic SOA architecture and is an effective modular platform for service deployment. To implement an SOA-based service, it is necessary first to establish service composition platforms, after which it is necessary to abstract away the functionality and communication capabilities of devices from them [70]. Lastly, a standard set of services should be available [71]. In a Service-Oriented Architecture (SOA), each service provided by an application or a device may be considered a standard service that can be used successfully and readily across a wide range of heterogeneous applications and devices without any modification. As a result, requirements in the SOA-based Internet of Things can be met more quickly and efficiently [70].

5.3.3 Middleware

Middleware is a service or software programming form that connects IoT technology and applications. Middleware abstracts away technology specifics and provides standard interfaces to develop applications rather than infrastructure compatibility [75]. Interoperability is made possible by the use of middleware between applications with different interfaces and devices.

The following are some of the advantages of using middleware [75]:

- Middleware is capable of facilitating the execution of a wide variety of applications.
- Middleware can run on a number of different operating systems and platforms.
- Middleware can facilitate distributed computing and service interaction across networks, devices, and applications.
- The middleware is capable of supporting standard protocols.
- Middleware may play an essential part in standardisation by providing standard interfaces and protocols that enable portability and interoperability.
- Middleware may also serve as a reliable high-level interface for programmes. Applications with reliable interfaces can run on any operating system or hardware. This attribute makes middleware suited for the Internet of Things since a large number of heterogeneous networks and devices are interconnected, and these networks and devices would be modified or updated regularly.

An extensive body of work has been done in the field of middleware, which may be split into five areas [78-79], which include semantic web-based middleware, message-oriented middleware, location-based service and surveillance middleware, pervasive middleware, and communication middleware. The reliable flow of information between communication protocols and diverse platforms (e.g., DDS, AMQP, XMPP, and MQTT) is crucial for message-oriented middleware [49][79]. A semantic web-based middleware platform can facilitate interoperability and interactions between different sensor networks. Task computing-based middleware [80], SOA-based middleware [81], and other comparable technologies are examples of what falls under this category. Integrated value services are provided by location-based surveillance and service middleware, which integrates the positions of devices and other related information [82]. Communication middleware is capable of ensuring reliable communication between heterogeneous applications and devices. Typical uses of communication middleware include Supervisory Control and Data Acquisition (SCADA), RFID (Fosstrak [83], for example), and sensor network (TinyREST [84], for example). Pervasive middleware is a type of software that is designed for usage in a pervasive computing environment and is capable of delivering services across several platforms [85].

The following issues must be addressed to incorporate middleware into the Internet of Things [79].

- The interoperability problem is to link heterogeneous devices.
- The scalability problem is the ability to operate well in small-scale or large-scale settings with many objects.
- The difficulty of abstraction provision is to give abstractions at multiple levels.
- The difficulty with spontaneous engagement is providing dependable service for unplanned occasions.
- The issue of infixed infrastructure is to deliver dependable services without the need for a permanent infrastructure.
- The complexity problem is enabling concurrent device connectivity and picking or scheduling the best services for each device. IoT middleware should provide privacy, trust, and security.

- Resource Management and Sharing: Numerous heterogeneous networks are combined to give data for IoT applications (smart grid, smart transportation, etc.). Some programmes can share network resources to minimise costs. In this scenario, timely delivery of information needed by diverse apps is a challenge in IoT. To maximise the usage of network resources [86-88], existing resource sharing solutions generally rely on spectrum sharing. Spectrum sharing has three dimensions: space, frequency, and time. Contrary to most current communication systems, IoT focuses on "thing–to–thing" networks, where "thing" refers not just to machines or devices but also human behaviours and other things. Thus, establishing an effective resource sharing mechanism across heterogeneous networks suitable for IoT is a future development problem.

Furthermore, most IoT smart devices (sensors, RFID, etc.) are resource-restricted and cannot retrieve energy from the environment. As a result, resource management should address energy conservation [89]. It is possible to prolong sensor life by harvesting energy from distributed power [90], to reduce sensor power consumption by utilising a duty-cycle scheme [91], and to equilibrate sensor energy consumption and lengthen sensor network life [40], [69]. However, designing a solution suited for IoT network infrastructures that are made up of heterogeneous networks remains an open research topic.

6. Quality of Service (QoS) in IoT

IoT raises various QoS concerns, including dependability, availability, performance, mobility, interoperability, and scalability; most of these concerns are addressed by [16]-[49][92].

On the one hand, IoT system availability refers to the capacity to provide services to clients at any time and from any location. The IoT must try to be interoperable with all devices and follow protocols such as 6LoWPAN and IPv6. Alternatively, dependability refers to delivering IoT services with a high success rate achieved in hardware and software across all IoT levels. Furthermore, mobility is a term that relates to the process of linking clients to their preferred services when they are on the move; nevertheless, mobile devices might be disrupted as they move from one gateway to the other. [93] proposes an IoT-based architecture for enhancing mobility and security in medical settings.

Moreover, IoT scalability is a term that relates to the ability of adding new functions, services, and devices without impairing service quality. Supporting new devices and adding new operations is a complex undertaking in the face of varied communication protocols and hardware platforms. Furthermore, ensuring interoperability on these big-scale systems made of a considerable number of diverse items belonging to multiple platforms is difficult [94].

Furthermore, IoT service performance is a major issue since it is based on the performance of many IoT system components, which must constantly grow and expand their service performance to meet the requirements.

7. Open Issues

An in-depth investigation into the Internet of Things has been discussed in detail. in previous sections, encompassing various areas like technologies, applications, protocols, architecture, scalability, security, social issues, energy efficiency, and so on. We recognised some of the significant problems and open questions that future researchers must solve based on this. We've summed them up below.

1) Self-immunity: Offering self-immunity to IoT nodes is critical. Because future IoT applications will require more device autonomy, they must detect physical intrusion or manipulation. For

instance, sensor nodes are placed in hostile locations like border crossings or battlefields. Other restrictions like difficulty reaching places, lack of resources, etc., may prevent the sensors from providing security or other communications assistance. In such instances, nodes should be able to defend themselves. Developing self-immunity against IoT gadgets is thus another challenging job. Some of these defence systems comprise Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). Although some scholars [95] have begun developing such methods, the field remains unexplored for further study.

2) Optimal Energy Utilisation: Another unresolved issue is energy management in IoT devices. Due to the high cost of battery replacement, especially for large-scale implementations like the Internet of Things, low-power communication is a crucial research topic. Many energy-efficient options exist at various levels in the ISO model, but batteries will eventually need to be replaced, which represents a substantial barrier to the widespread adoption of IoT technology in general.
3) Efficient Memory Utilisation: In a similar vein to energy restrictions, the nodes employed in several IoT applications are limited in terms of storage. Optimal exploitation of the given storage space (memory) is difficult to address. Even though some buffer management strategies for ad hoc networks have been established [96-97], there are numerous issues that need to be resolved.
4) Incorporating Emerging Naming and Addressing Techniques in IoT: Some of the next-generation network designs, such as Named Data Networking, can be used for naming and addressing IoT applications (NDN). In IoT, named data objects can be used directly instead of IPv4 or IPv6 addresses. Some academics [98-99] have already specified implementing NDN into IoT architecture. Since the Internet is heading toward a more content-centric architecture, further studies in this area are possible.
5) Scalability: Scalability issues develop when the IoT network expands in size. All devices should have enough address space. A large number of sensors generates enormous amounts of data. Proper information extraction procedures must be used to save valuable data. We must find the service provider among billions of devices in the IoT.
6) IoT Object Behavioural Analysis: Because most IoT applications require things to be autonomous, analysing their behaviour is critical. WSN-based IoT applications collect data and send it to gateways or other management information systems. Some nodes may refuse to cooperate, misbehave towards other nodes, or turn evil by harming other nodes. IoT applications must have suitable trust management techniques to detect anomalous object behaviour. Although several researchers [100-101] have worked in this area, more can be done.
7) New IoT Applications in DTN and Content-Centric Network (CCN): The Internet of Things enables physical things to perceive, compute, and communicate with one another. Adding delay tolerance to standard IoT can let items communicate when connectivity is disrupted. Guo *et al.* [102] propose the opportunistic IoT, which connects devices to establish infrastructure-less networks utilising short-term communication protocols like WiFi or Bluetooth. An opportunistic IoT relies on human movement and chance encounters for data transmission and sharing among devices. The Internet of Underwater Things (IoUT) was described by Domingo *et al.* [103] as a network of smart underwater gadgets. The delay tolerance of integrated RFID sensor networks was studied by Al-Turjman *et al.* [104]. Delay-tolerant IoT applications could be the focus of future study, although few academics have looked at it. Similarly, as Internet applications move towards P2P CCN approaches,

researchers must investigate how IoT could integrate into such a setting. [105] discusses IoT performance via ICN.

8) Unified Architecture: While many academics are still working on a uniform IoT architecture, one must be compatible with all present designs and address obstacles like abstracting heterogeneity and interoperability. Data should be routed efficiently in IoT. However, building effective communication protocols is complex, with limited resources and lossy wireless networks.
9) Thwarting DoS Attacks: Protecting IoT systems from DoS attacks is another outstanding challenge because the adversary continuously delivers multiple handshake packets in a short span of time. The existing DoS defences are insufficient. So, building methods to protect against DoS assaults is required.
10) Enormous Data Handling Capabilities: As the number of Internet-connected devices grows exponentially, IoT applications are projected to create enormous data from many sources. Also, many real-time applications demand extensive data analysis. So, future academics will have to build Big Data analytics for upcoming IoT applications [106]. [107] discusses IoT Big Data sensing and handling problems.
11) Quality of Service (QoS): Another research challenge that future academics will address is providing quality of service measurements for monitoring network traffic in IoT applications. Although service quality criteria differ from application to application, providing appropriate service quality to customers is difficult. Additionally, because of bandwidth restrictions and other connectivity challenges, maintaining the QoS assurances in IoT applications is an open subject that has to be solved.

8. IoT: Applications and Services

In many domains like retail, health care, home, industries, transportation, surveillance, etc., countless IoT applications are available, as seen in Figure 6. The following is a list of various IoT applications.

1) Smart Health Care: Incorporating Internet of Things capabilities into medical devices will improve the quality of care offered to patients, especially the elderly who require constant attention. The Internet of Things can be used to monitor the health of older people to identify falls, monitor the temperature conditions inside refrigerators, that contain medicines and vaccines, and monitor the status of patients in hospitals and at home. The development of wearable gadgets, which will aid in collecting medical data, is currently the primary emphasis of smart healthcare solutions. Smart health scenarios are demonstrated by a smart device attached to the patient and designed to transmit alerts to nursing staff and physicians if the patient's health begins to deviate from the norm. Although the expansion of the Internet of Things in healthcare is a promising topic, there are specific concerns to consider in terms of security and data privacy.

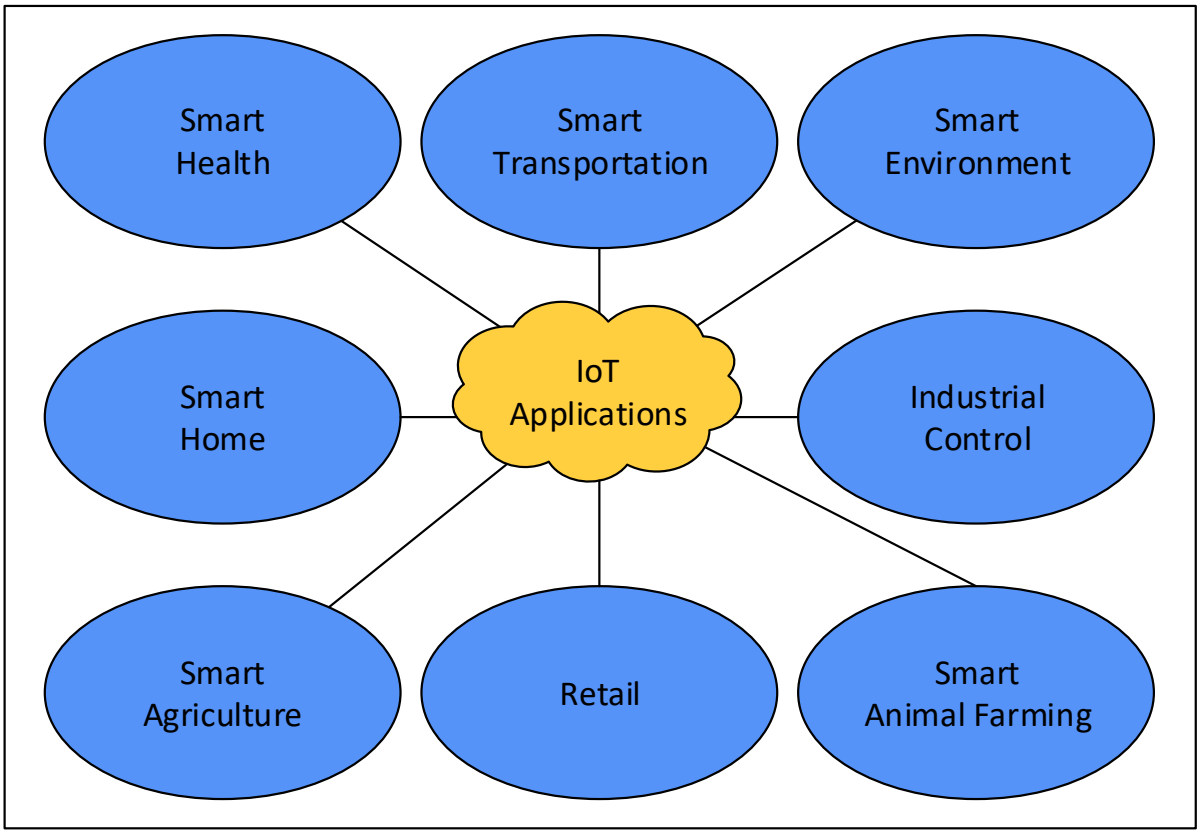


Fig. 6. Applications of Internet of Things

2) Smart Homes: The capacity to control any home gadget from a laptop or smartphone will be available in smart homes, and devices will be able to communicate with one another to provide us with valuable services. We can measure energy consumption and temperature with the help of smart metres. Temperature control, Light control, remote control, high-speed Internet access, camera surveillance, smart media, and smart appliances are just a few of the smart items that may be found in a smart home to make people's lives easier and more enjoyable.
3) Retail: Using the Internet of Things (IoT), it is possible to track down objects and keep track of their storage conditions. For example, it may be used to provide shopping recommendations to consumers preferences of customers, and it can also be utilised in the automatic stocking process by aiding in the rotation and control of items on shelves and warehouses of retail establishments, among other things.
4) Smart Transportation: Locating objects in big warehouses or ports, evaluating commodity quality during transportation, and tracking fragile products like gold or pharmaceuticals are all conceivable applications of the IoT. The following is an overview of a smart vehicular environment: one in which the various sensors assist in the analysis of traffic patterns and the notification of traffic jams, accidents, open parking spaces, and other events. This type of information assists passengers in driving safely and intelligently.
5) Industrial Control: It is common in industries to monitor ozone concentration, air quality, and temperature while also providing alerts in an emergency. The baggage handling machine used in airports is an example of this, as the sensors detect whether or not any baggage is travelling up the conveyor belt, and the machine stops if none is. The barcodes on the luggage allow for easy identification.

6) Smart Agriculture: When it comes to agriculture, the Internet of Things may be used to adjust climatic conditions to enhance fruit output, monitor soil moisture, and manage temperature and humidity conditions to avoid disease. Meteorological conditions like rain, drought, ice formation, and other occurrences can be predicted using the Internet of Things. A smart agriculture system in practise is a smart cow farm, where owners may get information about their cattle's behaviour, fertility, lactation, and mobility via smartphones, allowing them to boost the productivity of their herd.
7) Smart Environment: The IoT can monitor environmental conditions to detect and avoid natural disasters such as landslides, earthquakes, and other similar events. The IoT can be used to monitor CO_2 emissions from automobiles and companies and identify forest fires, among other things.

9. Conclusions

From virtual connections to social bonds, the Internet has made its way into our daily lives in a variety of ways. The Internet of Things (IoT) has given new possibilities to the Internet by enabling communication between items and humans, resulting in a wiser and more intelligent world. This has enabled the goal of "anytime, anywhere, anyhow, anything" communications to become a reality in the truest sense of the word. The IoT is believed to be the main component of the existing Internet, and its future course differs from the current Internet phase Internet, that we use and see every day. As a result, the architectural notion enters the scene. Architecture is a framework of technology-enabled items that allow them to interconnect and interact with other objects, whether they are similar or dissimilar, by putting a layer of human beings on top of them. It is evident that the existing IoT paradigm, that supports M2M communications, is becoming increasingly constrained by a variety of variables. New formulations are unavoidable for the long-term survival of the Internet of Things, and the researcher's job is to come up with a compelling notation for them. This paper begins by providing history and description for the Internet of Things (IoT). Second, extensive talks on the principles of IoT architectures are presented. Following that, in-depth examinations of the research problems are discussed. In this study, the challenges and prospective research prospects for future IoT researchers working in architecture and IoT, in general, are also discussed. Finally, we feel that this article serves as a starting point for developing a new architecture. The current design has a great deal of room for improvement on the semantic and security fronts. Ontologies tailored to specific domains or the invention of a new ontology format may be the subject of future research. It is anticipated that this work will be advantageous in terms of developing innovative IoT-based architectures and contributing to the research of our IoT Community.

Acknowledgement
This research was funded by IIUM-UMP-UiTM Sustainable Research Collaboration Grant 2020 (SRCG) under Grant ID: SRCG20-003-0003.
The authors express their personal appreciation for the effort of Ms Gousia Nissar and Ms Manasha Saqib in proofreading, editing and formatting the paper.

References

[1] Sfar, Arbia Riahi, Zied Chtourou, and Yacine Challal. "A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges." In *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, pp. 101-105. IEEE, 2017. https://doi.org/10.1109/SM2C.2017.8071828.

[2] Gatsis, Konstantinos, and George J. Pappas. "Wireless control for the IOT: Power, spectrum, and security challenges." In *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 341-342. IEEE, 2017.

[3] Khan, Burhan Ul Islam, Rashidah F. Olanrewaju, Farhat Anwar, Roohie Naaz Mir, Allama Oussama, and Ahmad Zamani Bin Jusoh. "Internet of Things—The concept, inherent security challenges and recommended solutions." In *Smart Network Inspired Paradigm and Approaches in IoT Applications*, pp. 63-86. Springer, Singapore, 2019. https://doi.org/10.1007/978-981-13-8614-5_5.

[4] Tan, Lu, and Neng Wang. "Future internet: The Internet of Things." In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5, pp. V5-376-V5-380. IEEE, 2010. https://doi.org/10.1109/ICACTE.2010.5579543.

[5] Khan, Burhan Ul Islam, Rashidah Funke Olanrewaju, Farhat Anwar, Roohie Naaz Mir, and Athaur Rahman Najeeb. "A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem." *International Journal of Information and Computer Security* 11, no. 4-5 (2019): 332-354. https://doi.org/10.1109/WoWMoM.2012.6263790

[6] Aleksandrovičs, Vladislavs, Eduards Filičevs, and Jānis Kampars. "Internet of Things: structure, features and management." *Information Technology and Management Science* 19, no. 1 (2016): 78-84. https://doi.org/10.1515/itms-2016-0015

[7] Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel JPC Rodrigues. "Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap." *IEEE Access* 9 (2020): 4466-4489. https://doi.org/10.1109/ACCESS.2020.3047895

[8] Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. "Interoperability in Internet of Things: Taxonomies and open challenges." *Mobile Networks and Applications* 24, no. 3 (2019): 796-809. https://doi.org/10.1007/s11036-018-1089-9

[9] Ray, Partha Pratim. "A survey on Internet of Things architectures." *Journal of King Saud University - Computer and Information Sciences* 30, no. 3 (2018): 291-319. https://doi.org/10.1016/j.jksuci.2016.10.003

[10] Zhang, Min, Tao Yu, and Guo Fang Zhai. "Smart transport system based on 'The Internet of Things'." *Applied Mechanics and Materials* 48-49 (February 2011): 1073-1076. https://doi.org/10.4028/www.scientific.net/amm.48-49.1073

[11] Yun, Miao, and Bu Yuxin. "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid." In *2010 International Conference on Advances in Energy Engineering*, pp. 69-72. IEEE, 2010. https://doi.org/10.1109/ICAEE.2010.5557611

[12] Liqiang, Zhao, Yin Shouyi, Liu Leibo, Zhang Zhen, and Wei Shaojun. "A crop monitoring system based on wireless sensor network." *Procedia Environmental Sciences* 11 (2011): 558-565. https://doi.org/10.1016/j.proenv.2011.12.088

[13] Singh, Dhananjay. "Developing an architecture: scalability, mobility, control, and isolation on future internet services." In *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1873-1877. IEEE, 2013. https://10.1109/ICACCI.2013.6637467

[14] Mashal, Ibrahim, Osama Alsaryrah, Tein-Yaw Chung, Cheng-Zen Yang, Wen-Hsing Kuo, and Dharma P. Agrawal. "Choices for interaction with things on Internet and underlying issues." *Ad Hoc Networks* 28 (2015): 68–90. https://doi.org/10.1016/j.adhoc.2014.12.006

[15] Lombardi, Marco, Francesco Pascale, and Domenico Santaniello. "Internet of Things: A general overview between architectures, protocols and applications." *Information (Basel)* 12, no. 2 (2021): 1-20. https://doi.org/10.3390/info12020087

[16] Khan, Rafiullah, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. "Future internet: the Internet of Things architecture, possible applications and key challenges." In *2012 10th International Conference on Frontiers of Information Technology*, pp. 257-260. IEEE, 2012. https://doi.org/10.1109/FIT.2012.53.

[17] Ning, Huansheng, and Ziou Wang. "Future Internet of Things architecture: like mankind neural system or social organization framework?" *IEEE Communications Letters: A Publication of the IEEE Communications Society* 15, no. 4 (2011): 461-463. https://doi.org/10.1109/lcomm.2011.022411.110120.

[18] Weyrich, Michael, and Christof Ebert. "Reference architectures for the Internet of Things." *IEEE Software* 33, no. 1 (2016): 112-116. https://doi.org/10.1109/ms.2016.20.

[19] Al-Khafajiy, Mohammed, Thar Baker, Hilal Al-Libawy, Atif Waraich, Carl Chalmers, and Omar Alfandi. "Fog computing framework for Internet of Things applications." In *2018 11th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 71-77. IEEE, 2018. https://doi.org/10.1109/DeSE.2018.00017

[20] Bonomi, Flavio, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. "Fog computing: A platform for Internet of Things and analytics." In *Big Data and Internet of Things: A Roadmap for Smart Environments*, pp. 169-186. Springer, Cham, 2014. https://doi.org/10.1007/978-3-319-05029-4_7

[21] Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." In *2014 Federated Conference on Computer Science and Information Systems*, pp. 1-8. IEEE, 2014. https://doi.org/10.15439/2014F503.

[22] Aazam, Mohammad, and Eui-Nam Huh. "Fog computing and smart gateway based communication for cloud of things." In *2014 International Conference on Future Internet of Things and Cloud*, pp. 464-470. IEEE, 2014. https://doi.org/10.1109/FiCloud.2014.83

[23] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "SIoT: Giving a social structure to the Internet of Things." *IEEE Communications Letters: A Publication of the IEEE Communications Society* 15, no. 11 (2011): 1193-1195. https://doi.org/10.1109/lcomm.2011.090911.111340

[24] Dalal, Priya, Gaurav Aggarwal, and Sanjay Tejasvee. "Internet of Things (IoT) in healthcare system: IA3 (Idea, Architecture, Advantages and Applications)." In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, pp. 1-6, 2020. https://dx.doi.org/10.2139/ssrn.3566282

[25] McGrath, Michael J., and Cliodhna Ní Scanaill. "Key sensor technology components: hardware and software overview." In *Sensor technologies*, pp. 51-77. Apress, Berkeley, CA, 2013. https://doi.org/10.1007/978-1-4302-6014-1_3

[26] Jovanović, Ugljša, Igor Jovanović, and Dragan Mančić. "Overview of temperature sensors for temperature measurement of PV modules." In *2018 26th Telecommunications Forum (TELFOR)*, pp. 1-8. IEEE, 2018. https://doi.org/10.1109/TELFOR.2018.8612096

[27] Li, Yanbing, Meng Yuan, and Jiyong Xu. "A pressure sensor study and research." In *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering*, vol. 2, pp. 255-258. IEEE, 2011. https://doi.org/10.1109/CCIENG.2011.6008114

[28] Beniwal, Gunjan, and Anita Singhrova. "A systematic literature review on IoT gateways." *Journal of King Saud University - Computer and Information Sciences,* 2021. https://doi.org/10.1016/j.jksuci.2021.11.007

[29] Javaid, Mohd, Abid Haleem, Shanay Rab, Ravi Pratap Singh, and Rajiv Suman. "Sensors for daily life: A review." *Sensors International* 2, no. 100121 (2021): 1-10. https://doi.org/10.1016/j.sintl.2021.100121

[30] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." In *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180-187. IEEE, 2015. https://doi.org/10.1109/ISCC.2015.7405513

[31] Zhang, Xialei, Xinyu Yang, Jie Lin, Guobin Xu, and Wei Yu. "On data integrity attacks against real-time pricing in energy-based cyber-physical systems." *IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society* 28, no. 1 (2017): 170-187, https://doi.org/10.1109/tpds.2016.2546259.

[32] Finkenzeller, Klaus. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.

[33] Herrojo, Cristian, Ferran Paredes, and Ferran Martín. "A new paradigm in chipless-RFID: all-dielectric permittivity contrast tags." In *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, pp. 163-166. IEEE, 2019. https://doi.org/10.1109/RFID-TA.2019.8892121

[34] Sunil, and Nitish Ojha. "Radio Frequency Identification (RFID) technology in library: Advantages and issues." In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 1206-1213. IEEE, 2018. https://doi.org/10.1109/ICISC.2018.8398996

[35] Du, Xiaojiang, Yang Xiao, Mohsen Guizani, and Hsiao-Hwa Chen. "An effective key management scheme for heterogeneous sensor networks." *Ad Hoc Networks* 5, no. 1 (2007): 24-34. https://doi.org/10.1016/j.adhoc.2006.05.012

[36] Le, Thang Nam, Wei Yu, Xiaole Bai, and Dong Xuan. "A dynamic geographic hash table for data-centric storage in sensor networks." In *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, vol. 4, pp. 2168-2174. IEEE, 2006. https://doi.org/10.1109/WCNC.2006.1696632

[37] Mallapuram, Sriharsha, Nnatubemugo Ngwum, Fang Yuan, Chao Lu, and Wei Yu. "Smart city: The state of the art, datasets, and evaluation platforms." In *2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)*, pp. 447-452. IEEE, 2017. https://doi.org/10.1109/ICIS.2017.7960034

[38] Muniz, Ruben, Luis Junco, and Adolfo Otero. "A robust software barcode reader using the Hough transform." In *Proceedings 1999 International Conference on Information Intelligence and Systems (Cat. No. PR00446)*, pp. 313-319. IEEE, 1999. https://doi.org/10.1109/ICIIS.1999.810282

[39] Wu, Miao, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. "Research on the architecture of Internet of Things." In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5, pp. V5-484-V5-487. IEEE, 2010. https://doi.org/10.1109/ICACTE.2010.5579493

[40] Yu, Wei, David Griffith, Linqiang Ge, Sulabh Bhattarai, and Nada Golmie. "An integrated detection system against false data injection attacks in the smart grid: smart grid, data security, false data injection attacks." *Security and Communication Networks* 8, no. 2 (2015): 91-109. https://doi.org/10.1002/sec.957

[41] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "A survey on sensor networks." *IEEE Communications Magazine* 40, no. 8 (2002): 102-114. https://doi.org/10.1109/mcom.2002.1024422

[42] Lin, Jie, Xinyu Yang, Wei Yu, and Xinwen Fu. "Towards effective en-route filtering against injected false data in wireless sensor networks." In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pp. 1-5. IEEE, 2011. https://doi.org/10.1109/GLOCOM.2011.6134278

[43] Wu, Dapeng, Boran Yang, and Ruyan Wang. "Scalable privacy-preserving big data aggregation mechanism." *Digital Communications and Networks* 2, no. 3 (2016): 122-129. https://doi.org/10.1016/j.dcan.2016.07.001.

[44] Suo, Hui, Jiafu Wan, Caifeng Zou, and Jianqi Liu. "Security in the Internet of Things: a review." In *2012 International Conference on Computer Science and Electronics Engineering*, vol. 3, pp. 648-651. IEEE, 2012. https://doi.org/10.1109/ICCSEE.2012.373

[45] He, Xuechen. "The two-dimensional bar code application in book management." In *2010 International Conference on Web Information Systems and Mining*, vol. 1, pp. 409-411. IEEE, 2010. https://doi.org/10.1109/WISM.2010.58

[46] Mukherjee, Amitava, Debashis Saha, and Chinmohan Biswas. "Present scenarios and future challenges in pervasive middleware." In *2006 1st International Conference on Communication Systems Software & Middleware*, pp. 1-5. IEEE, 2006. https://doi.org/10.1109/COMSWA.2006.1665199

[47] Singh, H. 2021. How are images stored on a computer, *Analytics Vidhya* Available at: https://www.analyticsvidhya.com/blog/2021/03/grayscale-and-rgb-format-for-storing-images/ (Accessed: 12 January 2022).

[48] Y Yang, Bo, Kaijie Wu, and Ramesh Karri. "Scan based side channel attack on dedicated hardware implementations of data encryption standard." In *2004 International Conference on Test*, pp. 339-344. IEEE, 2004. https://doi.org/10.1109/TEST.2004.1386969

[49] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. "Internet of Things: A survey on enabling technologies, protocols, and applications." *IEEE Communications Surveys & Tutorials* 17, no. 4 (2015): 2347–2376. https://doi.org/10.1109/comst.2015.2444095

[50] Gan, Gang, Zeyong Lu, and Jun Jiang. "Internet of Things security analysis." In *2011 International Conference on Internet Technology and Applications*, pp. 1-4. IEEE, 2011. https://doi.org/10.1109/ITAP.2011.6006307

[51] "IEEE Standard for Low-Rate Wireless Networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, (2020). https://doi.org/10.1109/IEEESTD.2020.9144691

[52] Kluge, Wolfram, Frank Poegel, Hendrik Roller, Matthias Lange, Tilo Ferchland, Lutz Dathe, and Dietmar Eggert. "A fully integrated 2.4-GHz IEEE 802.15.4-compliant transceiver for ZigBee™ applications." *IEEE Journal of Solid-State Circuits* 41, no. 12 (2006): 2767-2775. https://doi.org/10.1109/jssc.2006.884802

[53] Kim, Anna N., Fredrik Hekland, Stig Petersen, and Paula Doyle. "When HART goes wireless: Understanding and implementing the WirelessHART standard." In *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 899-907. IEEE, 2008. https://doi.org/10.1109/ETFA.2008.4638503

[54] Palattella, Maria Rita, Nicola Accettura, Luigi Alfredo Grieco, Gennaro Boggia, Mischa Dohler, and Thomas Engel. "On optimal scheduling in duty-cycled industrial IoT applications using IEEE802.15.4e TSCH." *IEEE Sensors Journal* 13, no. 10 (2013): 3655-3666. https://doi.org/10.1109/jsen.2013.2266417

[55] Palattella, Maria Rita, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. "Standardized protocol stack for the Internet of (Important) Things." *IEEE Communications Surveys & Tutorials* 15, no. 3 (2013): 1389-1406. https://doi.org/10.1109/surv.2012.111412.00158

[56] Baronti, Paolo, Prashant Pillai, Vince W. C. Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu. "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards." *Computer Communications* 30, no. 7 (2007): 1655-1695. https://doi.org/10.1016/j.comcom.2006.12.020

[57] Gomez, Carles, and Josep Paradells. "Wireless home automation networks: A survey of architectures and technologies." *IEEE Communications Magazine* 48, no. 6 (2010): 92-101. https://doi.org/10.1109/mcom.2010.5473869

[58] Bormann, Carsten, Angelo P. Castellani, and Zach Shelby. "CoAP: An application protocol for billions of tiny internet nodes." *IEEE Internet Computing* 16, no. 2 (2012): 62-67. https://doi.org/10.1109/mic.2012.29

[59] Gao, Weichao, James Nguyen, Wei Yu, Chao Lu, and Daniel Ku. "Assessing performance of constrained application protocol (CoAP) in MANET using emulation." In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*, pp. 103-108. 2016. https://doi.org/10.1145/2987386.2987400

[60] Tariq, Muhammad Ashar, Murad Khan, Muhammad Toaha Raza Khan, and Dongkyun Kim. "Enhancements and challenges in CoAP—A survey." *Sensors (Basel, Switzerland)* 20, no. 21 (2020): 1-29. https://doi.org/10.3390/s20216391

[61] Villaverde, Berta Carballido, Dirk Pesch, Rodolfo De Paz Alberola, Szymon Fedor, and Menouer Boubekeur. "Constrained application protocol for low power embedded networks: A survey." In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 702-707. IEEE, 2012. https://doi.org/10.1109/IMIS.2012.93

[62] Al-Masri, Eyhab, Karan Raj Kalyanam, John Batts, Jonathan Kim, Sharanjit Singh, Tammy Vo, and Charlotte Yan. "Investigating messaging protocols for the Internet of Things (IoT)." *IEEE Access: Practical Innovations, Open Solutions* 8 (2020): 94880–94911. https://doi.org/10.1109/access.2020.2993363

[63] Bertaux, Lionel, Akram Hakiri, Samir Medjiah, Pascal Berthou, and Slim Abdellatif. "A DDS/SDN based communication system for efficient support of dynamic distributed real-time applications." In *2014 IEEE/ACM 18th International Symposium on Distributed Simulation and Real Time Applications*, pp. 77-84. IEEE, 2014. https://doi.org/10.1109/DS-RT.2014.18

[64] Vinoski, Steve. "Advanced Message Queuing Protocol." *IEEE Internet Computing* 10, no. 6 (2006): 87-89. https://doi.org/10.1109/mic.2006.116

[65] Sarkar, Manasi, and Debdutta Barman Roy. "Prevention of sleep deprivation attacks using clustering." In *2011 3rd International Conference on Electronics Computer Technology*, vol. 5, pp. 391-394. IEEE, 2011. https://doi.org/10.1109/ICECTECH.2011.5942027

[66] Jara, Antonio J., Pedro Martinez-Julia, and Antonio Skarmeta. "Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the web of things." In *2012 Sixth international conference on innovative mobile and internet services in ubiquitous computing*, pp. 731-738. IEEE, 2012.. https://doi.org/10.1109/IMIS.2012.200

[67] Lee, Sejun, Jaehoon Paul Jeong, and Jung-Soo Park. "DNSNA: DNS name autoconfiguration for Internet of Things devices." In *2016 18th International Conference on Advanced Communication Technology (ICACT)*, pp. 410-416. IEEE, 2016. https://doi.org/10.1109/ICACT.2016.7423412

[68] Khan, Burhan Ul Islam, Farhat Anwar, Rashidah Funke Olanrewaju, Bisma Rasool Pampori, and Roohie Naaz Mir. "A novel multi-agent and multilayered game formulation for intrusion detection in Internet of Things (IoT)." *IEEE Access* 8 (2020): 98481-98490. https://doi.org/10.1109/ACCESS.2020.2997711.

[69] Olanrewaju, Rashidah Funke, Burhan Ul Islam Khan, Farhat Anwar, and Roohie Naaz Mir. "Internet of Things security vulnerabilities and recommended solutions." *International Journal of Engineering & Technology* 7, no. 4, (2018): 4899-4904. https://doi.org/10.14419/ijet.v7i4.23147

[70] Xu, Li Da. "Enterprise systems: State-of-the-art and future trends." *IEEE Transactions on Industrial Informatics* 7, no. 4 (2011): 630-640. https://doi.org/10.1109/tii.2011.2167156

[71] Gama, Kiev, Lionel Touseau, and Didier Donsez. "Combining heterogeneous service technologies for building an Internet of Things middleware." *Computer Communications* 35, no. 4 (2012): 405-417. https://doi.org/10.1016/j.comcom.2011.11.003

[72] Guinard, Dominique, Vlad Trifa, Stamatis Karnouskos, Patrik Spiess, and Domnic Savio. "Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of web services." *IEEE Transactions on Services Computing* 3, no. 3 (2010): 223-235. https://doi.org/10.1109/tsc.2010.3

[73] Ren, Xuebin, Xinyu Yang, Jie Lin, Qingyu Yang, and Wei Yu. "On scaling perturbation based privacy-preserving schemes in smart metering systems." In *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-7. IEEE, 2013. https://doi.org/10.1109/ICCCN.2013.6614162

[74] Zheng, Xu, Zhipeng Cai, Jianzhong Li, and Hong Gao. "Location-privacy-aware review publication mechanism for local business service systems." In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pp. 1-9. IEEE, 2017. https://doi.org/10.1109/INFOCOM.2017.8056976

[75] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The Internet of Things: A survey." *Computer Networks* 54, no. 15 (2010): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[76] Mello, Lucilene Dornelles, and Lauro Tatsuo Kubota. "Review of the use of biosensors as analytical tools in the food and drink industries." *Food Chemistry* 77, no. 2 (2002): 237-256. https://doi.org/10.1016/s0308-8146(02)00104-8

[77] Fu, Xinwen, Zhen Ling, Wei Yu, and Junzhou Luo. "Cyber Crime Scene Investigations (C^2SI) through cloud computing." In *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, pp. 26-31. IEEE, 2010. https://doi.org/10.1109/ICDCSW.2010.33

[78] Chaqfeh, Moumena A., and Nader Mohamed. "Challenges in middleware solutions for the Internet of Things." In *2012 International Conference on Collaboration Technologies and Systems (CTS)*, pp. 21-26. IEEE, 2012. https://doi.org/10.1109/CTS.2012.6261022

[79] Pingley, Aniket, Wei Yu, Nan Zhang, Xinwen Fu, and Wei Zhao. "A context-aware scheme for privacy-preserving location-based services." *Computer Networks* 56, no. 11 (2012): 2551-2568. https://doi.org/10.1016/j.comnet.2012.03.022

[80] Soni, Manish, and Bharat Pahadiya. "Detection and removal of vampire attack in wireless sensor network." *International Journal of Computer Applications* 126, no. 7 (2015): 46-50. https://doi.org/10.5120/ijca2015906101.L

[81] Roselli, Luca, Chiara Mariotti, Paolo Mezzanotte, Federico Alimenti, Giulia Orecchini, Marco Virili, and Nuno Borges Carvalho. "Review of the present technologies concurrently contributing to the implementation of the Internet of Things (IoT) paradigm: RFID, green electronics, WPT and energy harvesting." In *2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, pp. 1-3. IEEE, 2015. https://doi.org/10.1109/WISNET.2015.7127402

[82] Gómez-Goiri, Aitor, and Diego López-de-Ipiña. "A triple space-based semantic distributed middleware for internet of things." In *International Conference on Web Engineering*, pp. 447-458. Springer, Berlin, Heidelberg, 2010. https://doi.org/10.1007/978-3-642-16985-4_43

[83] Fosstrak – Welcome, *Fosstrak.Github.Io* Available at: https://fosstrak.github.io/ (Accessed: 15 December 2021)

[84] López, Pablo, David Fernández, Antonio J. Jara, and Antonio F. Skarmeta. "Survey of Internet of Things technologies for clinical environments." In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pp. 1349-1354. IEEE, 2013. https://doi.org/10.1109/WAINA.2013.255

[85] Mukaddam, Ayman, Imad Elhajj, Ayman Kayssi, and Ali Chehab. "IP spoofing detection using modified hop count." In *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 512-516. IEEE, 2014. https://doi.org/10.1109/AINA.2014.62

[86] Ling, Zhen, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia. "A new cell-counting-based attack against Tor." *ACM Transactions on Networking [a Joint Publication of the IEEE Communications Society, the IEEE Computer Society, and the ACM with Its Special Interest Group on Data Communication]* 20, no. 4 (2012): 1245-1261. https://doi.org/10.1109/tnet.2011.2178036

[87] Tsai, Chun-Wei, Chin-Feng Lai, Ming-Chao Chiang, and Laurence T. Yang. 2014. "Data mining for Internet of Things: A survey." *IEEE Communications Surveys & Tutorials* 16, no. 1 (2014): 77-97. https://doi.org/10.1109/surv.2013.103013.00206

[88] Zhao, Nan, F. Richard Yu, Ming Li, and Victor C. M. Leung. "Anti-eavesdropping schemes for Interference Alignment (IA)-based wireless networks." *IEEE Transactions on Wireless Communications* 15, no. 8 (2016): 5719-5132. https://doi.org/10.1109/twc.2016.2568188

[89] Romero, Daniel, Gabriel Hermosillo, Amirhosein Taherkordi, Russel Nzekwa, Romain Rouvoy, and Frank Eliassen. "RESTful integration of heterogeneous devices in pervasive environments." In *IFIP International Conference on Distributed Applications and Interoperable Systems*, pp. 1-14. Springer, Berlin, Heidelberg, 2010. https://doi.org/10.1007/978-3-642-13645-0_1

[90] Cammarano, Alessandro, Chiara Petrioli, and Dora Spenza. "Pro-Energy: A novel energy prediction model for solar and wind energy-harvesting wireless sensor networks." In *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, pp. 75-83. IEEE, 2012. https://doi.org/10.1109/MASS.2012.6502504

[91] Shu, Ting, Wei Liu, Tian Wang, Qingyong Deng, Ming Zhao, Neal N. Xiong, Xiong Li, and Anfeng Liu. "Broadcast based code dissemination scheme for duty cycle based wireless sensor networks." *IEEE Access* 7 (2019): 105258-105286. https://doi.org/10.1109/ACCESS.2019.2932006

[92] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of Things: Vision, applications and research challenges." *Ad Hoc Networks* 10, no. 7 (2012): 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[93] Valera, Antonio J. Jara, Miguel A. Zamora, and Antonio FG Skarmeta. "An architecture based on Internet of Things to support mobility and security in medical environments." In *2010 7th IEEE Consumer Communications and Networking Conference*, pp. 1-5. IEEE, 2010. https://doi.org/10.1109/CCNC.2010.5421661

[94] Liu, Yuxi, and Guohui Zhou. "Key technologies and applications of Internet of Things." In *2012 Fifth International Conference on Intelligent Computation Technology and Automation*, pp. 197-200. IEEE, 2012. https://doi.org/10.1109/ICICTA.2012.56

[95] Riahi, Arbia, Enrico Natalizio, Yacine Challal, Nathalie Mitton, and Antonio Iera. "A systemic and cognitive approach for IoT security." In *2014 International Conference on Computing, Networking and Communications (ICNC)*, pp. 183-188. IEEE, 2014. https://doi.org/10.1109/ICCNC.2014.6785328

[96] Al-Mahdi, Hassan, and Mohamed A. Kalil. "A dynamic hop-aware buffer management scheme for multi-hop ad hoc networks." *IEEE Wireless Communications Letters 6*, no. 1 (2017): 22-25. https://doi.org/10.1109/lwc.2016.2625278

[97] Sobin, C. C. "An efficient buffer management policy for DTN." *Procedia Computer Science* 93: (2016) 309-314. https://doi.org/10.1016/j.procs.2016.07.215

[98] Datta, Soumya Kanti, and Christian Bonnet. "Integrating named data networking in Internet of Things architecture." In *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1-2. IEEE, 2016. https://doi.org/10.1109/ICCE-TW.2016.7520967

[99] Baccelli, Emmanuel, Christian Mehlis, Oliver Hahm, Thomas C. Schmidt, and Matthias Wählisch. "Information centric networking in the IoT: Experiments with NDN in the wild." In *Proceedings of the 1st ACM Conference on Information-Centric Networking*, pp. 77-86. 2014. https://doi.org/10.1145/2660129.2660144

[100] Chen, Dong, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang. "TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things." *Computer Science and Information Systems* 8, no. 4 (2011): 1207-1228. https://doi.org/10.2298/csis110303056c

[101] Farhan, Laith, Rasha Subhi Hameed, Asraa Safaa Ahmed, Ali Hussein Fadel, Waled Gheth, Laith Alzubaidi, Mohammed A. Fadhel, and Muthana Al-Amidie. "Energy efficiency for green Internet of Things (IoT) networks: A survey." *Network* 1, no. 2 (2021): 279-314. https://doi.org/10.3390/network1030017

[102] Guo, Bin, Daqing Zhang, Zhu Wang, Zhiwen Yu, and Xingshe Zhou. "Opportunistic IoT: Exploring the harmonious interaction between human and the Internet of Things." *Journal of Network and Computer Applications* 36, no. 6 (2013): 1531-1539. https://doi.org/10.1016/j.jnca.2012.12.028

[103] Domingo, Mari Carmen. "An overview of the Internet of Underwater Things." *Journal of Network and Computer Applications* 35, no. 6 (2012): 1879-1890. https://doi.org/10.1016/j.jnca.2012.07.012

[104] Al-Turjman, Fadi M., Ashraf E. Al-Fagih, Waleed M. Alsalih, and Hossam S. Hassanein. 2013. "A delay-tolerant framework for integrated RSNs in IoT." *Computer Communications* 36, no. 9 (2013): 998-1010. https://doi.org/10.1016/j.comcom.2012.07.001

[105] Rao, Akhila, Olov Schelén, and Anders Lindgren. "Performance implications for IoT over information centric networks." In *Proceedings of the Eleventh ACM Workshop on Challenged Networks*, pp. 57-62. ACM, 2016. https://doi.org/10.1145/2979683.2979686

[106] Mukherjee, Arijit, Himadri Sekhar Paul, Swarnava Dey, and Ansuman Banerjee. "ANGELS for distributed analytics in IoT." In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 565-570. IEEE, 2014. https://doi.org/10.1109/WF-IoT.2014.6803230

[107] Zaslavsky, Arkady, Charith Perera, and Dimitrios Georgakopoulos. "Sensing as a service and big data." *arXiv preprint arXiv:1301.0159* (2013). http://arxiv.org/abs/1301.0159