Internet of Things Fundamentals, Architectures, Challenges and Solutions: A Survey

Maha Abdelhaq
Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia

Summary
As the number of people using the Internet increases, a new application known as the Internet of Things (IoT) has been emerged. Internet of Things makes it easier for machines and objects to exchange, compute, and coordinate information autonomously without human interference. It is a tool for attaching intelligence to a variety of contemporary objects in houses, hospitals, buildings, vehicles, and even cities. As a new emerging technology, the focus in current IoT surveys does not shed the light on deep understanding for IoT fundamentals, architectures, challenges, and solutions. For this reason, the objective of this paper is to introduce specifications for IoT definitions, characteristics, functional blocks, and different architectures as a cement for better understanding. Additionally, we present current documented IoT challenges, with the existing available solution for each challenge.

Key words:
Internet of Things (IoT); IoT fundamentals; IoT architectures; IoT challenges and solutions.

1. Introduction

Millions of people rely on the Internet for a variety of purposes, and it has become a fundamental necessity for many. As well as for leisure (movies, music, and games), many people rely on the Internet to carry out routine duties and requirements that they could not do. The Internet is used by around 48% of the global population, according to current estimates [1]. This indicates that more than half of the world's population has access to the Internet, thanks to its widespread use and the numerous advantages it offers. Another benefit of more individuals using the Internet is that they can communicate and synchronize with people all around the world. When items and machines can connect and interact with each other over the Internet, this is known as the Internet of Things (IoT) [2]. The idea behind this new technology is to automate the labor and link the devices that we use in our everyday lives via the Internet to the Internet. Sensors are attached to each object in order to gather data from the real-world environment. Local processing removes unneeded material from the information and stores it in local memory. All acquired data is transported from local storage to the cloud, where it is accessible to all objects. Finally, a suitable action is done based on the acquired data. It's not necessary to take action every time, but we may utilize this data to remotely manage and control equipment and objects, and to keep records for future reference.

The IoT can be implemented using a variety of technologies and sensors. A wide range of communication technologies are employed to implement the Internet of Things, including RFID, NFC, and wireless sensor networks [3]. IoT has been used in a wide range of applications. With the assistance of the Internet, they've gotten smarter and more robotic in their job [4]. To begin with, sensors are employed in the health care sector to monitor a person's body temperature, blood pressure and heart rate. There are various electronic appliances in the house, including refrigerators, microwave ovens, fan heaters, and air conditioning units. Another application is smart home. For the purpose of resolving a problem, sensors have been fitted to identify and report issues [5]. Animal tracking is the third use of IoT. In order to track an animal, GPS sensors are embedded in its body. Use it to keep an eye on the animal's food intake [6]. Smart robotics grippers that directly contact an item to capture sensory information are another IoT application. They are a relatively new development. Touch, motion, vision, optical, and force sensors are just a few of the many components that go into a smart gripper. In order for a smart gripper to be smart, it must be outfitted with sensors that can gather real-time data and use that data to make judgments. Due to design constraints like as cost, weight, and compactness, they must be limited in their scope [7]. In addition, the IoT has several applications, including smart transportation, infrastructure management, manufacturing, smart construction, smart agriculture, and smart retail. Figure 1 shows different applications in IoT.

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2022.22.1.26

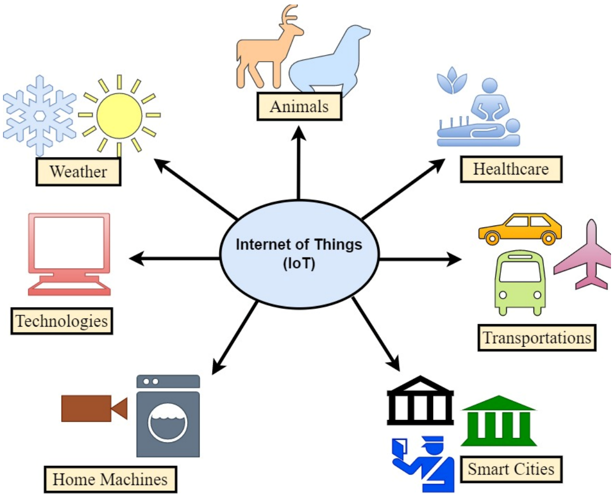

Fig. 1. IoT applications

The present IoT surveys do not give insight on the basics, architectures, difficulties, and solutions of IoT as a new emergent technology. For this reason, the objective of this paper is to introduce specifications for IoT definitions, characteristics, functional blocks, and different architectures as a cement for better understanding. Additionally, we present current documented IoT challenges, with the existing available solution for each challenge.

The structure of the survey is as follows: Section 2 provides a review for the most recent IoT related works. Section 3 displays a comprehensive discussion for IoT definitions, characteristics, and main functional components. Section 4 provides a very deep discussion for IoT architectures and their related specifications. Section 5 discusses the most recent IoT challenges and the existing solutions. Finally, section 6 concludes the survey.

2. Related Works

Internet of Things has been the subject of a wide range of studies. However, IoT related research is still excessively scattered and insufficient, and focused mostly on a few specific areas of this domain. A literature evaluation of some of these works is included in this part.

Internet-based human capital management system (HCMS) has several advantages and disadvantages that have been discussed in [8]. IoT healthcare applications and constraints were discussed to create boundaries and improve healthcare quality.

To reduce security threats, the authors in [9] presented a smart collaborative security paradigm. A medical care approach has been used to examine IoT security and privacy, as well as other aspects of security needs, threat models, and taxonomies.

The authors in [10] introduced a wide range of definitions for IoT concepts from a variety of scholars. The progress of the technology was discussed in a chronological order. A brief discussion was held on a variety of IoT topics, including its technological advances, transmission standards, structural design, and an outline of its future.

An in-depth look into forensics for IoT devices was given by [11]. IoT forensics has been shown to be affected by and facilitated by unique aspects in this study. Forensic data processing, tools, and layers were all investigated to determine the strengths and weaknesses of various IoT-related literature sources and categorize them accordingly.

The authors in [12] highlighted IoT characteristics and visions and Applications offered insights on various supporting technologies and communication protocols based on their capabilities, examined middleware and network domains.

The authors in [13] concentrated on the CSI development process. IoT security specialists have identified the security aspects that favor discussing the value, attraction, and possible engagement of a security label.

3. Fundamentals of IoT

IoT paradigm has opened the doors to new inventions, discoveries and interactions among things and people, which will, in turn, improve the exploitation of scarce resources and human quality of life. To comprehend the full picture of the IoT model, the following sections will address different IoT definitions, IoT characteristics, and smart devices' basic components.

3.1. IoT Definition

The concept of IoT has been introduced for the first time in 1999 by Kevin Ashton when he presented RFID as a technology for connecting the things [14]. The highlighted idea after that was every object and everything even if it is a machine or not can have an identification number which allow it to communicate with the other objects. IoT popularity has been increased in 2010 for its importance in many applications; such as industry, education and healthcare [15], school, transportation, agriculture, smart home and market domains [2, 4, 16, 17].

The ultimate advantage for IoT is in developing the human life by allowing the things to communicate with each other and manage themselves autonomously. This provides different services for people with less efforts [18, 19]. On the other hand, IoT is a newly born concept with huge number of technologies and emergent protocols. Thus, still the research does not introduce a consolidated definition for IoT. The following definitions have been introduced by different scientific resources:

- The first definition implies that IoT is an interconnected sensing and actuator devices that can share information across platforms through a common operating system provide the basis for innovative applications [20].
- The second definition entails that IoT is a network which is made up of Physical and virtual entities. The physical things can be a car, people, animals, machine, and non-machine objects. The virtual entities can be an email, twitter, database storage and Facebook [21]. Different abilities such as sensing, analyzing and processing, as well as self-management based on interoperable communication protocols and specific criteria are embedded in these entities [22].
- In the third definition IoT indicates that anything can be connected to anything at anytime, anywhere. [21]. and in [23], IoT refers to anything that can be accessed by any body from anywhere at any time by anyone for any service over any network, according to the author. As a result, the Internet of Things can be referred to as 6Anys.

As in the last definition, which is the most popular and obvious definition, IoT enables anything to communicate with anything, the “thing” could be a living or non-living, a machine or non-machine things after digitizing these things. Figure 2 depicts the definition very briefly.

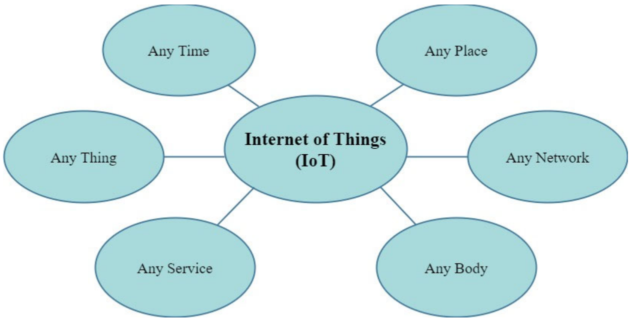

Fig. 2. IoT Definition

3.2. IoT Characteristics

As aforementioned IoT definitions, certain IoT characteristics can be concluded as in the following [23-25]:

- Dynamicity and Self-Adaptation: IoT devices can dynamically adapt to shifting contexts and conduct actions based on the user's context or perceived surroundings [26]. Consider, for example, a surveillance system consisting of several cameras. According on whether it is day or night, the security cameras may change their settings to regular or night infrared modes. They can also notify adjacent cameras to do so. Also, a decision-making criterion in IoT devices is, mainly based on the sensed environment context.
- Self-Configuration: An IoT device may be equipped with self-configuration capability, enabling the use of many different devices to work together to accomplish a certain goal, such as monitoring air pollution. If properly incorporated, these devices may be able to configure themselves with regard to the IoT architecture, establish a network, and obtain the latest software upgrades while requiring minimal human interference.
- Communication protocols’ Interoperability: A wide range of communication protocols may be supported by IoT devices, allowing them to communicate with other devices.
- Unique Identity: The devices equipped with IoT have distinct identities and unique identifiers, such as IP addresses or URLs. These identities are primary for devices communication with each other through different interfaces. IoT devices can be equipped with intelligent interfaces which could change according to the situation. Letting users to connect with their environments and have conversations with them.
- Integration into Information Network: It's not uncommon for IoT devices to be linked into the overall network that facilitates communication and data exchange across various devices and systems. Through the IoT, connected devices may find each other, explain themselves, and display their attributes. For example, an air pollution monitoring node can inform another linked node about its monitoring capabilities, allowing them to communicate and share data.
- Intelligent decision-making capability: IoT's multi-hop nature makes the whole network more energy efficient, increasing the lifetime of the network. Because IoT in this case uses an intelligent decision-making feature to aggregate data from various sensor nodes, and after aggregation, they collaborate to reach a final decision-making result.
- Distributive: The IoT model may have been built in an extremely distributed environment, where multiple sources collect data and afterwards analyze the data in a distributed method using unique smart entities. [27].

3.3. IoT Functional Blocks

While there are several different functions included in IoT systems, they are often made up of different functional blocks to serve distinct utilities. For instance, some blocks deal with sensing, communication, identification, actuation, and management as in the followings [3, 23, 24]:

- Device: An IoT system incorporates sensor devices, control devices, actuators, monitors, and managers. IoT enables the flow of data between linked devices and applications. Devices that connect to the IoT might gather data from other connected devices and analyze that data locally. Moreover, the data may be sent to cloud-based servers that perform various processing tasks. Furthermore, IoT devices may do some activities locally, while other tasks which are linked to restrictions, such as memory capacity, processing capabilities, and communication delays, will occur within IoT infrastructure, which has a specific amount of available bandwidth. A standard IoT device could be comprised of multiple communication interfaces, such as connectivity, sensors, actuators, audio/video, and memory I/O interfaces. Figure 3 shows IoT devices components and interfaces.

- Communication: This block is in charged in connecting devices and remote servers. There are a wide range of IoT protocols applied on different layers for communication, the layers vary based on the applied IoT architecture (discussed in the bellow sections).
- Services: The use of Internet of Things techniques has spread across multiple application domains, including home appliances, manufacturing, and offices. To improve IoT application development, IoT services must be implemented in specific ways. Services that have the capability to form connections and communicate can be grouped into services that are collaborative aware, identity-related services, services for finding devices, device modeling, device control, data analytics, information aggregation, and services that publish data across a variety of devices [28].
- Management: The unique feature of IoT devices is remote management with or without human intervention. Additionally, the devices can communicate data with each other in order to reach a choice appropriate for the situation later on. While trust management is vital to the seamless collection of IoT data and contextualized services, reliable data fusion and mining. Trust management also provides additional capabilities such as qualified services with context awareness, as well as heightened user privacy and information security. It assists individuals in working beyond their fear of uncertainty and risk, stimulating customer acceptance and use of IoT solutions and applications.[29, 30].
- Security: The data in IoT is susceptible to many intrusions such spoofing, denial of service, denial of service attack, sinkhole, sybil attack, and so on. Therefore, IoT systems should integrate several security functions, such as identity, authorization, trust, privacy, authentication, as well as data availability, confidentiality and integrity [31, 32].
- Application: Application layer is crucial in terms of users since it is the component that acts as a window to access system elements such as sensors and actuators. IoT applications enable users to observe and examine the system's current condition and make predictions about what will happen in the future.

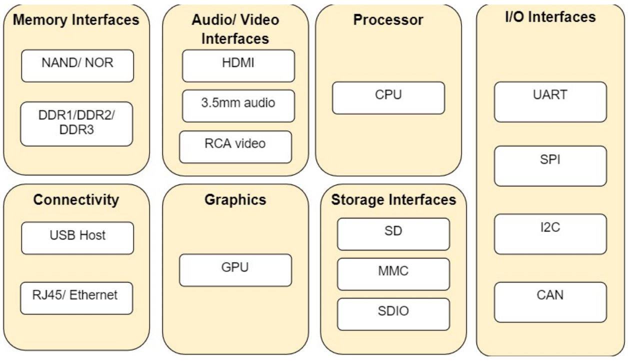

Fig. 3. IoT Device Components and Interfaces

4. IoT Architectures

The idea of IoT encompasses several architectural approaches. In another word, IoT's architecture is dependent on the data and applications you are using. Therefore, Each IoT solution has its own architecture. As a result, the researchers introduces several IoT architectures [21].

Based on our reviewing an enormous number of the IoT architectures introduced, we have concluded that they must have a tiered design in which standards and technologies may be developed independently at each layer. The connectivity of IoT endpoint devices to a network that transmits the data where it is, eventually used by applications is similar across the subsequent reviewed IoT architectures.

4.1. Three Layers IoT Architecture

This architecture is presented in [33] as a two analogous stacks: one of them called "IoT Data Management and Compute Stack" and the another one called "Core IoT Functional Stack". Even though the framework is reduced to three-layer stacks in both architectures, it doesn't mean the IoT approach is lacking in depth. the whole IoT architecture is intended to be simplified into its most basic building blocks, Next, it may be applied to understanding industry-specific design and deployment concepts.

4.1.1. Core IoT Functional Stack

This IoT architecture is depicted in Figure 4. The idea is that smart "things" or "objects" that can execute functions and provide new linked services are incorporated into IoT networks. Because of their "smart" functionality, these "things" utilize both contextual information and designed aims to carry out their functions. An external system is used to report the data that the smart object collects. Management platforms can be used to process data gathered from the smart object, as well as to direct the smart object's actions. For an IoT network to be operational, numerous components must function together from an architectural standpoint [33, 34]:

- "Things" layer: also called Perception layer, this layer includes IoT devices which should be able to give the information needed while also fitting into the environment context in which they are installed [33]. It Performs many functions which are sensing data from the environment, identifying objects in the same IoT system for the corporation purpose, actuating based on the data gathered by sensors, and communicating with human interactions with the device.
- Communications network layer: also called transmission layer, Smart IoT devices must interact with an external system if they are not entirely autonomous. This kind of communication commonly utilizes a wireless technology. This layer contains four sublayers, which are listed below:
  - Access network sublayer: A ubiquitous access area is created for the "things" layer by Access Network. The network functions as a means of connecting subscribers with the service providers. It provides end users with the ability to have a communications infrastructure that includes wireless communication, satellite communication, and mobile communication. Many types of network technologies can be used by the access network such as mobile ad hoc network (MANET), Wi-Fi network, WiMAX, and ZigBee.
  - Gateways and backhaul network sublayer: also called core network sublayer, it's a communication system that serves numerous smart objects within a certain region, where each area is surrounded by a shared gateway. The gateway has one-to-one connectivity with all the smart objects. The gateways' main function is to send information collected to the headend central station for processing. On another hand, As an IP router, this gateway relays messages between two different IP networks.
  - Network transport sublayer: to support the many types of IoT devices and the different media to utilize, the network and transport layer protocols must be implemented and cooperate with each other such as IP and TCP.
  - IoT network management sublayer: It is necessary to implement more protocols to enable the headend apps to communicate data with the sensors such as CoAP and MQTT.
- Applications layer: To process the acquired data at the third layer, an application must make intelligent decisions and direct the "things" or other systems to adjust to the assessed surrounding conditions.

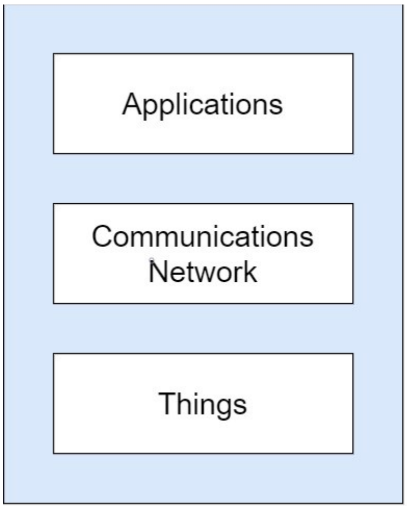

Fig. 4. Simplified IoT Architecture; IoT Functional Stack

4.1.2. IoT Data Management and Compute Stack

This IoT architecture deals with the collected data management and control. One of the major problems with IoT systems is the huge amount of data that IoT sensors create. As the number of IoT devices increases, these devices collected data also, tremendously increases. Obviously, standard network design is incapable of handling big data, thus new architecture should be employed to handle this issue. Therefore, the researchers have introduced using Cloud-based IT architecture (as appears in Figure 5) to manage the huge amount of data generated by IoT devices. In this architecture, it should be clear that the processing site is external to IoT smart devices. A cloud-based processing environment is the ideal place for this operation. However, connecting to the cloud application is mandatory for IoT devices, while data processing is done on that application. With view over all the IoT nodes, cloud applications today and in the future can handle all the insights.

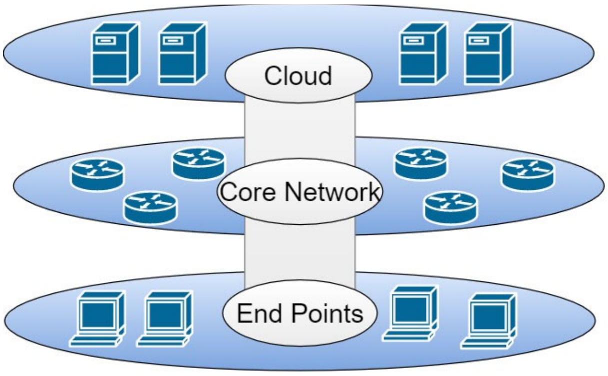

Fig. 5. Cloud-Based IT Architecture

But this architecture has several shortcomings such as, the amount of data, the range of connected items, and the increased efficiency constraints drive the demand for data analysis farther into the IoT system. These conditions are eliminating the delay of getting response from the cloud nodes, ensuring efficient use of network bandwidth, and improving local efficiency, especially when analyzing local highly sensitive data. Therefore, the researchers introduced using fog computing so that the collected data can be quickly processed and analyzed and in efficient way. As shown in Figure 6, In [33], a new layer has been added to the previously discussed architecture. However, In [35], the author has introduced a three layer fog-based IoT architecture as shown in Figure 7.

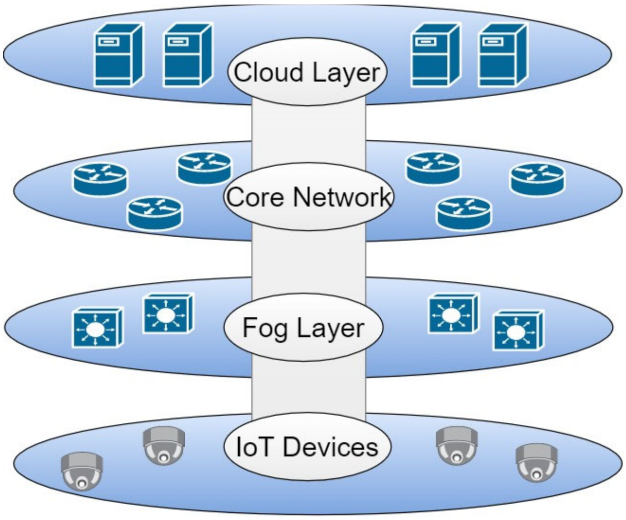

Fig. 6. Fog-Based IoT Architecture

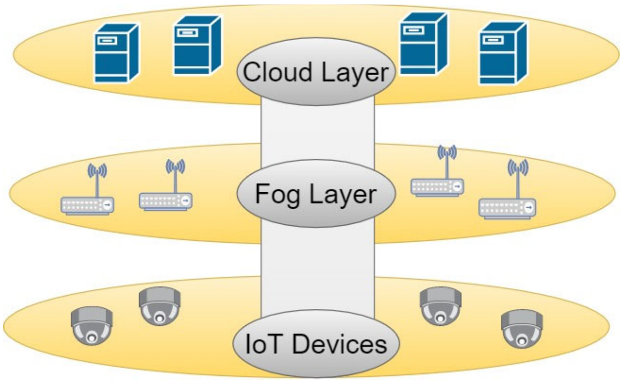

Fig. 7. Three Layers Fog-based IoT Architecture

Due of the near proximity of fog devices to edge devices, they are often installed as close to IoT endpoints as feasible. Because of its proximity to the sensors, the fog node has awareness of contextual information awareness of the sensors it is monitoring. Fog nodes can respond more rapidly and more effectively to IoT network events due to having awareness of context.

Fog layer can help in monitoring, controlling, and analyzing devices. There is no need to wait cloud-based central analytics and application servers to provide information to those devices. However, for more local computing acceleration (means to apply the analysis and management, locally at the IoT layer level), The researchers have suggested that IoT computation to be applied, in most cases on IoT devices. Figure 8 shows the introduced three layers edge-based IoT architecture or "IoT Data Management and Compute Stack"[33].

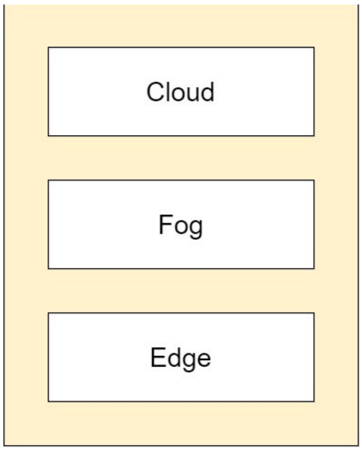

Fig. 8. Three Layers Edge-Based IoT Architecture

4.2. Four Layers IoT Architecture

Many four layers based IoT architectures have been introduced in the field of IoT research. However, to the best of our knowledge, the superior, well known, and trusted architecture is the one which supports the previously mentioned three layers IoT architecture or the IoT core functional stack. Researchers have introduced a new four layers IoT architecture [36]. The new architecture contains the same three layers as the three layers one, but it adds an additional layer which is support layer. Figure 9 depicts the new architecture layers. Three layers have the same functionality as in the previous basic architecture. The new support layer adds a type of security against network attacks. One of the security services introduced by this layer is authentication which is implemented using secret keys [1].

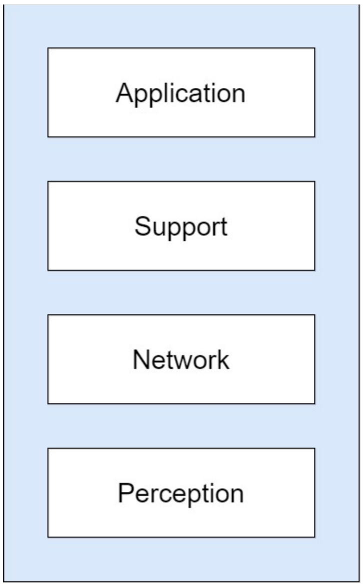

Fig. 9. Four Layers IoT Architecture

4.3. Five Layers IoT Architecture

IoT links “smart” things and connects many of them. The enormous traffic produced in this way has forced a high need for massive storage capacity and loads of computing power. This leads to new challenges in the areas of security. Therefore, Researchers have introduced a new five layers IoT architecture as shown in Figure 10 [37-39]. Three layers are the same layers which are existing in the previous three layers architecture which are Perception, Network and Application layers. The newly proposed two layers are Business and Processing layers. The specification for these two layers functions are as follows:

1. Processing Layer: in addition, called as middleware layer. It gathers data that is transmitted over the network layer. It uses the gathered information to do its own processing. It's charged with eliminating extraneous information, getting rid of the non-significant data, and extracting the valuable information. Additionally, it treats the issues related to IoT and big data to eliminate attacks which penetrates the huge amount of the received information from the network layer [40].
2. Business Layer: This layer of the IoT system manages the higher-level applications and service functions. The application-related data is being used to generate business models, flow-charts, graphs, and profit models. This helps users to deal with the smart objects which supports IoT feasibility. Other duties of this layer include treating the problems that concern users' privacy and security [40].

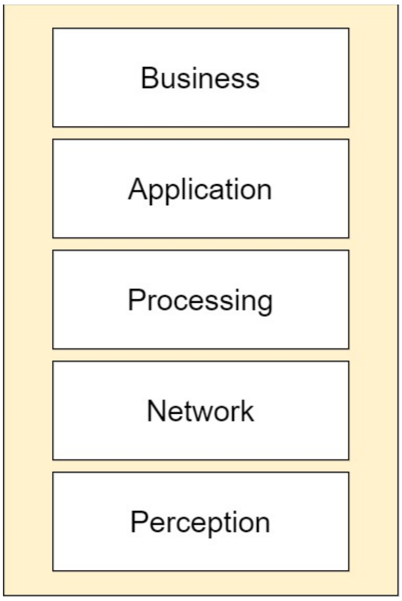

Fig. 10. Five Layers IoT Architecture

5. IoT Architectural challenges and existing solutions

IoT is expected to revolutionize Internet connectivity. There are several business prospects enabled by the Internet of Things, including in the domains of e-health, smart cities, and smart homes. Multiple long-range, short-range, and personal-area wireless networks and technologies are incorporated into the design of IoT applications. As a result, IoT will be ubiquitous, posing numerous challenges. Service providers and application developers can execute their services more efficiently if these issues are addressed carefully. This section introduces a review of the primary research challenges facing the Internet of Things [2, 16, 41]:

1. Scalability: IoT devices are continuously increasing in number. According to estimates, the number of IoT devices will approach or perhaps exceed 50 billion by 2020 [41]. To react to changing environmental conditions, the IoT system must be scalable. Scalability refers to the system's ability to respond to changing requirements [42]. The fundamental goal of making the IoT system scalable is to fulfill shifting demands as people's interests and environmental conditions change over time. Furthermore, scalability aids the system's efficiency by preventing any performance concerns that may develop as the system grows. One solution for this challenge is proposed by [43]. Using a virtual service supply model, the authors introduced the IoT PaaS platform.
2. Security: Security is becoming a more challenging issue for IoT as more "things" become connected to other "things" and people. Your attack surface has grown significantly, and if a device is compromised, its

connectivity becomes a serious problem. A hacked device can be used to conduct attacks on other computers and devices. IoT security is also present in almost every aspect of IoT.

3. Privacy: Many of the data collected by sensors in our daily lives will be specific to individuals and their actions as they become more prevalent in our lives. This data can include health information, shopping habits, and retail transactions. Therefore, this data has economic worth for corporations.
4. Big data and data analytics: The Internet of Things, with its huge number of sensors, will cause a data flood that will need to be dealt with. If this data can be analyzed efficiently, it will yield valuable information and insights. Massive amounts of data entering from many sources and in varied forms provide a difficulty, as does doing so in a timely manner and evaluating them.
5. Interoperability: Because of the necessity to handle a high number of heterogeneous items from many platforms, end-to-end interoperability is another problem for the Internet of Things. Both application developers and manufacturers of Internet of Things devices should take interoperability into account for the purpose of ensuring service delivery to all clients independent of the hardware platform requirements. IoT programmers should design their apps so that new features can be added without causing issues or causing existing features to be lost.
6. Availability: The IoT's availability must be implemented at the hardware and software stages to offer clients services from any location at any time. In the Internet of Things, software availability refers to the capacity of the apps to provide services concurrently to everyone in various locations. In the context of the Internet of Things, hardware availability means that there are always devices available that are consistent with the IoT's features and protocols. Provide redundancy for essential devices and services as a means of ensuring high availability for IoT services is suggested as a solution for this challenge [44].
7. Reliability: Reliability is defined as the ability of a system to perform as expected given its design specifications [44]. Reliability's goal is to make the supply of IoT services more successful. When it comes to emergency response applications, reliability is much more important and comes with more stricter criteria [45]. Reliability must be built into both the software and hardware components of the Internet of Things from the very beginning. The underlying communication must be reliable for the Internet of Things to work efficiently. [45] proposes a reliability scheme at the transmission level to minimize packet losses in IoT environments. Providing services to smart devices need reliable service composition. In [46] and [47] the researchers proposed a solution model for reliability over IoT.
8. Mobility: Because most services are expected to be supplied to mobile customers, IoT implementations must also address the issue of mobility. An essential premise of the Internet of Things is that consumers can stay connected to their desired services while on the move. When moving from one gateway to another, mobile devices may experience service interruptions. [47] use, as a solution for mobility, caching and tunneling to provide service continuity in its resource mobility system.
9. Management: The development of new lightweight management protocols is required to manage trillions of IoT smart devices. Growing IoT deployments can be aided by better management of IoT devices and applications [48]. Observing the machine-to-machine (M2M) connection of IoT objects, for instance, is critical to always ensuring connectivity for on-demand service provisioning. Solutions for this challenge are represented in introducing effective management protocols such as Light-weight M2M (LWM2M), The NETCONF Light protocol [49] and The MASH IoT Platform which gives you real-time access to IoT asset management on your smartphone.

6. Conclusion

IoT, a new concept that seeks to link numerous smart gadgets, technologies, and applications in order to improve the quality of our lives, is swiftly making its way into our daily lives. The IoT is expected to allow for the automation of all aspects of our daily lives. Therefore, the basic concepts in IoT should be well analyzed and studied for getting benefit from such technology with minimum problems. This survey provides a review for the most recent IoT related works and displays a comprehensive discussion for IoT definitions, characteristics, and main functional components. Also, it provides a very deep discussion for IoT architectures and their related specifications. In addition, this survey discusses the most recent IoT challenges and the existing solutions.

References

[1] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors,* vol. 18, p. 2796, 2018.

[2] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the Internet of things (IoT) in smart logistics: A comprehensive survey," *IEEE Internet of Things Journal,* 2021.

[3] W. a. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal*

of Network and Computer Applications, vol. 163, p. 102663, 2020.

[4] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Internet of Things for Agricultural Applications: The State-of-the-art," *IEEE Internet of Things Journal,* 2021.

[5] I. U. Khan, M. Shahzad, and M. Hassan, "Internet of things (IoTs): applications in home automation," *IJSEAT,* vol. 5, pp. 79-84, 2017.

[6] M. H. Memon, W. Kumar, A. Memon, B. S. Chowdhry, M. Aamir, and P. Kumar, "Internet of Things (IoT) enabled smart animal farm," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 2067-2072.

[7] Z. Bi, Y. Liu, J. Krider, J. Buckland, A. Whiteman, D. Beachy, *et al.*, "Real-time force monitoring of smart grippers for Internet of Things (IoT) applications," *Journal of Industrial Information Integration,* vol. 11, pp. 19-28, 2018.

[8] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi, and H. T. Kadhum, "An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT)," *Wireless Personal Communications,* vol. 114, 2020.

[9] D. Sharma and R. Tripathi, "Performance of Internet of Things (IOT) Based Healthcare Secure Services and Its Importance: Issue and Challenges," in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020, pp. 1-4.

[10] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*, ed: Springer, 2019, pp. 27-51.

[11] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems,* vol. 92, pp. 265-275, 2019.

[12] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks,* vol. 144, pp. 17-39, 2018.

[13] J. Blythe and S. Johnson, "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," in *Living in the Internet of Things: Cybersecurity of the IoT-2018*, 2018, pp. 1-7.

[14] M. Erfanmanesh and A. Abrizah, "Mapping worldwide research on the Internet of Things during 2011-2016," *The Electronic Library,* 2018.

[15] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. Da Xu, *et al.*, "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Transactions on Industrial Informatics,* vol. 10, pp. 2180-2191, 2014.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials,* vol. 17, pp. 2347-2376, 2015.

[17] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities," *IEEE Internet of Things Journal,* 2021.

[18] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," in *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, 2012, pp. 1-7.

[19] L. Tan and N. Wang, "Future internet: The internet of things," in *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, 2010, pp. V5-376-V5-380.

[20] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 2013.

[21] K. S. Mohamed, *The era of internet of things*: Springer, 2019.

[22] S. Hendriks, "Internet of Things: How the world will be connected in 2025," 2016.

[23] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University-Computer and Information Sciences,* vol. 30, pp. 291-319, 2018.

[24] A. Bahga and V. Madisetti, *Internet of Things: A hands-on approach*: Vpt, 2014.

[25] S. Sebastian and P. Ray, "Development of IoT invasive architecture for complying with health of home," *Proceedings of I3CS, Shillong,* pp. 79-83, 2015.

[26] E. de Matos, R. T. Tiburski, C. R. Moratelli, S. Johann Filho, L. A. Amaral, G. Ramachandran, *et al.*, "Context information sharing for the Internet of Things: A survey," *Computer Networks,* vol. 166, p. 106988, 2020.

[27] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: state of the art," *Robots and Sensor Clouds,* pp. 55-75, 2016.

[28] M. Gigli and S. G. Koo, "Internet of things: services and applications categorization," *Adv. Internet Things,* vol. 1, pp. 27-31, 2011.

[29] V. Aleksandrovičs, E. Filičevs, and J. Kampars, "Internet of Things: Structure, Features and Management," *Information Technology & Management Science (Sciendo),* vol. 19, 2016.

[30] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications,* vol. 42, pp. 120-134, 2014.

[31] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment," *Computer Communications,* 2020.

[32] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review,* vol. 38, p. 100312, 2020.

[33] C. Press, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things," 2017.

[34] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience,* vol. 32, p. e4946, 2020.

[35] A. Yousefpour, G. Ishigaki, R. Gour, and J. P. Jue, "On reducing IoT service delay via fog offloading," *IEEE Internet of Things Journal,* vol. 5, pp. 998-1010, 2018.

[36] D. Darwish, "Improved layered architecture for Internet of Things," *Int. J. Comput. Acad. Res.(IJCAR),* vol. 4, pp. 214-223, 2015.

[37] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *2010*

3rd international conference on advanced computer theory and engineering (ICACTE), 2010, pp. V5-484-V5-487.

[38] Z. Alansari, N. B. Anuar, A. Kamsin, M. R. Belgaum, J. Alshaer, S. Soomro*, et al.*, "Internet of things: infrastructure, architecture, security and privacy," in *2018 International conference on computing, electronics & communications engineering (iCCECE)*, 2018, pp. 150-155.

[39] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering,* vol. 2017, 2017.

[40] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," *Journal of Network and Computer Applications,* vol. 49, pp. 112-127, 2015.

[41] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*: Cisco Press, 2017.

[42] H. F. Atlam, R. Walters, and G. Wills, "Internet of things: state-of-the-art, challenges, applications, and open issues," *International Journal of Intelligent Computing Research (IJICR),* vol. 9, pp. 928-938, 2018.

[43] F. Li, M. Vögler, M. Claeßens, and S. Dustdar, "Efficient and scalable IoT service delivery on cloud," in *2013 IEEE sixth international conference on cloud computing*, 2013, pp. 740-747.

[44] D. Macedo, L. A. Guedes, and I. Silva, "A dependability evaluation for Internet of Things incorporating redundancy aspects," in *Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control*, 2014, pp. 417-422.

[45] N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, "Reliability for emergency applications in internet of things," in *2013 IEEE International Conference on Distributed Computing in Sensor Systems*, 2013, pp. 361-366.

[46] L. Li, Z. Jin, G. Li, L. Zheng, and Q. Wei, "Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach," in *2012 IEEE 19th International Conference on Web Services*, 2012, pp. 584-591.

[47] F. Ganz, R. Li, P. Barnaghi, and H. Harai, "A resource mobility scheme for service-continuity in the Internet of Things," in *2012 IEEE International Conference on Green Computing and Communications*, 2012, pp. 261-264.

[48] M. Rajan, P. Balamuralidhar, K. Chethan, and M. Swarnahpriyaah, "A self-reconfigurable sensor network management system for internet of things paradigm," in *2011 International Conference on Devices and Communications (ICDeCom)*, 2011, pp. 1-5.

[49] V. Perelman, M. Ersue, J. Schönwälder, and K. Watsen, "Network configuration protocol light (NETCONF Light)," *Internet Eng. Task Force (IETF), Fremont, CA, USA, Network,* 2012.