Proceedings of Machine Learning Research 1–4

Protocol for IoT Network Research and Development ref: http://paper.ijcsns.org/07$_{b}ook/202203/20220307.pdf$

Bagiya Lakshmi S BAGIYALAKSHMI59@GMAIL.COM
Shiv Nadar University, chennai

Abstract

It is always important to attract new researchers to work on this area and be a part of it. The best way to attract researchers to work in any research area and have their interest is to give them a clear background and roadmap about it. In this way, researchers can easily find a deep point to start their research based on their interest. This paper presents an overview and roadmap about IoT technologies from the most five vital aspects: IoT architecture, communication technologies, type of IoT applications, IoT applications protocols and IoT challenges.

Key contributions/ideas from the author

The authors has given the definition for IoT, How IoT technologies played vital role in simplifying the work. This paper presents an overview and roadmap about IoT technologies from the most five vital aspects. Based on these aspects, a researcher might be able to create a clear plan to start their research. The first aspect is the fundamental of the IoT structure and its layers. The second aspect is related to the communication technologies that link IoT devices in a network. The third aspect is about selecting an environment area for deploying IoT devices to provide services to endusers, based on the IoT application types. The fourth aspect is related to the communication protocols at the application layer. The final aspect concerns the challenges that IoT systems face.

They gave the basic archtiture diagram of IoT. They say that IoT architecture contains four components namely **Preception layer, Middleware layer, Application layer and Network layer**.

They have given detailed explanations of various communication technologies.And also IoT applications have been explained breifly. Let's dive into Architecture of IoT.

1. Background and Roadmap for IoT (IoT Architecture)

The IoT architecture can be categorised into four main layers: perception layer, network layer, middleware layer and application layer. The main objective of this classification is to assist IoT developers in identifying the area of any technical issues based on this classification.

1.1. The Perception Layer

The perception layer is the first layer that the IoT system begins to execute. It is likely same as the physical layer in the OSI network. This layer is responsible for collecting and exchanging data from the surrounding areas in the physical world. Sensors and actuators are the two primary items that can detect and sense the changes in the real-world environment, for example measuring the temperature of a room and then sending the collected data to the next layer, which is the network layer for connectivity. **Sensors**: A sensor is an electronic device that can detect and sense the physical environment such as measuring the temperature by using a thermistor. **Actuators**: An actuator is a machine that can move the IoT devices from one state to another state such as switching the light off or on by using a Rely device . **IoT Data**: The IoT objects such as sensors and actuators generate two types of data. Measurement data is when sensors generate data to detect and sense the events in real world of the surrounding environment such as temperature, humidity etc. Context-data provides information about the description of an object and its condition such as battery life, latency, etc. and sends this information to the users. IEEE 802.15.4 was introduced in 2003 as a wireless personal area network standard for the physical layer and MAC, which is preferable in cases where high power and high-rate wireless communication systems are not required . It covers small areas only, and the maximum transmission range that it can reach is about 100m

1.2. The Network Layer

The network layer is the second layer in the IoT architecture. It acts as the brain of the IoT systems [11]. The primary aim of the network layer is to gather data from the perception layer and transmit this information to the middleware layer for further analysis and processing. Internet getaways such as WiFi, RFID, etc. operate at this layer to execute different network communication services . In this section, the communication technologies, routing, and the architecture of IoT networks will be discussed.

Communication technologies can be defined as the mechanism type that links IoT devices in a network for the purpose of data transmission. There are various communication mechanisms in the market, such as WiFi. In this section, seven communication mechanisms with their description are listed below. There are more than these seven in the market; however, we believe the following seven are the most important.

Sigfox: Sigfox could be considered as the first global IoT network in which IoT devices can transmit data without the need to install any network connections. The management of transmitting data between IoT devices proceeds in the cloud by the software-based communication that the Sigfox offers. This management leads to minimising the cost of connectivity and power consumption [13]. The Sigfox network architecture consists of three majors' parts: base stations, IoT devices and central networks. The communication protocol in Sigfox is designed to send small messages (0 to 12 bytes).

NB-IOT: Researchers are giving more concern to the NBIoT due to its low-cost, low power consumption, longdistance indoor coverage. It is the most popular choice for most of the IoT nodes [15]. The bandwidth of NB-IoT for both uploading and downloading is the best choice for lowcost devices, and it is about 180 kHz, which is considered as a low-frequency bandwidth. NB-IoT provides connectivity for IoT devices over long-distances, and the maximum coverage that it can serve is about 15km. The latency in NBIoT is preferable in many IoT applications, which is about 10ms.

Zigbee: Zigbee has been launched as a wireless communication protocol. In comparison with other communication protocols, the cost of establishing a ZigBee network is low. It covers small areas with a low data rate and can provide service monitoring in small areas, such as homes . The coverage of a Zigbee network is the same as a WiFi network because both provide the same bandwidth, which is 2.4 GHz.

NFC: Near Field Communication was introduced as wireless communication technology to provide connectivity in a very small area. NFC has added value and brings many advantages to the IoT technology. One of its remarkable gains is in the way of communications, since it does not require any pairing to set up, so it is much easier than Bluetooth, which requires paring . The main disadvantage of NFC is the short coverage, which is about 4 cm .

Radio Frequency Identification: RFID can be classified as one of the wireless communication technologies. The primary objective of RFID is to collect data from the surrounding areas in a limited range from 1m to 12m by broadcasting radio signals and it processes this information to implement services such as monitoring, tracking, etc. RFID tags and RFID readers are the two main parts of the RFID system; tags such as cards collect information by broadcasting radio waves, whereas readers act as a brain to execute processing.

Bluetooth: Bluetooth technology can be utilised to provide connectivity for IoT devices in a limited range. The maximum range that Bluetooth can cover is about 10m.

1.3. The Middleware Layer

The middleware layer is the third layer in the IoT architecture. It analyzes and stores the received data from the network layer. It works as a bridge to link the IoT system to the computing systems and databases for further processing. It is responsible for preparing the data to be utilized in the application layer. Machine learning and artificial intelligence systems might be used at this layer to transform the collected data into valuable information to support the system in the decision-making process at the application layer.

]

1.4. The Application Layer

The application layer is the top layer in the IoT architecture and its main purpose to provide services for the end-users . This layer generates the processed data from the middleware layer to meet the QoS in IoT applications in various cases to deliver services to the end-user. It works as a chain to enable end-users to use IoT applications such as smart homes, smart cities, smart industries, etc. End-user can access these IoT applications through internet-enabled devices such as smartphone, laptop, television, etc.

IoT in healthcare: The main objective of proposing IoT is to provide more convenient life for humans by organizing their basic tasks. The treatment of patients in the healthcare systems can be enhanced when the IoT devices utilized in the system [34]. This can be achieved by combining the IoT sensors with the health monitoring gadgets used by patients to provide further analyses. These sensors gather information about the status of patients and send this information to the internet for further processing. Doctors and nurses use the analysed and processed data to monitor the status of patients remotely [35]. Moreover, healthcare systems might witness significant improvements when applying IoT systems in the environment regarding data accuracy when reporting the patient's status like their temperature and blood pressure to doctors and nurses compared to writing the data manually where mistakes might happen.

IoT in smart buildings: The smart building has been established to provide more convenient living arrangements for residents. The IoT systems can monitor and control the appliances in building like remote monitoring via Internet [36]. Switching appliances off and on remotely through smartphone apps can play an important role in reducing the power consumption as the control of these appliances can be done easily. IoT systems can also provide safety monitoring to protect residents from any external risks by using cameras and alarm systems effectively [37]. In addition, smart buildings might play an important role not directly in decreasing the conflicts between the family members because everything in the house can be handled easily. For instance, an intelligent vacuum can clean the living room automatically, which will allow the family members to have more time to set together in a clean place without making any effort.

IoT in transportation: Nowadays, the demand for the public transportation system (PTS) has risen recently due to the significant increase in the number of daily trips because of growing urbanization. The demand for PTS in urban cities is high, and the traditional PTS has achieved significant contributions in terms of reducing air pollution, traffic accidents and road congestion [38]. One of the main disadvantages of using public transportation is the time that passengers spend in stations waiting for buses and trains. Knowing the location of buses and the exact arrival time will encourage commuters to use public transportation in their daily life, and this can be achieved by integrating the IoT systems into PTS [39]. From an economic perspective, the income of public transportation might increase when integrating IoT systems in their environment because the number of passengers will increase when the trips are scheduled accurately.

IoT in smart energy: The IoT sensors can be integrated with electronic gadgets to measure and analyse the power consumption of these gadgets for further processing and monitoring [40]. Monitoring power consumption effectively can play an essential role in reducing the cost of bills. It also benefits to the environment in several ways such as minimizing the air pollution. Electric companies will also benefit, as this monitoring will decrease the pressure and load on these companies in terms of reading and reporting consumers' bills [41]. All that will lead to increase the confidence between the electric companies IoT in agriculture: Establishing the IoT technology in the agriculture environment can play an essential role in improving the farming environment. Farmers can easily monitor their crop yield when effectively using IoT devices [42]. This technology will bring several benefits to the agriculture environment in term of many aspects. It helps farmers to limit the time to produce more with less effort. The performance of the production can be examined after generating the data from the IoT sensors [43]. The IoT sensors will assist in increasing the success of crop production as these sensors can make destinations in early stages; for instance, greenhouse agriculture can be closed directly when sensors detect heavy rain.

IoT in industry: IoT systems in industry can handle and control the manufacturing processes at the real-time without any delays. The M2M communications can play an essential role in reducing the number of workers in industries, which minimize the cost of manufacturing. Integrating IoT systems into various industries has enhanced efficiency, improved the QoS as well as maintenance services. Supervisors in industries can easily examine the performance of manufacturing by pulling the data from the IoT sensors [44]. From an economic perspective, the number of industries in the country might increase as traders can establish new industries with less cost compared to the past, as the number of workers will decrease when integrating IoT systems into their environment.

2. IoT Challenges

Researchers are continuously working to overcome the challenges faced by IoT technology.

2.1. Security

Securing IoT systems is one of the most critical challenges that experts and researchers have been trying to overcome. Exchanging data among IoT nodes should be protected from any external attack to create a confidential IoT environment . Protecting IoT devices will encourage consumers to utilise the IoT systems in their homes, since they know their privacy is protected

2.2. Limited power

Due to the massive rise in the number of IoT devices, there is now a storage demand to promote IoT networks' energy efficiency. In addition to the number of IoT devices, researchers have proposed several complex algorithms to improve other parameters such as security, data rate and bandwidth, which can contribute to increasing the workload and consuming more power . To the best of our knowledge, researchers have to focus on three network areas to reduce the power consumption in the IoT devices. These areas are the routing and clustering in the WSNs, and the fog computing services in the IoT networks.

2.3. Availability

As the IoT devices require real-time processing, the devices should be available all the time to avoid delays. In some cases, a service might not be available for a user when he/she sends a request, which might negatively impact the work process, and leading to poor outcomes . Several reasons might affect the IoT systems and make it unavailable and not ready for use. These reasons can be like sensors ageing, dead battery, and more . Researchers have to be aware of the quality and the lifetime of the sensors and hardware devices to make the system available as long as they can,

2.4. Scalability

Scalability is the ability of the IoT systems to handle the growth in the number of IoT devices while overcoming the challenges associated with that growth . Horizontal sensing and vertical sensing are the two main features that have to be enhanced to improve IoT systems' scalability. Adding more devices and nodes to the network belongs to the horizontal sensing, whereas increasing the capacity of a network by adding more resources such as CBU, RAM, and Power belongs to vertical sensing . Achieving a high level of scalability will increase the IoT devices' chance to become successful in the future and to be more reliable. Researchers must focus on finding a way to add more resources, such as CPU and IoT devices without affecting the system's interoperability. A system is called interoperable when multiple IoT sensors can work together in the right place and time to perform functions without any issues.

2.5. Maintenance

The cost of maintaining IoT devices might be more expensive than establishing them. It is vital in IoT to have a resiliency system in which nodes can recover and fix errors without any interactions to reduce the cost of maintenance. There are various ways to reduce the cost of maintenance in the IoT environment. The deployment of the IoT devices has to be set in such a way that they can easily be located when they need to be fixed. It is vital to be aware of the IoT devices' range as these devices work with a limited range to avoid damages and incorrect results. The quality of the IoT sensors has to be high to avoid maintains as much as possible.

3. Conclusion

This paper aims to attract more new researchers and developers to start their research in IoT networks. This paper has provided researchers with a comprehensive background about the area in terms of five main aspects: IoT architecture, communication technologies, type of IoT applications, IoT applications protocols and IoT challenges. Future studies will investigate and analyse IoT networks' five most vital challenges individually to help researchers determine their paths when targeting a challenge from the five mentioned challenges.