Investigating the structure and challenges of the Internet of Things

Zhila mohamadian, Seyed hossein hoseinnejd

Department of Computer Engineering. Ahar Branch, Islamic Azad University, Ahar, Iran

Abstract

Advances in wireless networking and communications technologies have led to the emergence of Internet-related innovations known as the Internet of Things.The Internet of Things is defined as a pattern in which objects equipped with sensors and processors communicate with each other to pursue a meaningful goal.The IoT is able to integrate and transparently integrate a large number of heterogeneous and diverse end systems by providing free access to select subset of data to improve a range of digital services.In this paper, we survey protocols, and applications in this new emerging area ,then analyze the challenges of the IoT .

1. Introduction

Today, the IoT is a new topic in various fields of research, academia, industry and government, and has become one of the most influential technologies in the modern world.

The definition of the Internet of Things seems to be challenging, and this challenge is due in part to the diversification of the domain and the variety of services that are anticipated for it. In fact, there are various groups, including academics, researchers, innovators, and large corporations that have defined the term.

It should be said that almost any physical object, if it is possible to connect to the Internet so that it can exchange information on the network without the need for human intervention or can be controlled through the Internet, can become an Internet of Things device.

Sensors and actuators are devices, which help in interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it.

The storage and processing of data can be done on the edge of the network itself or in a remote server. If any preprocessing of data is possible, then it is typically done at either the sensor or some other proximate device. The processed data is then typically sent to a remote server. The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to limitations of size, energy, power, and computational capability. As a result the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy. Along with the challenges of data collection, and handling, there are challenges in communication as well. The communication between IoT devices is mainly wireless because they are generally installed at geographically dispersed locations. The wireless channels often have high rates of distortion and are unreliable. In this scenario reliably communicating data without too many retransmissions is an important problem and thus communication technologies are integral to the study of IoT devices

2.uses of the IoT

What are the uses of the Internet of Things? There are no restrictions on IoT applications and this topic is used in transportation, agriculture, smart greenhouse, medicine, online medical equipment, surveillance and security, surveillance cameras, training and business. This issue is fully addressed below. Just as the advent of the Internet has affected a wide range of users, the Internet of Things has affected and will continue to affect a wide range of users. Depending on the scale of the connection and the number of devices involved, IoT also has significant and specific applications for a particular user.

IoT in factories: With IoT for factories, manufacturers can automate duplicate tasks in each part of the entire production process. The information collected by sensors embedded in factory devices can be used to design solutions to optimize the production line.

IoT for individuals and homes: People use IoT devices through coverage technologies such as smartwatches, health trackers, and devices that help them receive and collect information instantly. By applying the Internet of Things b. Various aspects of connected homes can be accessed remotely and controlled by the homeowner through a computer or a smart handheld, smart phone, tablet, and more .

IoT in education: The Internet of Things can make education more accessible in a variety of ways.

There are endless opportunities to integrate IoT solutions into the school environment. Some of these cases in

Are further expressed. It is worth noting that these cases serve as a solid basis for building a deeper understanding of Internet use

Objects are considered in education. From the Internet of Things you can learn foreign languages, smart and connected classes

Task, axis, education for students with disabilities and exceptional education, physical education, classroom security, supervision

Classes using "video as sensor" technology (Sensor a as Video,) Automation of attendance monitoring,

He used students' physical and mental health, home learning, and "Personalized Learning."

2-1 Smart Cities

Smart Transport.

Smart transport applications can manage daily traffic in cities using sensors and intelligent information processing systems. The main aim of intelligent transport systems is to minimize traffic congestion, ensure

(1) Traffic surveillance and management applications: vehicles are connected by a network to each other, the cloud, and to a host of IoT devices such as GPS sensors, RFID devices, and cameras. These devices can estimate traffic conditions in different parts of the city. Custom applications can analyze traffic patterns so that future traffic conditions can be estimated.

(2) Applications to ensure safety: smart transport does not only imply managing traffic conditions. It also includes safety of people travelling in their vehicles, which up till now was mainly in the hands of drivers. There are many IoT

applications developed to help drivers become safer drivers. Such applications monitor driving behavior of drivers and help them drive safely by detecting when they are feeling drowsy or tired and helping them to cope with it or suggesting rest [1, 2]. Technologies used in such applications

are face detection, eye movement detection, and pressure detection on the steering (to measure the grip of the driver's hands on the steering). A smartphone application, which estimates the driver's driving behavior using smartphone sensors such as the accelerometer, gyroscope, GPS, and camera, has been proposed by Eren et al. [4]. It can decide whether the driving is safe or rash by analyzing the sensor data.

(3) Intelligent parking management (see Figure 9): in a smart transportation system, parking is completely hassle free as one can easily check on the Internet to find out which parking lot has free spaces. Such lots use sensors to detect if the slots are free or occupied by vehicles.This data is then uploaded to a central server

(4) Smart traffic lights: traffic lights equipped with sensing, processing, and communication capabilities are called smart traffic lights. These lights sense the traffic congestion at the intersection and the amount of traffic going each way. This information can be analyzed and then sent to neighboring traffic lights or a central controller. It is possible to use this information creatively. For example, in an emergency situation the traffic lights can preferentially give way to an ambulance. When the smart traffic light senses an ambulance coming, it clears the path for it and also informs neighboring lights about it. Technologies used in these lights are cameras, communication technologies, and data analysis modules.

3. Architecture of IoT

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers.

3.1. Three- and Five-Layer Architectures. The most basic architecture is a three-layer architecture [4–5] as shown in Figure 1. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

(i) The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

(ii) The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

(iii) The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the fivelayer architecture, which additionally includes the

processing and business layers [4–6]. The five layers are perception, transport, processing, application, and business layers (see Figure 1). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

(i)The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

(ii) The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

(iii) The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further

Another architecture proposed by Ning and Wang [7] is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

4. Taxonomy

The first architectural component of IoT is the perception layer. It collects data using sensors, which are the most important drivers of the Internet of Things [8]. There are various types of sensors used in diverse IoT applications. The most generic sensor available today is the smartphone. The smartphone itself has many types of sensors embedded in it [9] such as the location sensor (GPS), movement sensors (accelerometer, gyroscope), camera, light sensor, microphone, proximity sensor, and magnetometer. These are being heavily used in different IoT applications. Many other types of sensors are beginning to be used such as sensors for measuring temperature, pressure, humidity, medical parameters of the body, chemical and biochemical substances, and neural signals. A class of sensors that stand out is infrared sensors that predate smartphones. They are now being used widely in many IoT applications: IR cameras, motion detectors, measuring the distance to nearby objects, presence of smoke and gases, and as moisture sensors

Subsequently, we shall discuss related work in data preprocessing. Such applications (also known as fog computing applications) mainly filter and summarize data before sending it on the network. Such units typically have a little amount of temporary storage, a small processing unit, and some security features. The next architectural component that we shall discuss is communication. We shall discuss related work on different communication technologies used for the Internet of Things. Different entities communicate over the network [10–11] using a diverse set of protocols and standards. The most common communication technologies for short range low power communication protocols are RFID (Radio Frequency Identification) and NFC (Near Field Communication). For the medium range, they are Bluetooth, Zigbee,

and WiFi. Communication in the IoT world requires special networking protocols and mechanisms. Therefore, new mechanisms and protocols have been proposed and implemented for each layer of the networking stack, according to the requirements imposed by IoT devices. We shall subsequently look at two kinds of software components: middleware and applications. The middleware creates an abstraction for the programmer such that the details of the hardware can be hidden.This enhances interoperability of smart things and makes it easy to offer different kinds of services [17]. There are many commercial and open source offerings for providing middleware services to IoT devices. Some examples are OpenIoT [21], MiddleWhere [22], Hydra [13], FiWare [14], and Oracle Fusion Middleware. Finally, we discuss the applications of IoT in Section 9. We primarily focus on home automation, ambient assisted living, health and fitness, smart vehicular systems, smart cities, smart environments, smart grids, social life, and entertainment.

5. Sensors and Actuators

All IoT applications need to have one or more sensors to collect data from the environment. Sensors are essential components of smart objects. One of the most important aspects of the Internet of Things is context awareness, which is not possible without sensor technology. IoT sensors are mostly small in size, have low cost, and consume less power. They are constrained by factors such as battery capacity and ease of deployment. Schmidt and Van Laerhoven [15] provide an overview of various types of sensors used for building smart applications.

5.1. Mobile Phone Based Sensors. With the increasing popularity of smartphones among people, researchers are showing interest in building smart IoT solutions using smartphones because of the embedded sensors.Some of the sensors inside a modern smartphone are as follows.

(1) The accelerometer senses the motion and acceleration of a mobile phone . The data patterns captured by the accelerometer can be used to detect physical activities of the user such as running, walking, and bicycling.

(2) The gyroscope detects the orientation of the phone very precisely. Orientation is measured using capacitive changes when a seismic mass moves in a particular direction

(3) The magnetometer detects magnetic fields. This can be used as a digital compass and in applications to detect the presence of metals.

(4) The GPS (Global Positioning System) detects the location of the phone, which is one of the most important pieces of contextual information for smart applications. The location is detected using the principle of trilateration [16]. The distance is measured from three or more satellites (or mobile phone towers in the case of A-GPS) and coordinates are computed.

(5) The light sensor detects the intensity of ambient light. It can be used for setting the brightness of the screen and other applications in which some action is to be taken depending on the intensity of ambient light. For example, we can control the lights in a room.

be used to draw inferences and take further action. 5.6. Actuators. Let us look at some examples of actuators that are used in the Internet of Things. An actuator is a device, which can effect a change in the environment by converting electrical energy into some

form of useful energy. Some examples are heating or cooling elements, speakers, lights, displays, and motors. The actuators, which induce motion, can be classified into three categories, namely, electrical, hydraulic, and pneumatic actuators depending on their operation. Hydraulic actuators facilitate mechanical motion using fluid or hydraulic power. Pneumatic actuators use the pressure of compressed air and electrical ones use electrical energy

6.IoT security

"Security" is one of the most important challenges of the Internet of Things. Sensors in many cases of very sensitive data such as they compile what the app store itself does. Keep this information secure to gain and maintain trust consumers are a very important issue. But so far the security of the information recorded by IoT devices is often very high It has been weak. Many IoT devices pay little attention to the basics of security, such as data encryption.

Defects in software - even in older, well-used code - are commonly discovered, but many IoT devices do not have the ability to patch, which means that they are always at risk. Hackers right now

Actively targets IoT devices such as "routers" and webcams; Because of their lack of inherited security,

Their hereditary ability to fall into the trap of massive patents has made it easy.

The current state of IoT technology makes it harder to trust in terms of security. Lack of IoT security such as lack of IoT security programming in organizations. Think of industrial systems that are connected to the Internet and without protection is abandoned, worrying. The Internet of Things (IoT) is like a bridge between the digital and physical worlds, and that means being hacked devices can have dire consequences in the real world. Meanwhile, the optional takeover of a driverless car,

It can be a very dangerous ending

7. Middleware

Ubiquitous computing is the core of the Internet of Things, which means incorporating computing and connectivity in all the things around us. Interoperability of such heterogeneous devices needs well-defined standards. But standardization is difficult because of the varied requirements of different applications and devices. For such heterogeneous applications, the solution is to have a middleware platform, which will abstract the details of the things for applications. That is, it will hide the details of the smart things. It should act as a software bridge between the things and the applications. It needs to provide the required services to the application developers [17] so that they can focus more on the requirements of applications rather than on interacting with the baseline hardware. To summarize, the middleware abstracts the hardware and provides an Application Programming Interface (API) for communication, data management, computation, security, and privacy. The challenges, which are addressed by any IoT middleware, are as follows: [17, 18, 19]. (1) Interoperability and programming abstractions: for facilitating collaboration and information exchange between heterogeneous devices, different types of things can interact with each other easily with the help of middleware services. Interoperability is of three types: network, semantic, and syntactic. Network interoperability deals with heterogeneous

interface protocols for communication between devices. It insulates the applications from the intricacies of different protocols. Syntactic interoperability ensures that applications are oblivious of different formats, structures, and encoding of data. Semantic interoperability deals with abstracting the meaning of data within a particular domain. It is loosely inspired by the semantic web.

(2) Device discovery and management: this feature enables the devices to be aware of all other devices in the neighborhood and the services provided by them. In the Internet of Things, the infrastructure is mostly dynamic. The devices have to announce their presence and the services they provide. The solution needs to be scalable because the devices in an IoT network can increase. Most solutions in this domain are loosely inspired by semantic web technologies. The middleware provides APIs to list the IoT devices, their services, and capabilities. In addition, typically APIs are provided to discover devices based on their capabilities. Finally, any IoT middleware needs to perform load balancing, manage devices based on their levels of battery power, and report problems in devices to the users.

(3) Scalability: a large number of devices are expected to communicate in an IoT setup. Moreover, IoT applications need to scale due to ever increasing requirements. This should be managed by the middleware by making required changes when the infrastructure scales.

(4) Big data and analytics: IoT sensors typically collect a huge amount of data. It is necessary to analyze all of this data in great detail. As a result a lot of big data algorithms are used to analyze IoT data. Moreover, it is possible that due to the flimsy nature of the network some of the data collected might be incomplete. It is necessary to take this into account and extrapolate data by using sophisticated machine learning algorithms .

(5) Security and privacy: IoT applications are mostly related to someone's personal life or an industry. Security and privacy issues need to be addressed in all such environments. The middleware should have built in mechanisms to address such issues, along with user authentication, and the implementation of access control.

(6) Cloud services: the cloud is an important part of an IoT deployment. Most of the sensor data is analyzed and stored in a centralized cloud. It is necessary for IoT middleware to seamlessly run on different types of clouds and to enable users to leverage the cloud to get better insights from the data collected by the sensors.

(7) Context detection: the data collected from the sensors needs to be used to extract the context by applying various types of algorithms. The context can subsequently be used for providing sophisticated services to users.

8.conclusion

The Internet of Things is a massive network of fixed or portable intelligent objects that are interconnected.

Different types of objects with different physical mobility, different processing capabilities, different communication capabilities, different communication protocols and even the personal preferences of their owners are studied in this topic. The Internet of Things has various issues such as the possibility of management, discovery of required services, heterogeneity, large scale,

etc.The technologies in the core infrastructure layers are showing signs of maturity. However, a lot more needs to happen in the areas of IoT applications and communication technologies. These fields will definitely mature and impact human life in inconceivable ways over the next decade.

References

[1] W. Hu, X. Hu, J.-Q. Deng et al., "Mood-fatigue analyzer: towards context-aware mobile sensing applications for safe driving,"in Proceedings of the 1st ACM Workshop on Middleware for Context-Aware Applications in the IoT (M4IOT '14), pp. 19–24, ACM, Bordeaux, France, December 2014.

[2] H. Singh, J. S. Bhatia, and J. Kaur, "Eye tracking based driver fatigue monitoring and warning system," in Proceedings of the India International Conference on Power Electronics (IICPE '10), pp. 1–6, New Delhi, India, January 2011.

[3] H. Eren, S. Makinist, E. Akin, and A. Yilmaz, "Estimating driving behavior by a smartphone," in Proceedings of the IEEE Intelligent Vehicles Symposium (IV '12), pp. 234–239, Madrid, Spain, June 2012

[4] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68– 90, 2015.

[5] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China, August 2010.

[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257–260, December 2012

[7] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.

[8] M. Swan, "Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0," Journal of Sensor and Actuator Networks, vol. 1, no. 3, pp. 217–253, 2012.

[9] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Communications Magazine, vol. 48, no. 9, pp. 140–150, 2010.

[10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[11] D. Zeng, S. Guo, and Z. Cheng, "The web of things: a survey," Journal of Communications, vol. 6, no. 6, pp. 424–438, 2011.

[12] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: a study ," International Journal of Compute

[13] M. Eisenhauer, P. Rosengren, and P. Antolin, "A development platform for integrating wireless devices and sensors into ambient intelligence systems," in Proceedings of the 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops (SECON Workshops '09), pp. 1–3, IEEE, Rome, Italy, June 2009.

[14] T. Zahariadis, A. Papadakis, F. Alvarez et al., "FIWARE lab: managing resources and services in a cloud federation supporting future internet applications," in Proceedings of the 7th IEEE/ ACM International Conference on Utility and Cloud Computing (UCC '14), pp. 792–799, IEEE, London, UK, December 2014

[15] A. Schmidt and K. Van Laerhoven, "How to build smart appliances?" IEEE Personal Communications, vol. 8, no. 4, pp. 66–71, 2001

[16] How Do Global Positioning Systems, or GPS, Work?, 2005, https://www.nasa.gov/audience/foreducators/topnav/materials/ listbytype/How Do Global Positioning Systems.html# .VmxoY5Ph5z0.

[17] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: a study ," International Journal of Computer Science & Engineering Survey, vol. 2, no. 3, pp. 94–105, 2011.

[18] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in Proceedings of the 13th International Conference on Collaboration

Technologies and Systems (CTS ’12), pp. 21–26, Denver, Colo, USA, May 2012.

[19] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, “Middleware for internet of things: a survey,” IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70–95, 2016.