International Journal of Computer Applications Technology and Research
Volume 10–Issue 05, 119-122, 2021, ISSN:-2319–8656

IoT an Overview: Advantage, Disadvantage and Applications

Bhagwati Charan Patel
Department of Information Technology, SSTC, SSGI
Bhilai, India

Ram Shankar Tripathi
Scholar
Department of Information Technology SSTC, SSGI
Bhilai, India

Naveen Goel
Department of Electrical and Electronics Engineering,
SSTC, SSGI
Bhilai, India

Abstract: Internet of Things (IoT) is a well-known term that has gained massive encouragement over a few years. The future of the human race will be significantly influenced by the application of IoT over the coming years. The Internet is everywhere and touched almost every corner of the globe affecting our lives in previously unimagined ways. As a living entity, the Internet is constantly evolving, and now, an era of widespread connectivity through various smart devices (i.e., things) that connect with the Internet has begun. IoT looks more like an umbrella covering many protocols, technologies, and concepts that depend on specific industries. It will lead to the development of efficient mechanisms with high scalability and interoperability features among the things or objects. IoT is a reality that is progressing day by day, connecting billions of people and things to form a vast global network. IoT has applications in various domains like agriculture, industry, military, and personal spaces. There are potential research challenges and issues in IoT that act as a hurdle in the complete exploration of IoT in real-time implementation.

Key Words: Internet of Things, IoT architecture, RFID, Smart technology, Cloud computing, WSN

1. INTRODUCTION

The Internet of Things (IoT) is a kind of network which is created by the different devices performing separate tasks for some common purposes. We are entering an era of the “Internet of Things”. This term has been defined by different authors in many different ways. Let us look at two of the most popular definitions. Vermesan et al. [1] define the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators. Another definition by Pe˜na-L´opez et al. [2] defines the Internet of Things as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object. Main components [3] of IoT are sensors and physical objects. With the help of Wireless sensor Network and RFID, information is exchanged in this era of internet of things every device is uniquely identified. 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. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment). An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner and accessed to the network [4].

IoT is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established. Over 9 billion ‘Things’ (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to a whopping 20 billion.

There are four main components used in IoT as shown in Fig. 1:

1. **Low-power embedded systems –** Less battery consumption, high performance are the inverse factors play a significant role during the design of electronic systems.
2. **Cloud computing –** Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
3. **Availability of big data –** We know that IoT relies heavily on sensors, especially real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
4. **Networking connection –** In order to communicate, internet connectivity is a must where each physical

object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

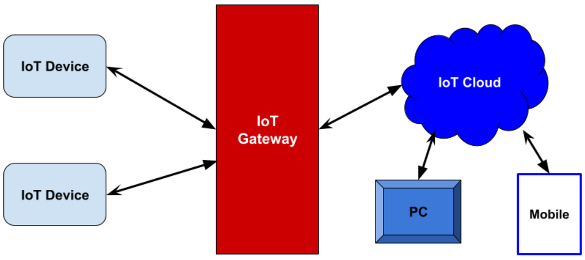

Fig. 1 IoT Structure

2. ARCHITECTURE OF IOT

The layered architecture in context of IoT has five layers named business, application, middle, network, and perception layers [5-8] as shown in Fig. 2.

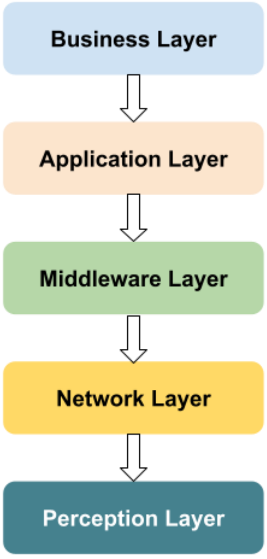

Fig. 2 IoT Architecture

1. Business Layer: Once IoT data is procured, it is valuable only if it applies to business planning and strategy. Every business has specific goals and objectives that it wants to accomplish by gathering intelligence from data. Business owners and stakeholders use data from past and present data to plan precisely for the future.

2. Application Layer: In this layer, Data is further processed and analyzed to gather business intelligence. Here IoT systems get connected with middleware or software that can understand data more precisely.

3. Middleware Layer: It transports data from sensor to control rooms for processing the information safely. It serves the requests taken from the network layer. There is data base which may be used if needed to perform ubiquitous computing and decision making about the results. The SOA architecture of IoT has applications, service management, service composition, object abstraction objects [9-12]. Apart from this it needs a trust, privacy, and security management.

4. Network Layer: 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.

5. Perception Layer 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.

3. IOT − KEY FEATURES

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below:

Artificial Intelligence – IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favourite cereal run low, and to then place an order with your preferred grocer.

Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

4. CHALLENGES

This emerging IoT has tremendous usages as well as dangers also, as it connects with the physical world. Internet threat today steals credit cards. Who can tell that future internet will not ruin home security system and disrupt hospital? Different heterogeneous devices connecting to each other in unsupervised way giving birth of insecurity of internet operation. Two important issue/challenges of IoT can be low power and security function. There are lot of vulnerabilities in IoT because of its nature of network [13-15]. The security requires resilience to the attacks, access control, data authentication, and client privacy.

5. ADVANTAGES OF IOT

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer:

- Improved Customer Engagement – Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
- Technology Optimization – The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.
- Reduced Waste – IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- Enhanced Data Collection – Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

6. DISADVANTAGES OF IOT

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues:

- Security – IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
- Privacy – The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
- Complexity – Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.
- Flexibility – Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- Compliance – IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

7. PRACTICAL APPLICATIONS

The versatility of IoT has become very popular in recent years. There are many advantages to having a device based on IoT. Mckinsey Global Institute reports that IoT business will reach 6.2 trillion in revenue by 2025. There are lots of applications are available in the market in different areas.

(i) Personal Home Automation System: Home Automation system is the major example in this area.

Wemo Switch Smart Plug: It is the most useful devices which connected home devices in the Switch, a smart plug. It plugs into a regular outlet, accepts the power cable from any device, and can be used to turn it on and off on hit a button on your smartphone.

(ii) Enterprise: In the enterprise area many applications are there like environmental monitoring system, smart environment etc.

Nest Smart Thermostat: It is connected to the internet. The Nest learns automatically your family’s routines and will automatically adjust the temperature based on your activities, to make your house more efficient. There is also a mobile app which allows the user to edit temperature and schedules.

(iii)Utilities: smart metering, smart grid, and water monitoring system are the most useful applications in the various utility area.

(iv)Energy Management: Advanced Metering Infrastructure is the major example in this area.

(v) Medical and Health Care: Remote health monitoring and emergency notification system are examples of IOT in the medical field.

Health patch Health Monitor: It can be used for the patient who can’t go to doctors, letting them get ECG, heart rate, respiratory rate, skin temperature, body posture, fall detection, and activity readings remotely.

(vi) Transportation: Electronic toll collection system is the most useful example in this area.

(vii) Large scale deployment: There are various large projects ongoing in the world. Songdo (South Korea), the first of its kind fully wired Smart City, is near completion. Everything in this city is planned to be wired, connected and turned into a data stream that would be monitored by an array of computers without any human interaction.

8. CONCLUSIONS

This paper surveys the IoT standards, technology, architectures, and enabling technologies of the IoT with special attention of security, privacy, and trust aspects. Various techniques and ways are described and analysed on the basis of important parameters. Treats, attacks and vulnerabilities of various levels are analysed.

REFERENCES

[1] O. Vermesan, P. Friess, P. Guillemin et al., “Internet of things strategic research roadmap,” in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.
[2] I. Pe˜na-L´opez, Itu Internet Report 2005: The Internet of Things, 2005.
[3] Louis COETZEE1, Johan EKSTEEN2,"The Internet of Things –Promise for the Future? An Introduction", IST Africa 2011 Conference Proceedings
[4] O. Said and M. Masud, “Towards internet of things: survey and future vision,” International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.
[5] Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on 2012 Dec 17 (pp. 257-260). IEEE.
[6]. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on 2012 Mar 23 (Vol. 3, pp. 648-651). IEEE.
[7]. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018 May 1; 82: 395-411.
[8]. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014 Nov 1; 20(8):2481-501.
[9]. Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805.
[10] 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.
[11] 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.
[12] 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.
[13]. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. 2013 Jul 5; 57(10):2266-79.
[14]. Vasilomanolakis E, Daubert J, Luthra M, Gazis V, Wiesmaier A, Kikiras P. On the security and privacy of internet of things architectures and systems. In Secure Internet of Things , 2015 International Workshop on 2015 Sep 21 (pp. 49-57). IEEE.
[15]. Weber RH. Internet of Things–New security and privacy challenges. Computer law & security review. 2010 Jan 1; 26(1):23-30.