World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

INTERNET OF THINGS: CHALLENGES AND SOLUTIONS

Matthew N. O. Sadiku, Shuza Binzaid*, and Sarhan M. Musa

Roy G. Perry College of Engineering Prairie View A&M University, Texas, USA.

Article Received on 27/02/2019 **Article Revised on 17/03/2019** **Article Accepted on 07/04/2019**

***Corresponding Author**
Shuza Binzaid
Roy G. Perry College of Engineering Prairie View A&M University, Texas, USA.

ABSTRACT

The Internet of things (IoT) is a relatively new concept. It presents numerous benefits to consumers and proves a financial boon for businesses. Pervasive introduction of sensors and devices into currently intimate spaces, such as homes, cars, and wearables, poses some challenges. There are also challenges in deploying IoT by government agencies and private industries. This paper attempts to address these challenges and offers solutions.

KEYWORDS: Internet, Internet of Things, Challenges, Solutions.

INTRODUCTION

The Internet has evolved to be an ever more pervasive and critical infrastructure connecting society and enabling global commerce. The next phase of the Internet is the Internet of things (IoT), which connects smart things or devices equipped with sensors. IoT may be regarded as an extension of the Internet in which large numbers of devices are networked. These devices communicate with each other without any human interaction. The amount of data that IoT devices can generate is staggering.

The IoT represents one of the most significant disruptive technologies of the century. Consumer products, cars and trucks, sensors, and other everyday objects are being combined with Internet connectivity. We are surrounded by the Internet of things every moment.

The central concept of the Internet of Things is to connect anything, anytime, and anywhere through Internet. IoT is being deployed across the globe to solve some of the most pressing

issues. Although the Internet of Things (IoT) is gaining wide acceptance, some companies are reluctant to implement it. Several challenges need to be addressed in order to encourage continued IoT deployments.

OVERVIEW OF INTERNET OF THINGS

The term "Internet of things" was introduced by Kevin Ashton from the United Kingdom in 1999. Internet of Things (IoT) is a network of connecting devices embedded with sensors. It is a system of interconnected computing devices that permit interaction between people to machines, people to people, machines to people, and machines to machines. It envisions everything in the physical world will be connected and integrated securely through Internet infrastructure. As shown in Figure 1, devices or things can be connected to the Internet through three main technology components: physical devices and sensors (connected things), connection and infrastructure, and analytics and applications.[1]

The IoT architecture is typically divided into three layers, i.e. perception layer, network layer, and application layer. The perception layer is responsible to extract information from things and to transform it into a digital format. The network layer transports the digital signals via the network, while the application layer transfers digital signals into different contexts. This is illustrated in Figure 2.[2]

There are four main technologies that enable IoT.[3]

1. Radio-frequency identification (RFID) and near-field communication (NFC).
2. Optical tags and quick response codes: This is used for low cost tagging.
3. Communication systems (such as WiFi and ZigBee),
4. Wireless sensor network (WSN): This is used to monitor physical properties in specific environments.

These technologies enable devices to be smart. Other related technologies are cloud computing, machine learning, and big data.

IoT is an enabling technology that provides various kinds of services like supply chain automation M2M, pedestrian navigation, remote appliance avoidance, and air quality control. IoT helps people and communities by making their systems smarter and their lives easier, more secure, and safer. IoT transforms ordinary products such as cars, buildings, and machines into smart, connected objects that can communicate with people and each other.

These applications have given birth to smart everything, smart cars, smart homes, smart refrigerators, smart cities, smart parking, smart health, smart environment, transportation, shopping, agriculture, lighting, grid, and energy. Some of these smart devices are illustrated in Figure 3.[4] From smart grid to data analytics, all future technologies are a part of IoT. For example, IoT solutions like RFID tags and GPS sensors can be used by retailers to monitor the movement of goods from manufacturing to when a customer buys it.

Implementtion Challenges and Solutions

The Internet of things is a technology that can fundamentally revolutionize the way we live and interact. This fantastic opportunity also presents a number of significant challenges.[5] The common implementation challenges that organizations may face when implementing the IoT and how to address them is presented next.[1,6,7]

1. Security: Security is one of the forefront challenges because any platform connected to IoT poses the risk of being insecure and open to hackers. Many businesses are wary of the security and privacy issues associated with IoT. IoT service providers need to be sure that their data is going to be safe. Increase in connected devices leads to an increase in endpoint vulnerability. Many IoT platforms consider security a core element and work to ensure that any potential leaks are stopped before hackers find them.

Government, police, and IoT device manufacturers should find effective IoT security solutions. Security should be built in as the foundation of IoT systems, with rigorous validity checks, authentication, and data verification. Device manufacturers should build security into software applications and network connection that links the devices. Data security can be addressed by using a comprehensive governance mode, which provides secure access to sensitive data. Combining public and private infrastructure also can help protect data in transit. Companies have started to look at protecting their IoT ecosystem as well as their customers'. When choosing security cameras, you should select the brand that has confidential encryption, such as SSL encryption.

2. Interoperability and Standards: IoT consists of heterogeneous networks which connect all kinds of devices. Interoperability is the key to open markets to competitive solutions to IoT. The first requirement of Internet connectivity is that connected devices should be able to "talk the same language" of protocols. This makes interoperability the most basic core value. Recently, there has been a significant proliferation of Internet-capable devices and it is

unlikely these devices are created by the same manufacturer. Implementing IoT often involves procuring devices that do not have IoT label. The complexity of procuring these devices and the lack of the IoT standard can make it difficult for stakeholders.

Some IoT standards are still in development. The IEEE published its draft P2413 standard for IoT architecture, creating a universal language for IoT. Since IoT devices are usually purpose-built, universal security standards are difficult to develop. The use of open and widely available standards for IoT devices and services will provide greater user benefits.

3. Technology Infrastructure: Infrastructure is critical for emerging IoT applications such as smart buildings, smart homes, smart cities, smart grid, intelligent transportation systems, and ubiquitous healthcare, to name a few. Most businesses lack the infrastructure and network components that huge volumes of IoT data require. For a new technology, there is no need to overinvest in infrastructure all at once. You can gradually get more sophisticated with your IoT solutions. The massiveness of connected devices to the Internet will pressure the adoption of IPv6, which is a technology considered most suitable for IoT.

4. Workforce: It is challenging to change the mentality of the current workforce. It can be difficult to convince those in the upper levels about the opportunities of IoT projects. Sometimes, there is not enough technical skill to gain valuable insights from the huge amount of data collected from IoT. Businesses should hire experts with the relevant IoT training.

5. High Investment Cost: The high initial costs in IoT investments can scare some companies off. But IoT costs are declining rapidly. IoT projects implementations with reasonable costs are recommended. Breakthroughs in the cost of sensors and processing power are enabling ubiquitous connections right now. The sensing devices such as RFID tags, sensors, actuator, etc. be designed to minimize cost.

6. Energy: IoT consists of various low-power embedded devices. IoT devices are resource-constrained. These devices are not full fledged resource-equipped, which inspired the concept of resource-constrained wireless sensor networks (WSNs). IoT uses low-power lossy networks, which complicates security issues by adding an additional constrain, energy. Since an energy source needs to supply each sensor in IoT, a tremendous amount of energy would be needed to run thousands of these sensors. This is a serious challenge that IoT has to

handle. There are many ways to provide power such as main power supply, battery, solar system, etc. Smart devices may need to use smart battery.

These are some major challenges that influence the decision-making process of potential customers for a successful IoT implementation. Other challenges include privacy and data protection, power consumption of devices, limited battery, global misinformation systems, global cooperation, intelligent data analytics, big data problems, and quality of service issues.[8] These challenges are being addressed by a vast range of organizations and government agencies around the world. In spite of the challenges, the adoption of IoT continues to expand.

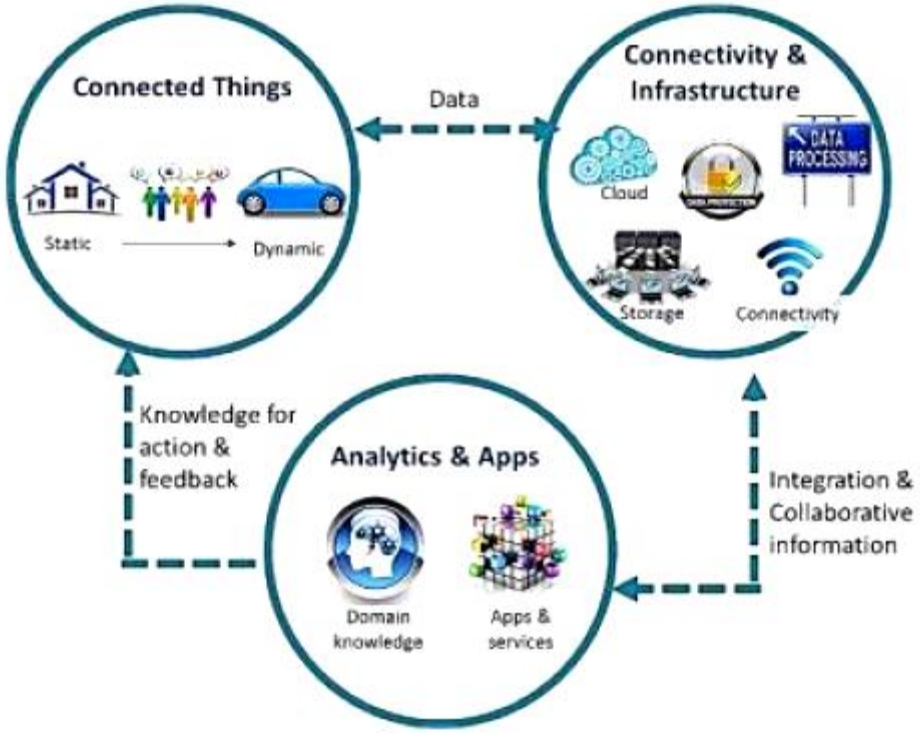

Figure 1: Components of the Internet of things.[1]

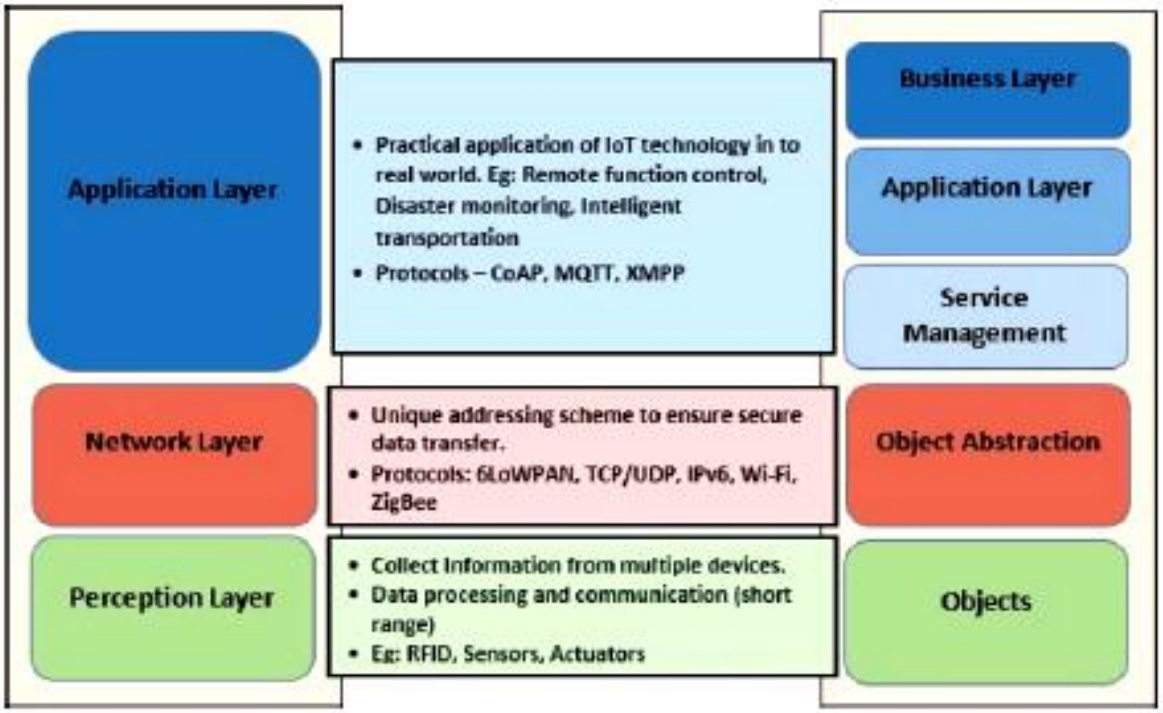

Figure 2: Typical IoT architecture.[2]

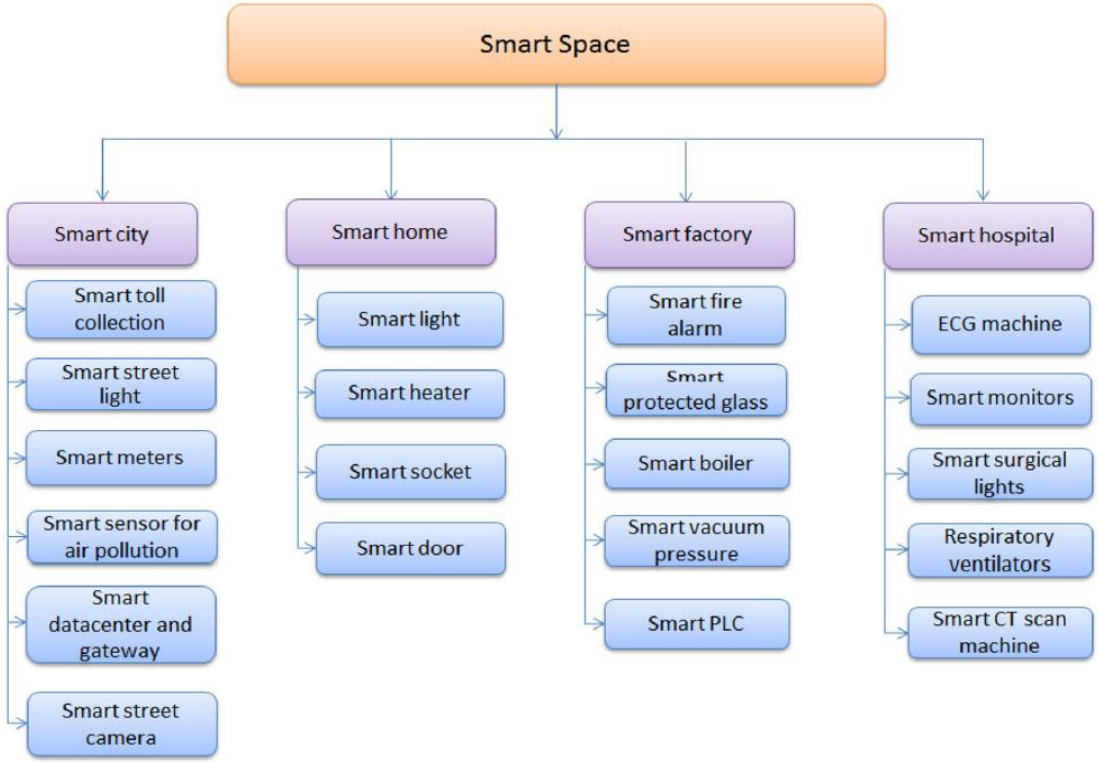

Figure 3: Smart space components and devices.[4]

CONCLUSION

The era of the Internet of things has already started and it will drastically transform our way of life. The IoT is the concept that everything around us from cars to laptops, can be connected. The widespread adoption of the IoT has increased many folds recently. However, the rapid growth of IoT has presented some significant challenges. IoT's development has been restricted by these challenges.[9] Security happens to be the most prominent challenge. More information on challenges and solutions of IoT can be found in the books in.[10-12] and other books available in Amazon.com.

REFERENCES

1. "Internet of things: Security and privacy concerns," https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/InternetofThings.aspx.
2. B. N. Silva, M. Khan, and K. Han, "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges," IETE Technical Review, 2018; 35(2): 205-220.
3. M.N.O. Sadiku, and S.M. Musa and S. R. Nelatury, "Internet of things: An introduction," International Journal of Engineering Research and Advanced Technology, 2016; 2(3): 39-43.
4. S. Singh et al., "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, 2017; 1-18.
5. C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, 2017, pp. 155-184.
6. N. Dyness, "Six IoT implementation challenges, and solutions," Control Engineering, October 2018, p. 21.
7. L. Sears, "5 IoT challenges and solutions," August 2017 https://www.govloop.com/5-iot-challenges-solutions/
8. P. J. Ryan and R. B. Watson, "Research challenges for the Internet of things: What role can or play?" Systems, vol. 5, no. 1, 2017.
9. J. Saleem et al., "IoT standardisation-challenges, perspectives and solution," Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, June 2018.
10. P. B. Purushothaman, IoT Technical Challenges and Solutions. Boston, MA: Artech House, 2017.

11. S. C. Mukhopadhyay (ed.), Internet of Things: Challenges and Opportunities. Springer, 2014.
12. Q. F. Hasan, A. R. Khan, and S. A. Madani (eds.), Internet of Things: Challenges, Advances, and Applications. Boca Raton, FL: Taylor & Francis, CRC Press, 2018.