ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2017

Internet of Things – Future Outlook

Meenakshi Nadimpalli*

Global Information Technology Executive, 2412 Amherst Rd, Middleton, WI – 53562, USA

Abstract: In this paper we discuss how the Internet of Things (IoT) ecosystem will change and disrupt difference industries. In spite of many research papers there is a need of discussion on security challenges by the Internet of Things and recommendations on how they can be overcome. To provide a basis for discussing Future Outlook of IoT, a vision for how IoT could change the world in the distant future has been discussed. We also discussed the comprehensive analysis regarding what the Internet of Things holds for the future, how it is yet to disrupt and transform industries, possible challenges, and solutions. It provides systematic exploration of existing IoT products in the marketplace and highlights of potentially significant research directions and trends.

Keywords: Internet of things; Security threats; Security challenges; Sensor technology; Computer devices; Consumer satisfaction; Industry disruption; Computer networks; Network traffics; Modern technology.

I. INTRODUCTION

The Internet of Things (IoT) is a dynamic global information network consisting of Internet-connected objects, such as radio frequency identifications, sensors, and actuators, as well as other instruments and smart appliances that are becoming an integral component of the Internet [1-6]. IoT is barely an embryonic concept but it has already elicited scientific and economic debates. Currently, the scalability of products and services, as well as the relationship between countries majorly depend on the strength of the computer networks. The implication is that the Internet of Things has changed the way people socialize and work. The forecasts for the IoT are remarkable in the world of business [7]. Most countries are already anticipating a drastic rise in the rate at which they will be using the concept in the near future. Despite everything, yet, the Internet of Things is accompanied with substantial drawbacks that could hamper the realization of its prospective paybacks. Today's news items are filled with features concerning hackers, security reservations, and privacy issues [3]. As a result, while technical benefits continue to be realized, challenges seem to be major deterrents to the growth of the Internet of Things. The review entails the dialogue concerning the future of IoT, how the ecosystem is yet to change or disrupt various sectors, the possible security challenges, and approaches to handling such issues. The phrase Internet of Things has been in use since the late 1990s. It was first used by Ashton Kevin, a technologist from Britain, to mean a system in which the world was able to interlink with the Internet through sensor technology. In today's scenario, IoT has found a more developed meaning as it is now used to describe the connection between the Internet and various objects including computer devices, telephone lines, as well as sensors [8,9]. Even though the term IoT appears as a novel idea, the idea of using computer networks in observing and controlling devices is a century old concept. For example, by the mid-1960s, technicians had already come up with mechanisms for remote monitoring of electricity grids. By late 1980s, there were further progresses in computer technology and firms could use wirelessly integrated machines in their production. Nonetheless, most of the early innovations in the wireless technology tended to be weaker and there was the need for more development [7]. Therefore, the Internet of Things surfaced. With the continued rise in the demand curve, technologists are envisioning a future where data mining techniques will shift to the cloud. Organizations will be forced to have dedicated data gathering systems that will further stir the advancement within the scope of Artificial Intelligence. Ideally, the thriving Internet of Things is yet to become a key focus in the whole telecommunications sector by the year 2022. There is already an incessant growth in evidence revealing the potential of IoT in creating efficiency in the industrial sectors [7]. The implication is that there are marvellous opportunities with regards to the modern computer technologies. So far we have analysed the history how IoT is evolved over the time. In this section we discuss some of the statistics and facts related to the IoT which allows how the IoT has grown over the years and how it is expected to grow in the future. By 2020, there will be 50 to 100 billion devices connected to the Internet, ranging from smartphones, PCs, and ATMs (Automated Teller Machine) to manufacturing equipment in factories and products in shipping containers [8]. According to Cisco Internet Business Solutions Group, as depicted in Figure 1. The number of things connected to the

Internet exceeded the number of people on Earth in 2008. According to CISCO, each individual on earth will have more than six devices connected to the Internet by 2020 [8].

Source: A Survey of Internet of Things from Industrial Market Perspective [8].

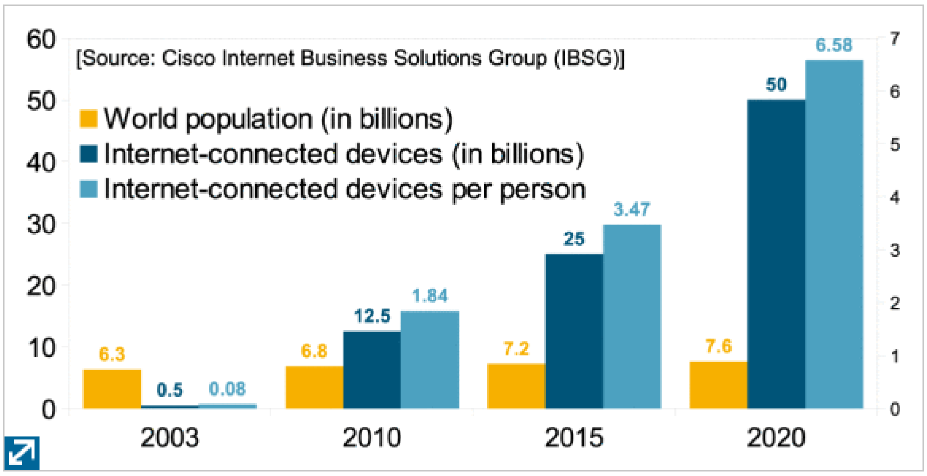

Figure 1: Growth in internet connected devices/objects by 2020.

With respect to the evolution of technical skills, it is evident that the IoT will be the avenue through which businesses will connect with both their clients and fellow associates. Such a unique network would mean that strategies towards consumer satisfaction will become much developed. The relationship will equally ensure that technologies are used for the rightful purpose of bettering both business and customer wellbeing. It is also hoped that through IoT, venture owners and technologists will team up to plan and influence consumer needs by giving them much more than they will ever expect [7]. However, because of the potential challenges, it is important to review if the IoT will positively change or shake the way various industries operate.

II. METHODOLOGY

The study utilized the literature review approach by analysing a total of seven sources including peer reviewed journals, books, and academic blogs. The core of the research was to identify previous works that had already explored the arena of Internet of Things. Key words such as IoT, Internet, modern technology, and computer networks, were used to facilitate the location of relevant publications. Through the various books, peer reviewed journals, and academic blogs, it was possible to come up with a comprehensive analysis regarding what the Internet of Things holds for the future, how it is yet to disrupt and transform industries, possible challenges, and solutions.

III. HYPOTHESIS

1). The Internet of Things will have a ground breaking impact on how industries conduct their operations.

2). The Internet of Things is characterized by major security threats that may influence the rate at which industries adopt it.

IV. OUTCOMES AND DISCUSSIONS

As expected, it was evidenced that with the surge of the Internet of Things, other forms of innovation may emerge as supplements. For example, there will be the need to create a single system that connects consumers to the individual companies that deal with hospitality, agriculture, construction, and transport. Development in this manner will be necessary because the current computing power has not been strong enough to support applications used in IoT. In addition, there will be a prospective emergence of special software for IoT that will link with the personal computing programs [7].

Additionally, the review revealed that companies may experience a future where all data will be stored in the clouds. Through this, it will be easier for many startups to make fortunes by creating technologies that can simplify the lives of consumers. The cloud model of storage will be important because it will allow such startups to expand easily. In ideal cases, emerging entrepreneurial ventures seem to be in a better position to notice the desires of average consumers as opposed to market leaders. The established firms tend to be centered on the sums of profit that a technology can bring [9]. As a result, there is always the notion that bigger companies are destined to grow slowly because of their level of hesitation in adopting technologies.

On the other hand, it was concluded that companies with IoT techniques will be disrupted as hiring will become a major challenge. Essentially, there is an extensive difference between the IoT and the normal Internet. On average, people spend long periods on their computers and a majority of modern graduates would rather work for a high-tech company than those which are slow to adopt work from home initiatives [6]. Therefore, even while most organizations are thinking of introducing IoT, they may still fail to stand the trends of the modern virtual companies.

Similarly, it is anticipated that even though firms will achieve in the development of more reasonable IoT strategies, the actual process may not be stress-free. Currently, organizations that have taken up the initiative to develop IoT products may be regarded to have achieved in acknowledging the wishes of consumers. However, most of them have tended to concentrate more on these technologies than the actual customer needs. Such companies have seen a decline in their profit margins and they now hold that the IoT is a modern concept that still needs critical reevaluation [6].

Furthermore, it is also possible that the Internet of Things may not mean that standards will stop being discordant. The IoT has a major issue with regard to the lack of common principles. The deficiency of shared standards has always caused challenges when developers want to merge various connectable gadgets. The lack of common standards is equated to the problems that have been deteriorating the health sector [8]. The sad part is that no one has shown interest in addressing the relevance of the IoT standards regardless of the visible benefits.

With the drastic growth of the IoT, it is predictable that diversity will again become a drawback as it was in the past. For example, it will not be easy to sway the female gender to take up vocations that deal with technology because of the prevalent underrepresentation that they have faced in the industry. The other scope through which diversity will come into play in will be the idea of border protection. In other words, it will be challenging to change the government’s decision regarding immigrants despite the possibility of diverse talents possessed by these individuals. There are technical experts in regions such as China, yet it may not be possible to have them work within the American premises because of border policy concerns [9].

More importantly, the self-driven cars will be major disruptors of the taxi sector. A number of locomotive firms are working tirelessly towards the development of fully self-sufficient automobiles [9]. While the prospective comfort and safety benefits appear wonderful to travelers, a majority of employees in this sector are already envisioning the danger of redundancy. The fact that the cars will need remote controllers will only mean that most former drivers will have to resort to some other means of earning income. The other aspect is that total lack of traffic will imply that most businesses, especially those on the roadsides, may begin to tumble.

V. SECURITY CHALLENGES POSED BY THE IOT

The Internet of things is aimed to offer unparalleled and global access to services that will transform every sector from healthcare, transport, to hospitality. Nonetheless, it is important to note that such unrestricted access to the various services presents key security concerns. First, there is the problem of ineffective authorizations where most customers are forced to depend solely on weak secret codes for user verification purposes [3]. Most gadgets allow handlers to get into the systems through easy a passcodes like “abcd”.

Moreover, the IoT systems often lack transport encryptions since some gadgets have no in-built capacities to encode data while it is in the process of being conveyed. This becomes a major challenge if the Internet is used. Some devices also have insecure interfaces. Ideally, such web frameworks tend to be highly vulnerable to attacks by the Open Web Application Security Project; a common hacking tool [9]. The most targeted users are those people who have weak passwords and individuals who tend to be poor in session management.

It is an assumption that the lack of standard IoT principles implies that there will be no protective code practices. In other terms, developers will come up with services that do not adhere to safe coding initiatives. The challenge will majorly be experienced in the health care domain. Since most of the gadgets used convey facts over computer networks do not have any form of encryption, there is the risk of malicious individuals trying to disfigure the information. For instance, when the patient is noticed to be reliant on certain types of diets, it may be possible to tell much about them [3]. If such information is divulged, aspects such as their supplier details and religious affiliation may become public without their validation.

VI. OVERCOMING THE SECURITY CHALLENGES

The Internet of Things can only be termed as being safe if its systems have inbuilt security measures. Besides, it is advisable that every aspect of the IoT undergoes a security check to ascertain the level of vulnerability. One of the leading strategies to ensure the safety of IoT is through the analysis of the device platforms. Strongly configured platforms are known to be free from possible compromises including freedom of access. In this view, the base platforms to the devices must be reviewed and security features scrutinized for any data security threats [7]. The confirmation is important as it leads to prompt detection and removal of harmful interfaces.

There also needs to be verification of the network traffics. Both the wireless and the wired networks have to be put under deep evaluation against unprotected or adjustable data. There is always a relationship between security and performance, hence the need for encryption. In certain cases, minor coding procedures may be applicable for increased performance. In addition, it would be necessary to verify the relevance of security details. By doing this, it would be possible to certify the best performing security measure. The data channels also need to be checked for the possibility of any attacks. Such verification should be done by constant check on new entrants, which will assist in the minimization of the various forms of advanced risks on the IoT networks [7].

Most companies that have adopted the IoT solutions have also gone for the secure code analysis strategy of minimizing the challenges. Ideally, prompt reviews on the safety of codes can help in the timely control of the security challenges. The expense underwent in mitigating security flaws becomes much low in a case where susceptibility is diagnosed at the initial stages. The secure code analysis strategy can also work in hand with the end user tests. It is the trial that helps in the identification of exposed areas along the web interface [7]. The strategy is regarded as highly flexible and it can work in many models of IoT solutions.

According to Stankovic's research, it is mentioned that healing security attacks, a system needs to detect the attack, diagnose the attack, and deploy countermeasures and repairs to perform all of this in a lightweight manner due to the types of low capacity devices involved [6]. Also is it necessary to have significant hardware support for providing encryption, authentication, attestation and tamper proof keys.

VII. CONCLUSION

In conclusion, the Internet of Things is evidenced to be a prerequisite for the high performance of the various industries of the contemporary universe, including healthcare, transport, and hospitality. Even though the IoT has several advantages in the world of business, it equally has the potential to cause massive disruptions in various industries including transport and manufacturing. For example, while it is beneficial in enhancing transport, the concept will similarly lead to redundancy in the taxi business as the autonomous mode of operating the cars will render people jobless. On the flip side, the IoT is similarly flawed with significant security challenges, which may turn away potential adopters. Therefore, further studies need to dwell on measures that can be put in place to ensure that the security concerns are controlled.

VIII. REFERENCES

1. SA John, Research Direction for the Internet of Things. IEEE Internet of things 2014; 1: 3-9.
2. S Dhananjay, T Gaurav, et al. A survey of Internet-of-Things: Future vision, architecture, challenges and services. Internet of things (WF-IoT) IEEE world forum 2014: 287-292.
3. G Jorge, M Edmundo, et al. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials 2015; 17: 1294-1312.
4. W Andrew, A Anurag, et al. The Internet of Things- A survey of topics and Trends. Information Systems Frontiers 2015; 17: 261-274.
5. P Charith, LH Chi, et al. A Survey of Internet of Things from Industrial Market Perspective. IEEE 2014; 2: 1660-1679.
6. B Tony, 2017 Trends to Watch: Big Data. Ovum TMT intelligence 2016.
7. G Jorge, M Edmundo, et al. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials 2015; 17: 1294-1312.
8. R John, the Disruptor Array. CFA Institute Magazine 2015; 26: 33-36.
9. L Danny, D Victoria, Disruptive Technologies and their Implications for Economic Policy: Some Preliminary Observations. Institute for International Economic Policy 2016: 1-32.