**International Journal of Academic Management Science Research (IJAMSR)**
**ISSN: 2643-900X**
**Vol. 4, Issue 5, May – 2020, Pages: 71-75**

# Internet of Things Issues and Challenges

**Amina Salim Abeid**

Researcher: Micheweni, North Pemba

***Abstract*****:** *The advancement of Information and Communication technologies has brought tremendous changes in the world and it has a predominant influence on the developing economy and information society. The growth of these technologies has a positive impact across various economic sectors, this technology is also used largely for the development of innovative products and services in order to address societal, market, and business challenges (White paper, 2018). Internet of things comprises of smart devices that use wireless technology to talk to each other and to users. Nowadays, there are billions of devices are aimed to be interconnected in the internet of things (IoT) network using a wireless network connection, such devices offer a smarter, more efficient for users, impacting business, manufacturing, healthcare, retail, security and transport (K. sha et al 2018). Today, the internet of things (IoT) is considered to have the potential to improve the quality of life of the citizens and the economic growth of the county. Adoption of the internet of things (IoT) technology in various aspects such as smart cities, smart transportation, smart logistics, smart industries, smart meter and smart grid enhance interaction with the people and improve their current operational efficiency. The qualitative infrastructure of the ICT sectors provides an environment for the development of innovative IoT solutions. Because of the dynamic ICT ecosystem, it contributes largely to the implementation of new IoT based solution and protects the way for a data-driven economy (White paper, 2018). This paper adopts the survey of different kinds of literature as a methodology used aimed to discuss the issues and challenges of the internet of things. Among the challenges including security, privacy, trust and connectivity challenges.*

**Keywords:** IoT, ICT, 4IR, ICT ecosystem, smart buildings, security, privacy, trust, connectivity

## 1. Introduction

The fourth industrial revolution (4IR) is creating an environment in which everything will be perceptible, interconnected and intelligent. Internet of things is a communication network of physical objects. The internet is not only a network of computers, but it has evolved into a network of device of all type and sizes, such devices including vehicles, smartphones, toys, medical instruments, home appliances, camera, animals, people, industrial system, smart buildings, all communicating and sharing information based on specified protocols in order to achieve smart reorganizations, positioning, tracing, safe and control and personal real-time online monitoring, online upgrading, process control and administration (Keyur, K.P et al, 2016).


**Figure 1: Internet of Things Devices**

Internet of Things is the foundation of this new age. Information and communication technology powers the ability of internet of things to restructure traditional industries (Pooja Yadav et al, 2018). IoT combines connectivity with sensors, devices and people, enabling a form of a free-flowing conversation between man and machine, software and hardware. Although the potential for IoT is massive, its practical execution remains in its early stages. As a result, it's difficult to estimates the future impact with precision. International Data Corporation (IDC) estimates that there will be 30 billion connected devices in the market by 2020. IDC also

estimates the economic value of IoT to be around $1.46 trillion in 2020. Gartner forecasts 20.8 billion connected devices and $3 trillion IoT economic value during the same timeframe (EY, 2018).
Cisco IBSG estimates internet of things was born between 2008 and 2009 (Figure 2). During 2003, there were 500 million devices connected to the internet, and according to the U.S. Census Bureau, there was 6.3 billion world population. Furthermore, Cisco IBGS predicts there will be 25 billion devices connected to the internet by 2015 and 50 billion by 2020. However, due to the rapid change of technology and advances in the internet, the estimation presented will dynamically change (Cisco IBGS, 2011).

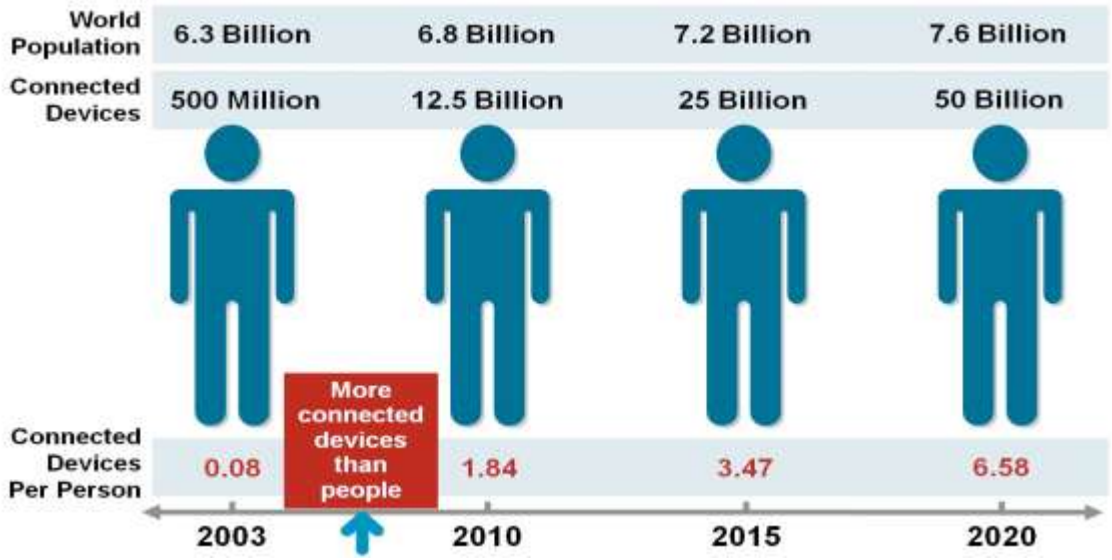


**Figure 2: The Internet of Things was born between 2008 and 2009**

It is obvious that, in the future, everything will be connected to the internet than simply connected people. This is due to the fact that IoT shortens business processes, boosts productivity, and provides better products and services, while, at the same time releasing a huge potential for innovation. For example, the government want to make everything intelligent, including street lighting, parking, and bicycle, to the water meter, gas meter, fire protection and environmental monitoring, so government hope that IoT will improve the quality of life standard and increase city management efficiency. Apart from that, IoT will bring a new wave of connectivity services that bring great opportunities for development. At the same time, the IoT platform is used to integrate the data of different industries.

Because everything becomes connected and intelligent, IoT brings huge economic value. It is driving the digital transformation of all industries. From government and organization to businesses and local communities around the world. Everyone is researching and investing in the IoT. They collect, analyze, and apply data generated through the IoT, facilitating the rapid development of all industries (White paper, 2018).

## 2. Literature Review

This section, the study will discuss the characteristics of IoT which are interconnectivity, things related services, heterogeneity/diversity, dynamic change, enormous scale and smart data collection and smart handling. In addition to that, the study also will discuss challenges that face IoT systems including security, privacy, trust and connectivity challenges (Keyur, K.P et al, 2016; White paper, 2018).

### *2.1 IoT Basic Characteristics*

**Things-related services**: The IoT is capable of providing Things-related services within the constraints of things, such as privacy protection and semantic consistency between physical and their associated virtual objects. In order to provide Things-related services within the constraints of things, both the technologies in the physical world are required.
**Interconnectivity**: With regard to IoT, anything (physical or virtual things) can be interconnected through the backbone of the communication system upon which various broadcasting and telecommunication services are operated (communication infrastructure).
**Dynamic changes**: The device state dynamically changes, for instance, sleeping and waking up, connected and/or disconnected as well as the context of devices, such as speed and location. Also, the number of devices can change dynamically.
**Heterogeneity/diversity**: In IoT system, the devices should be heterogeneous as based on different networks and hardware platforms. They can interact with other devices or service platforms through different networks.

Diversity is another characteristic of IoT. Identifiers in the physical world and information world are different. In the physical world, the identifiers of physical things of the IoT devices may be different according to applied technologies.

**Enormous scale**: In the context of IoT system, there are several devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the number of devices connected to the current internet. Most important will be the management of the generated data and its interpretation for application purposes. This relates to the semantics of data and efficient data handling.

**Smart data collection and smart handling**: The IoT is able to distribute sensors widely and collect data quickly and effectively to form a new way of collaboration among connected devices. Smart data processing of such collected data is a key IoT feature. The different kinds of data produced by physical devices of IoT systems can be a stream, batch, and asynchronous data. Such data can be processed and used for system feedback, allowing for process improvement, fault detection and incorporation of real-world context into business workflows.

*2.2 Challenges of The Internet of Things*

*2.2.1 Security challenge*

Security is known to be an essential pillar of the internet while the major challenge for the IoT. As time goes the trend of IoT expands from millions of devices to tens of billions. As the number of connected devices increases the chance of vulnerabilities also increase, such as low device standard designed (K. sha et al 2016). Due to the increasingly large number of devices in the world which need to be connected to the internet course the spread of numerous nodes and devices being installed to networks present malicious actors with immeasurable attack vectors and opportunities to carry out their malicious deeds, especially since a considerable number of them suffer from security holes. Apart from that, scalability issues also contribute to the creation of insecure IoT products. This is due to the fact that nowadays security solutions being used have been created with generic computing devices in mind. Therefore, IoT devices often lack the computational power, storage capacity and properly operating system to be able to deploy such solutions (Abdulaziz Aldaej, 2019). There three main triangles whereby information security challenges can be identified, namely confidentiality, integrity and availability.

- **Confidentiality**: This is a fundamental challenge for the IoT system whereby data are generated and the system accesses these data dynamically. The key factors to assure confidentiality of data in the IoT system is proper management of data sources and the capability to handle the classified data from a specific device. Confidentiality may not be guaranteed for the current solutions because of big volumes of generated data sources and lack of effective control over dynamically streamed data. To obtain confidentiality, various encryption schemes can be applied as well as current systematic and asymmetric algorithms should be updated before implementing in IoT based applications (D. Mendez et al 2017).
- **Integrity:** deals with the first damages or failures of physical devices. Devices and data can be protected by preserving against disruption. In IoT system data integrity will rely on the robustness and fault tolerance of the entire system. The integrity of the IoT system can be affected by the internal and external source as well as by internal process. For example, in sensor networks, many RFIDs remain unattended most of the time. This gives an opportunity to external attackers to either modify data while storing it to the node or while transferring it to the network (D. Mendez et al 2017). By using password protection might be the possible way out to strengthen the integrity of the systems caused by external and internal sources of attacks. Multilevel security (MLS) helps to avoid unauthorized modifications due to the internal process, such as malicious running code. A trusted platform module (TPM)26 is another hardware solution proposed for integrity challenges.
- **Availability**: to sustain the required level of availability, the IoT system should show the levels of performance requested by the application. The suitable level of hardware and software performance used in the IoT network should be able to cope with the requirements of the users. One example of availability challenge could be demonstrated by denial of service (DOS) attack. DOS attacks prevent devices to access resources from the network. Commands for DOS attack can be generated remotely to obstruct the IoT system (Z. Sheng et al, 2013). DOS attacks in IoT may concern not only the traditional vectors, for instance, resources of providers, bandwidth, etc. but also they can affect the data acquisition of wireless communication from IoT. Implementation of distributed architecture rather than a centralized one can help to improve the availability of the IoT system (D. Mendez et al 2017).

*2.2.2 Privacy challenge*

The significant growth of the IoT availability during the recent year has tremendously increased the risks to privacy breaches. The primary difference between traditional internet and the IoT is the amount of data being collected by the users. This large volume of data collected and analyzed can be used to derive intelligence. Therefore, privacy becomes a great concern, for example, when used in a medical domain, IoT may pose threats to the privacy of people's medical information. When used in the smart home, IoT may expose one's personal life to the outside world, which can be potentially dangerous (K. sha et al 2018). In addition, the issue of privacy in IoT becomes more important in the process of collecting personal data from various environments because sometimes it might include the third party. Faulty provisioning of data, threating its confidentiality and integrity which is very crucial aspects, because it may allow unauthorized users' sensitive data by malicious parties. This issue might become an obstacle towards the widespread adoption of IoT technology, this is due to the fact that information about the personal behavior of the users can be

misused without their permission for commercial purpose. Therefore, an organization should evaluate third-party engineering teams to determine what level of security they apply to their network infrastructure, applications, and APIs (Application Program Interface). And the recommendation should be done for the alternative standard if the level of security is not sufficient (Pooja Yadav et al, 2018).

*2.2.3 Trust Challenge*

Trust is a very crucial component in security design. A big portion of the IoT system is exposed in public areas and communication is done through wireless networks, which makes them vulnerable to malicious attacks (Z. Zang et al, 2015). Trust is fundamental in all human-human and human-technology interactions (economic, business social and political). In this situation, the nodes are communicating with each other establishing social relationships including friendship, ownership and community. Therefore, trust issue remains a challenge for IoT system because friends can share services and resources only when they trust each other. The level of trust between two friends decides their future interactions. Trust attacks on a network aim at breaking the social relationships of friendship, and finally influencing the entire network. Providers of IoT products and services should work towards enhancing trust via proper strategies to achieve specific goals such as human-centred goals, ethical goals and technical goals. To build the trust level between friends in IoT systems, there are various management protocols or mechanisms that are proposed (Spyros G Tzafestas, 2018).

*2.2.4 Connectivity Challenge*

Nowadays, we rely on the centralized, client /server architecture to authenticate, authorize and connect different nodes in a network. The future of IoT will depend on decentralizing IoT networks. This phenomenon can become possible by moving functionality to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of time-critical operations and cloud servers take on data gathering and analytical responsibilities. Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker (Calsoft, 2018). Networks will be implemented in meshes topology with no single point of failure. This model will have its own set of challenges, especially from a security perspective, but these challenges can be met with some of the emerging IoT technologies such as the Phantom protocol.

## 3 Conclusion

Information and Communication Technology (ICT) are essential elements of the global economy as well as today's society and life. For the advancement of technology, both public and private sectors across the world are transforming their countries and businesses with ICT programs ranging from research and innovation, infrastructure building, and skill development. Internet of Things (IoT) is one of the ICT innovations that has attracted various stakeholders around the world. Despite the challenges of IoT system like security, privacy, trust, connectivity and so on but the IoT is assumed as a disruptive innovation to improve the business process within and across public and private sectors. It describes a world where anything can be connected and can interact in an intelligent manner.

## REFERENCES

Abdulaziz Aldaej (2019), "Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)", IEEE Access.

D. Mendez, I. Papapanagiotou and B. Yang, "Internet of Things: Survey on Security and Privacy," Cornell University Library, 2017

Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wangb, Weisong Shi (2018), "On security challenges and open issues in the Internet of Things", *Future Generation Computer Systems* 83 (2018) 326–337

Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wangb, Weisong Shi (2016), "Security in Internet of Things: Opportunities and Challenges", *International Conference on Identification, Information and Knowledge in the Internet of Things*, 512-518.

Keyur K Patel and Sunil M Patel (2016), "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", *International Journal of Engineering Science and Computing*, 6(5), 6122-6131.

Pooja Yadav, Ankur Mittal and Hemant Yadav (2018), "IoT: Challenges and Issues in Indian Perspective" 978-1-5090-6785-5/18/$31.00 © 2018 by IEEE.

Spyros G Tzafestas (2018), "Ethics and Law in the Internet of Things World", School of Electrical and Computer Engineering, National University of Athens, Zographou, GRI5773 Athens, Greece; tzafesta@cs.ntua.gr 99-12

Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann and K. Leung (2013), "A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities," Wireless Communications, IEEE, 20(6), 91–98.

Z. Zang, M. Cho, S. Shieh (2015), "Emerging security threats and countermeasures in IoT, in Proceedings of 10th ACM Symposium on Information, Computer and Communication Security. 1-6.