JOURNAL OF MANAGEMENT AND ACCOUNTING STUDIES 2020(03)

Available online at http://journals.researchub.org

Governance of IoT in order to Move ahead of the calendar & live the future today

***Somayyeh Poolayi*[1*], *Amir H. Assadiyan*[2]**

[1]*Computer Engineering Dep. of Islamic Azad University- (IAUM) Mashhad, Iran*

[2]*University of Applied Science and Technology, Iranian Academic Center for Education, Culture and Research-(ACECR) Khorasan Razavi Branch, Mashhad, Iran*

ARTICLE INFO

Article history:

Received 27 Mar 2020
Received in revised form 21 Jane 2020
Accepted 01 July 2020

Keywords:

IoT,

OT,

IT,

IoT challenges

ABSTRACT

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The Internet of Things (IoT) world may be exciting, but there are serious technical challenges that need to address, especially by developers. In this handwriting, learn how to meet the security, analytics, and testing requirements for IoT applications. A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technologies (OT) and information technology (IT), allowing unstructured machine-generated data to analyze for insights that will drive improvements. The Internet of things (IoT) is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security. Therefore, there are some important challenges in privacy and maintaining security of the Internet of things. In this paper, we are going to list the typical items which can be major challenges facing IoT.

1. Introduction

The **Internet of things** (**IoT**) is a set of physical devices, vehicles, home appliances, and other items connected with electronics, software, sensors, actuators, and network connectivity which enable these objects to send and exchange data, like a network (Brown, 2016; Internet of Things Global Standards Initiative, 2015). Each equipment is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, (Internet of Things: Science Fiction or Business Fact?, 2016) creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention (Vermesan & Friess, 2013; Santucci, 2016; Mattern & Floerkemeier, 2016; Lindner, 2015). When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.

"Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, cameras streaming live feeds of wild animals in coastal waters, (http://www.microwavejournal.com) automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, (Erlich, 2015) or field operation devices that assist firefighters in search and rescue operations (Wigmore, 2014). Legal scholars suggest regarding "things" as an "inextricable mixture of hardware, software, data and service" (Noto La Diega, & Walden, 2016).

These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices (Hendricks, 2015). The quick expansion of Internet-connected objects is also expected to generate large amounts of data from diverse locations, with the consequent

**Corresponding author:* Somayyeh.Poolayi@gmail.com
DOI: https://doi.org/10.24200/jmas.vol8iss03pp38-42

necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. In recent years with the massive growth in global cyber threat, there has been a significant rise in exploitation of IoT technologies for committing cyber terror crimes (Gadish, 2017).

1.1. Challenges

For the IoT industry to thrive there are three classifications of challenges to overcome and this is true for any new trend in technology not only IoT: technology, business and society (http://www.microwavejournal.com; https://blog.apnic.net; https://www.sitepoint.com).

A. Technology

This part is covering all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems and that's not an easy mission, there are many technological challenges, including Security, Connectivity, Compatibility & Longevity, Standards and Intelligent Analysis & Actions (https://www.linkedin.com).

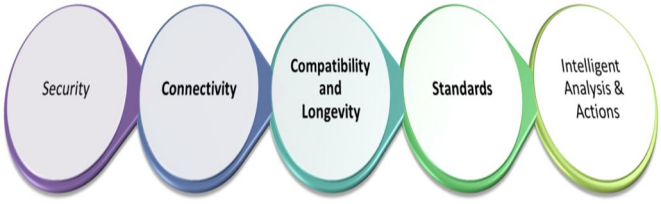

Figure 1. Technological Challenges

Security: IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even the radio in your car are signifying a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes.

The more important shift in security will come from the fact that IoT will become more ingrained in our lives. Concerns will no longer be limited to the protection of sensitive information and assets. Our very lives and health can become the target of IoT hack attacks (http://www.microwavejournal.com).

There are many reasons behind the state of insecurity in IoT. Some of it has to do with the industry being in its "gold rush" state, where every vendor is hastily seeking to dish out the next innovative connected gadget before competitors do. Under such circumstances, functionality becomes the main focus and security takes a back seat.

Connectivity: Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies (https://blog.apnic.net). At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

This model is sufficient for current IoT ecosystems, where tens, hundreds or even thousands of devices are involved. But when networks grow to join billions and hundreds of billions of devices, centralized systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities (https://www.linkedin.com).

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. Networks will be created in meshes 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 Block chain (http://iot.ieee.org).

Compatibility and Longevity: IoT is growing in many different directions, with many different technologies competing to become the standard. This will cause difficulties and require the deployment of extra hardware and software when connecting devices.

Other compatibility issues stem from non-unified cloud services, lack of standardized M2M protocols and diversities in firmware and operating systems among IoT devices.

Some of these technologies will eventually become obsolete in the next few years, effectively rendering the devices implementing them useless. This is especially important, since in contrast to generic computing devices which have a lifespan of a few years, IoT appliances (such as smart fridges or TVs) tend to remain in service for much longer, and should be able to function even if their manufacturer goes out of service.

Standards: Technology standards which include network protocols, communication protocols, and data-aggregation standards, are the sum of all activities of handling, processing and storing the data collected from the sensors (https://www.sitepoint.com). This aggregation increases the value of data by increasing, the scale, scope, and frequency of data available for analysis.

Challenges facing the adoptions of standards within IoT:

***Standard for handling unstructured data*:** Structured data are stored in relational databases and queried through SQL for example. Unstructured data are stored in different types of NoSQL databases without a standard querying approach.

***Technical skills to leverage newer aggregation tools*:** Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

Intelligent Analysis & Actions: The last stage in IoT implementation is extracting insights from data for analysis, where analysis is driven by cognitive technologies and the accompanying models that facilitate the use of cognitive technologies.

Factors driving adoption intelligent analytics within the IoT:

Artificial intelligence models can be improved with large data sets that are more readily available than ever before, thanks to the lower storage

Growth in crowdsourcing and open- source analytics software: Cloud-based crowdsourcing services are leading to new algorithms and improvements in existing ones at an unprecedented rate.

Real-time data processing and analysis: Analytics tools such as complex event processing (CEP) enable processing and analysis of data on a real-time or a near real-time basis, driving timely decision making and action.

Challenges facing the adoptions of intelligent analytics within IoT:

- ***Inaccurate analysis due to flaws in the data and/or model***: A lack of data or presence of outliers may lead to false positives or false negatives, thus exposing various algorithmic limitations
- ***Legacy systems' ability to analyze unstructured data***: Legacy systems are well suited to handle structured data; unfortunately, most IoT/business interactions generate unstructured data
- ***Legacy systems' ability to manage real- time data***: Traditional analytics software generally works on batch-oriented processing, wherein all the data are loaded in a batch and then analyzed

The second phase of this stage is intelligent actions which can be expressed as M2M and M2H interfaces for example with all the advancement in UI and UX technologies.

Factors driving adoption of intelligent actions within the IoT:

- Lower machine prices
- Improved machine functionality
- Machines "influencing" human actions through behavioral-science rationale
- Deep Learning tools

Challenges facing the adoption of intelligent actions within IoT:

- Machines' actions in unpredictable situations
- Information security and privacy
- Machine interoperability
- Mean-reverting human behaviors
- Slow adoption of new technologies

B. Business

The bottom line is a big motivation for starting, investing in, and operating any business, without a sound and solid business model for IoT we will have another bubble , this model must satisfy all the requirements for all kinds of e-commerce; vertical markets, horizontal markets, and consumer markets. But this category is always a victim of regulatory and legal scrutiny.

End-to-end solution providers operating in vertical industries and delivering services using cloud analytics will be the most successful at monetizing a large portion of the value in IoT. While many IoT applications may attract modest revenue, some can attract more. For little burden on the existing communication infrastructure, operators have the potential to open up a significant source of new revenue using IoT technologies.

IoT can be divided into 3 categories, based on usage and clients base:

- **Consumer IoT** includes the connected devices such as smart cars, phones, watches, laptops, connected appliances, and entertainment systems.
- **Commercial IoT** includes things like inventory controls, device trackers, and connected medical devices.
- **Industrial IoT** covers such things as connected electric meters, waste water systems, flow gauges, pipeline monitors, manufacturing robots, and other types of connected industrial devices and systems.

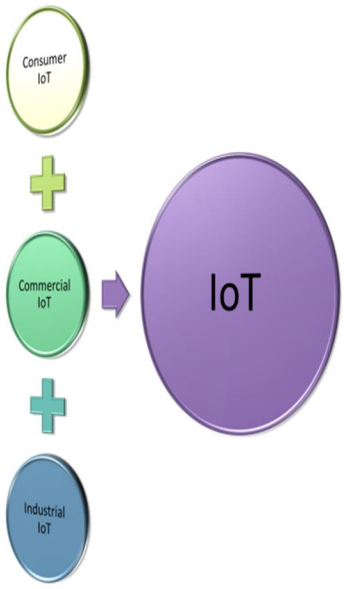

Figure 2. Categories of IoT

Clearly, it is important to understand the value chain and business model for the IoT applications for each category of IoT.

C. Society

Understanding IoT from the customers and regulators prospective is not an easy task for the following reasons:

- Customer demands and requirements change constantly.
- New uses for devices—as well as new devices—sprout and grows at breakneck speeds.
- Inventing and reintegrating must-have features and capabilities are expensive and take time and resources.
- The uses for Internet of Things technology are expanding and changing—often in uncharted waters.
- Consumer Confidence: Each of these problems could put a dent in consumers' desire to purchase connected products, which would prevent the IoT from fulfilling its true potential.
- Lack of understanding or education by consumers of best practices for IoT devices security to help in improving privacy, for example change default passwords of IoT devices.

1.2. Privacy

The IoT creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them.

This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the IoT?

In order to realize the opportunities of the IoT, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technologies and services.

1.3. Regulatory Standards

Regulatory standards for data markets are missing especially for data brokers; they are companies that sell data collected from various sources. Even though data appear to be the currency of the IoT, there is a lack of transparency about; who gets access to data and how those data are used to develop products or services and sold to advertisers and third parties. There is a need for clear guidelines on the retention, use, and security of the data including metadata (the data that describe other data).

2. Conclusions

"Today computers -- and, therefore, the internet -- are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes of data available on the internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code.

The problem is, people have limited time, attention and accuracy -- all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

IPv6's huge increase in address space is an important factor in the development of the Internet of Things. The address space expansion means that we could "assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths." In other words, humans could easily assign an IP address to every "thing" on the planet. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation. Connectivity options for electronics engineers and application developers working on products and systems for the Internet of Things include. Although the concept wasn't named until 1999, the Internet of Things has been in development for decades. The first internet appliance, for example, was a Coke machine at Carnegie Melon University in the early 1980s. The programmers could connect to the machine over the internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.

2.1. List of Symbols

CEP	Complex Event Processing
IoT	Internet of Things
IT	Information Technology
MEMS	Micro-ElectroMechanical Systems
OT	Operational Technologies
SQL	Structured Query Language

REFERENCES

Internet of Things Global Standards Initiative. ITU. Retrieved 26 June 2015.

Internet of Things: Science Fiction or Business Fact? (PDF). Harvard Business Review. November 2014. Retrieved 23 October 2016.

Vermesan, O., & Friess, P. (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.

Santucci, G. (2016). The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects. (PDF). European Commission Community Research and Development Information Service. Retrieved 23 October 2016.

Mattern, F., & Floerkemeier, C. (2016). From the Internet of Computers to the Internet of Things. (PDF). ETH Zurich. Retrieved 23 October 2016.

Erlich, Y. (2015). A vision for ubiquitous sequencing. Genome Research. **25** (10): 1411–1416. doi:10.1101/gr.191692.115. ISSN 1088-9051. PMC 4579324. PMID 26430149.

Hendricks, D. (2015). The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.

http://www.microwavejournal.com/articles/27690-addressing-the-challenges-facing-iot-adoption

https://www.sitepoint.com/4-major-technical-challenges-facing-iot-developers/

https://www.linkedin.com/pulse/iot-implementation-challenges-ahmed-banafa?trk=mp-author-card

https://www.linkedin.com/pulse/why-iot-needs-fog-computing-ahmed-banafa?trk=mp-author-card

https://blog.apnic.net/2015/10/20/5-challenges-of-the-internet-of-things/

Wigmore, I. (June 2014). Internet of Things (IoT). TechTarget.

Lindner, T. (13 July 2015). The Supply Chain: Changing at the Speed of Technology. Connected World. Retrieved 18 September2015.

Noto La Diega, G., & Walden, I. (1 February 2016). Contracting for the 'Internet of Things': Looking into the Nest. Queen Mary School of Law Legal Studies Research Paper No. 219/2016. SSRN 2725913.

Nordrum, Amy (18 August 2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE.

Brown, E. (13 September 2016). Who Needs the Internet of Things?. Linux.com. Retrieved 23 October 2016.

Brown, E. (20 September 2016). 21 Open Source Projects for IoT. Linux.com. Retrieved 23 October 2016.

http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

Gadish, O. (18 July 2017). Cyber Terror: How It Happens And What We Can Do. OGM.

"Molluscan eye". Retrieved 26 June 2015.