# Evaluation of IoT: Challenges and Risks on Communication Systems

Mostafa Alghentawi
*Department of Electrical and Electronic Engineering*
*Karabuk University*
Karabuk, Turkey
Mustafa.alghentawi@gmail.com

***Abstract*— Internet of Things (IoT) is a new-fangled prototype, which supplies a chain of new services/products for the upcoming technological innovations wave. IoTs' applications are roughly boundless in terms of enabling a smooth integration between the digital world and the physical world; where IoT can be implemented everywhere like smart (environment, city or businesses), security, smart business process, home automation, energy sector, education, healthcare and so on. Moreover, despite all the massive efforts of researchers, developers, experts to cover the full potential of IoT, there are still various problems and challenges need to deal with. In this survey paper, we will present a preface on some important aspects, applications and protocols with regards to the emerging area of IoT. This paper also will highlight the challenges of IoT might face, applications that have the possibility to achieve a fundamental change in human life, in addition to the risks of IoT and its impacts on our life in terms of privacy invasion and security issues. Moreover, SWOT Analysis will be conducted by identifying the Internal Factors of the IoT (Strength and Weaknesses) as well as the External Factors (Opportunities and Threats).**

***Keywords*— *internet of things, vision and mission, IoT's architecture, implications of IoT, network protocols, challenges, risks, SWOT analysis***

## I. Introduction

The Internet has become ever-present, where it touched roughly each corner surrounding and affected human life in inconceivable paths. Today, the universe is getting into the Internet of Things era (famous as IoT). The 'IoT' expression has been founded in 1999 [1], whereas the earliest IoT principles have been published shortly after by Neil Gershenfeld in his book 'When Things Start to Think' [2]. Several authors have defined IoT as a term in different ways. Under [6], the authors have gone through two of the most popular definitions of IoT.

The first has defined simply as "an interactivity between the digital and physical worlds using a numerous number of actuators and sensors", while the other has defined as "A model in which networking and computing aptitudes are embedded at any kind of imaginable objects". The purpose of using these aptitudes is to know and control the status of the object or to alter its status if required; for achieving complex functions that need high intelligence.

### A. Vision and Mission Statement

The vision statement concentrates on tomorrow (future) and what the organizations and industries want to ultimately become, while the mission statement concentrates on today and what the organizations or industries do and spend to achieve it. The purpose of displaying those statements is both of them are vital in directing goals in the organizations [7]. Here, we will display the vision and mission statement of three of the most top companies involved in IoT [8,9,10].

- Tesla

*Vision*: "to build the most persuasive vehicles company presently by driving the world's changeover to electric transportations."

*Mission*: "to speed up the world's changeover to green energy."

- Microsoft

*Vision*: "to assist persons and enterprises over the world recognize their complete potentials."

*Mission*: "to enable people and businesses on the earth for implementing more."

- Samsung

*Vision*: "Affect the world with our progressive products and technologies, and layout that emboss people's lives and contribute to social growth by designing a modern future."

*Mission* : "Samsung will devote the technology and human resources to set up top products and services that contribute to a benefidcent global society."

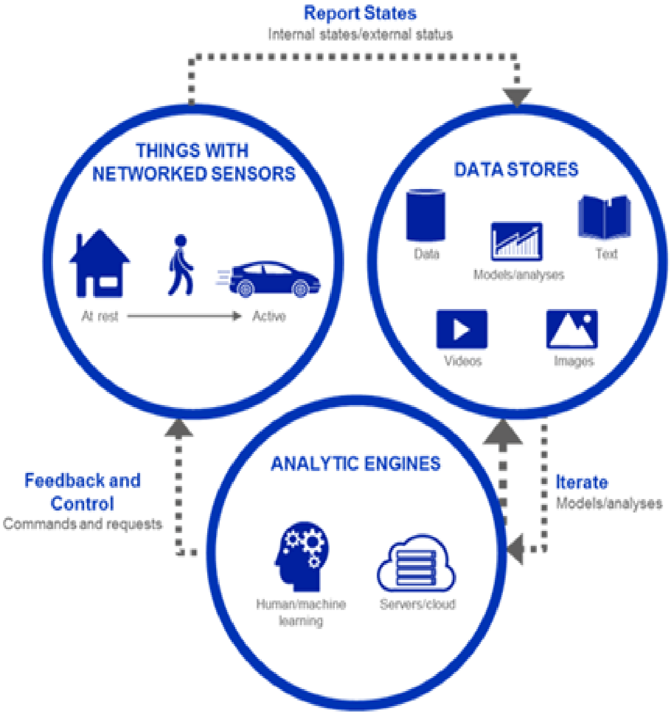


Fig. 1. The Data Processing Stage in IoT

TABLE I. THE BEST IOT COMPANIES IN 2018 [16]

| Name | 2018 CRN IoT Categories |
|---|---|
| SAP | IoT Software and Services |
| ARM | Iot Hardware |
| Google | Iot Hardware |
| Samsara | Iot Hardware |
| Nvidia | Iot Hardware |
| Fortinet | Iot Security |
| Siemens | Industrial IoT Providers |
| Cisco Systems | Iot Hardware |
| Cradlepoint | Iot Security |
| Schneider Electric | Industrial IoT Providers |
| Dell Technologies | Iot Hardware |
| Intel | Iot Hardware |
| Amazon Web Services | IoT Software and Services |
| Sierra Wireless | Iot Hardware |
| GE | Industrial IoT Providers |
| Eaton | Industrial IoT Providers |
| IBM | IoT Software and Services |
| PTC | IoT Software and Services |
| Qualcomm | Iot Hardware |
| Verizon | IoT Software and Services |
| Oracle | IoT Software and Services |
| AT&T | IoT Software and Services |
| SonicWall | Iot Security |
| Ayla Networks | IoT Software and Services |
| Hewlett Packard Enterprise | Iot Hardware |
| Honeywell | Industrial IoT Providers |
| Johnson Controls | Industrial IoT Providers |
| PAS | Industrial IoT Providers |
| ForeScout | Iot Security |
| Eurotech | Iot Hardware |
| Samsung | Iot Hardware |
| Vertiv | Iot Hardware |

## II. IOT REVOLUTION

According to Gartner Research [14], the number of connected things around the world is estimated to reach 14.2 ones thousand million and 25 thousand million in 2019 and 2021 respectivelly. Moreover, Gartner mentioned that the sensor's prices of IoT will be declined in 2019, which will give the means to the companies to use them in order to earn insights in different industries such as retail, energy, manufacturing and others.

In 2020, each of logistics and transportation, discrete manufacturing, and utility industries are separately planning to outlay more than $40 thousand million on IoT services platforms and systems [15].

Also, McKinsey forecasts that the IoT market in 2020 will be worth $581Billion with an annual growth rate ranging from 7-15%. In 2021, only the Industrial market is predicting to reach $123 Billion of IoT with an annual growth rate of 7.3% [15]. Table 1 shows the best IoT companies in 2018 and their specializations [16].

### *A. IoT Components*

The mechanism of IoT is based fully on actuators and sensors apparatus, which ease the interaction with the physical material. The actuators are tools used for creating effects, these effects can make modifications or changes to the environment (Ex: the AC temperature controller), while the sensors are collecting the stored surrounding data and then processing these data intelligently for deriving beneficial inferences from it (Ex: a mobile phone can be considered as a sensor, provided that supply responses about its present status) [6]. Industries are using diverse types of sensors longly. Yet, the revolution of the IoT has taken the development of sensors into an altered level. The below points show the list of the most crucial sensors which extremely being used in the IoT world. For farther details, the explanation of each sensor and its uses can be found in [11].

- Sensors of Temperature
- Sensor of Chemical
- Sensors of Accelerometer
- Sensor of Proximity
- Sensor of Pressure
- Sensor of Smoke
- Sensor of Gas
- Sensors of Level
- Sensor of Water quality
- Sensors of Image
- Sensors of Motion detection
- Sensor of IR
- Sensors of Humidity
- Sensors of Accelerometer
- Sensors of Gyroscope
- Sensors of Optical

The second component is connectivity, where the collected data is transmitted to a cloud infrastructure over different mediums of transportations (Ex: Wi-Fi, cellular networks, Bluetooth, WAN (Wide-Area Networks, etc.,) [13]. The third component is data processing as shown in Fig. 1., after the cloud obtains the collected data, the software starts to process these data whether the data is simple or complicated (Ex: checking the reading temperatures on appliances if it within an appropriate range or identifying objects using visual devices) [13]. Finally, the last main component is the user, where the information can be available to the end user by triggering alarms on their phones or emails [13].

### B. *IoT's Architecture*

IoT's implementation is relying on an architecture which consists of sundry layers ranging from the acquired data layer at the basis, to the application layer upward. The architecture layers are designed to meet the requirements of various organizations whether were private, public or governmental. The Fig. 2. is showing the common layered architecture of IoT. The layered architecture is divided into two separated parts at the top of the internet layer for serving the communication purpose of common media and using data in applications. The two layers at the bottom of the internet layer are contributing to capturing data [17].

- Application layer is accountable for the delivery process of various applications (such as logistics, healthcare, retail, manufacturing, etc) to the end IoTs' users.
- Middleware layer is accountable for essential functions such as information and managing device, beside its responsibility towards access control, semantic analysis, Object Naming Service, data aggregation, information discovery, filtering and information service. It can be run in bidirectional mode, so it is considered as the critical layer in IoT architecture.
- Access gateway layer is responsible for routing, diffusing and subscribing message, besides, it contributing to performing cross-platform communication if needed. This layer is considered as the initial stage of data handling.
- Edge layer is the layer of hardware, where it is comprising of embedded systems (Ex: information processing), sensor networks (Ex: information collection), radio-frequency identification tags (Ex: providing identification and information storage).

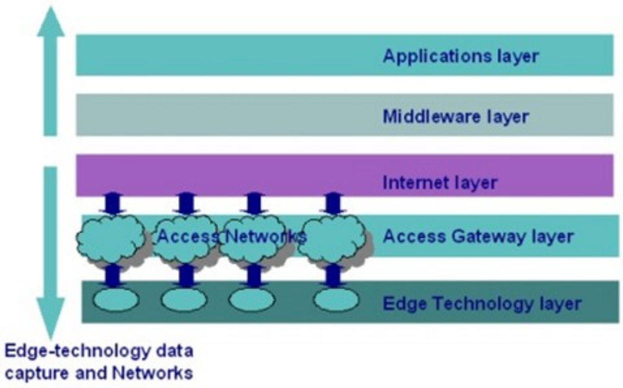


Fig. 2. The Main Layers of IoT Architecture

### C. *Software Architecture Options*

According to [3,4,5], the systems of IoT are involving several trade-offs and design drivers. significant factors include cost, energy efficiency, update, security, communication latency and dynamic programmability. These factors are broadly determining the architecture options that will be shown in Figure 3. On the other hand, software architecture choices are divided into seven classes, ranging from the simple class to the most complicated one as following:

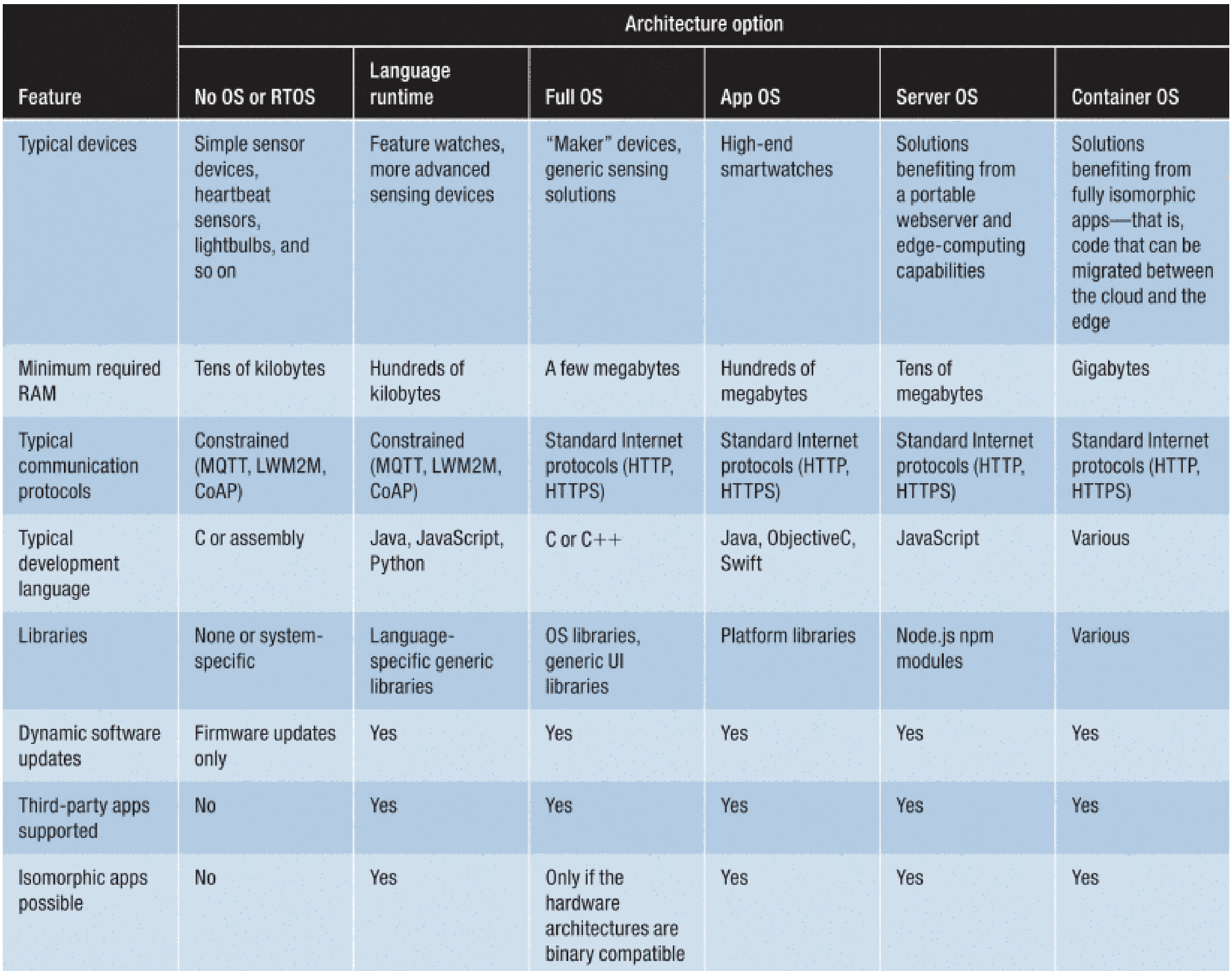
- Architectures of no-OS (Operating System)
- Architectures of language-runtime
- Architectures of server-OS
- Architectures of full-OS
- Architectures of app-OS
- Architectures of RTOS (Real-Time OS)
- Architectures of container-OS

### D. *IoT Security*

Several papers and researches had been done with regards to the area of IoT security, some of them will be reviewed in this section. Hwang and Kim have declared that the standards of security are classified into six groups which they are: authorization, availability, authentication, confidentiality, non-repudiation and integrity. The consequences based on their research were the majority of previous works are dealing with the standards of authentication, authorization, confidentiality and integrity, but the studies on availability and nonrepudiation were insufficient [25]. The security requirements and elements have been mentioned in research conducted by Oh and Kim, these requirements are classified into three groups of IoT characteristics which are resource constraint, heterogeneity and dynamic environment, while the elements are IoT network, server, Platform, user, attacker and cloud [24]. Furthermore, Yun et al. have gone with a study on the method of interworking using Interworking Proxy Entity (IPE) between one-M2M and non-one-M2M systems by applying the OAuth 2.0 framework for the security issues [26]. Yet, there are few limitations that can be used like allowing people to intervene in some scenarios, especially in the process of issuing access token where the login or authorization code is needed. As known, IoT appliances are generally automated, and these appliances are integrated with the security process, while the consequence of appliance use will be limited if the security process is not automated. Therefore, the resource owner password credentials grant form can exceed this restriction in issuing access token. This grant form allows issuing access token with no further process that requires human involvement when the needed data are given in advance. So, only the trusted appliances can use this form, due to; the sensitivity of the resource owner's credentials [12].

### E. *Standards and Protocols*

The greatest number of connected appliances through the internet is known with so-called machine-to-machine (M2M) systems; where the term of M2M is usually used to describe the exchanged information and its performance between the device and network without any assistance by humans.



| Feature | Architecture option | | | | | |
|---|---|---|---|---|---|---|
| | No OS or RTOS | Language runtime | Full OS | App OS | Server OS | Container OS |
| Typical devices | Simple sensor devices, heartbeat sensors, lightbulbs, and so on | Feature watches, more advanced sensing devices | "Maker" devices, generic sensing solutions | High-end smartwatches | Solutions benefiting from a portable webserver and edge-computing capabilities | Solutions benefiting from fully isomorphic apps—that is, code that can be migrated between the cloud and the edge |
| Minimum required RAM | Tens of kilobytes | Hundreds of kilobytes | A few megabytes | Hundreds of megabytes | Tens of megabytes | Gigabytes |
| Typical communication protocols | Constrained (MQTT, LWM2M, CoAP) | Constrained (MQTT, LWM2M, CoAP) | Standard Internet protocols (HTTP, HTTPS) | Standard Internet protocols (HTTP, HTTPS) | Standard Internet protocols (HTTP, HTTPS) | Standard Internet protocols (HTTP, HTTPS) |
| Typical development language | C or assembly | Java, JavaScript, Python | C or C++ | Java, ObjectiveC, Swift | JavaScript | Various |
| Libraries | None or system-specific | Language-specific generic libraries | OS libraries, generic UI libraries | Platform libraries | Node.js npm modules | Various |
| Dynamic software updates | Firmware updates only | Yes | Yes | Yes | Yes | Yes |
| Third-party apps supported | No | Yes | Yes | Yes | Yes | Yes |
| Isomorphic apps possible | No | Yes | Only if the hardware architectures are binary compatible | Yes | Yes | Yes |

Fig. 3. Architecture's Options Used in IoT

*Lightweight M2M Protocol* is responsible for the communication process and used for operating the communication between the M2M objects like M2M management, client software, and service enablement platform, which is included in server software. This protocol also aids in service fulfillment and application management remotely to the devices connected with the internet. Lightweight M2M protocol has some specific features, such as the dependence on efficient and secure Internet Engineering Task Force (IETF) standards (such as Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS)). The interfaces of Lightweight M2M Protocol implicate some processes as services reporting, management processes, and registration [18].

*Constrained Application (CoAP) Protocol* is also responsible for the communication process, but can be considered as a recent one in terms of communication protocols. CoAP is mainly destined for IoT physical tools and insufflated by the Hypertext Transfer Protocol (HTTP). CoAP is using the connection of one-to-one type, but could not support the Transmission Control Protocol/Internet Protocol (TCP/IP) due to its design, which is only suitable for lightweight and thin IoT hardware. Moreover, CoAP uses User Datagram Protocol (UDP) over IP; and is a more efficient and dynamic protocol compared to HTTP, especially when the use of lesser resources and implementations of more features such as executing, observing (notifying any change in the status of server or device), discovering features (finding the surrounding devices), reading and writing [18].

*Message Queue Telemetry Transport (MQTT) Protocol* is a messaging protocol which proceeded over TCP/IP. MQTT is a lightweight communication protocol but it is not M2M communication due to its use of a message broker server between devices. It consists of three major elements (subscriber, broker and publisher). Concerning security area, MQTT supports Transport Layer Security (TLS) and Secure Sockets Layer (SSL) [18].

In general, there what is good and what is better. The choose of the best protocol depends on which category of IoT's application is involved. For example, MQTT is better for WAN network condition due to the existing concept of the broker, while CoAP is better for web services due to its harmonic with HTTP.

## III. IoT Applications

As claimed by John Stankovic in his survey that the main IoTs' applications can be classified into14 fields, where these fields are: retails, smart homes, healthcare, smart factories, environment, smart cities, Lifestyle, user interactions, supply chains, energy, agriculture, transportations, emergency and culture and tourism. However, Stankovic's survey was conducted over 30 countries and he found the most used applications were in 4 areas which are: transportations, healthcare, smart cities and smart homes [18].

### A. *Retail and Logistics*

Retail and supply chain management is a very common term nowadays, so applying IoT in this sector will have lots of advantages, which are including the monitoring of inventory over the supply chain, product tracking and payment processing. Besides, IoT puts forward abundant applications like quick payment solutions, guidance of products places and prices in accordance with the shopping list and control the rotation of products on shelves to automate inventory process within the shop itself or in a warehouse. In this type of IoT's application, two main IoT elements are used, which are WSN and RFID, but the implemented bandwidth range is small. On the other hand, the IoT in logistics may include item location, quality of shipment, flee tracking, storage incompatibility detection, etc. Compared to retail felid, logistics used the same two IoT elements but the difference in bandwidth, where it ranges from medium to large in logistics [21]. Lots of information of IoT domains on retails, supply chain and logistics can be found in [22].

### B. *Smart Cities*

The integration between cities and IoT technologies has created a new term with so-called smart cities as well as led to developing the smartness of cities by launching many applications which will contribute and sustain the development's acceleration in this sector. Some of these applications are the instantaneous monitoring of vibrations for buildings and bridges of the city, monitoring the availability spaces of parking, monitoring the vehicles and traffic jam, sound and visual monitoring of some rough and tough levels within the city, smart highway roads in the option of climate conditions and unexpected circumstances, detection of waste and trash level within the container (waste management), smart parking, noise urban maps, smart lighting, intelligent transportation systems and so on. This domain of IoTs' applications is using single sensors, WSN and RFID as elements of IoT, while the bandwidth is ranging from small to large due to abundant and diversified of its application [21].

### C. *Medical and Healthcare*

The use of IoT technologies has consequence many benefits over the healthcare sector, these benefits can be in tracking for devices, patients as well as the authentication of people and staff (tracking is a function used to identify objects and their motions if required), sensing and automatic data collection [20]. Sensors devices are used to diagnosing patient's status and providing the up to date information about the patient's health. Sensors can be applied to improve the monitoring methods of vital functions like heart rate, temperature, blood pressure, blood glucose, etc. The automatic data collection is applied for automating care, reducing processing time, automating processes and medical inventory management. This domain of IoTs' applications is using WSN, RFID, NFC, Bluetooth WiFi, etc, while the bandwidth is ranging from small to large due to the abundant and diversified of its application [21]. Lots of information on IoT domains in healthcare can be found in [22].

### D. *Environment Domain*

Utilization of IoT technologies is one of the farthest hopeful market segments at the point of conserve the environment; where will be a boost of Wireless Identifiable Devices (WID) usage within the friendly programs that specializes in the environment topics. [17].

## IV. Challenges

The workflows in homes, firms or industries will be characterized by cross-organization integration, which will lead to requiring a high operation dynamic as well as the ad-hoc relations. For now, the availability support of Information and Communication Technologies (ICT) is very slight. The following part highlights the most key challenges that face the IoT technologies so far:

### A. *Network Foundation*

The limitations of the existing IoT's are considered as the prime challenge to IoT in terms of manageability, scalability and mobility [17].

### B. *Security, Privacy and Trust*

The barriers that face IoT in terms of security are:

- Architecture's securing to be ensured at both design and execution time.
- Proactive identification and preservation from the malignant software.
- Proactive identification and preservation from the arbitrary attacks.

The barriers that face IoT in terms of privacy are:

- Data privacy (such as controlling over personal's information) and location privacy (such as monitoring over individual's physical location).
- The necessity for imposing protection laws as well as privacy enhancement technologies.
- The development of tools, standards, protocols and methodologies which will lead to the identity management of objects.

The barriers that face IoT in terms of trust are:

- The necessity to exist a fluid exchange for critical and sensitive data (Ex: the communication with trusty services will be done by smart objects instead of users or organizations themselves).
- Trust must be a key part of IoT's design and its architecture and must be contributed in.

### C. *Managing Heterogeneity*

Overseeing and being in charge of heterogeneous applications, objects, devices and environments account for a major challenge. The challenges can be comprised of:

- Providing smart and useful services by collecting a large amount of surrounded information and data.
- Enhancement in the mechanisms of sensor data stream processing.
- Designing techniques for sensor data discovery.
- Designing a dynamical architecture for sensor storage and networking.
- Sensor data management, correlation and aggregation filtering techniques design.

### D. Regulatory and Legal Issues

It can mainly be applied on devices return to medical, insurance, banking, manufacturing equipment and infrastructure equipment. Most of these issues are complying with chronic and elderly laws such as HIPAA, Directive 95/46/EC, GAMP 5, CFR 21 part 11, etc. These laws may delay in the process of bringing products to the market as well as the rise of their cost over time [23].

### E. Architecture and Standardization Shortage

The persistence of fragmentation in the implementation of IoT may increase the cost and decrease the value of IoT to the end clients [23].

## V. Risks of IoT

IoT is a technology like other technologies that have been invented by humans, where it has many advantages as well as many disadvantages and negative aspects. Any object linked to the Internet has an address called Internet Protocol (IP), this IP indeed is a networking software, and responsible for performing specific tasks as well as the interacting of objects with internet. It can easily be hacked due to the weakness of security system [27]. This part will highlight the critical problems and risks that may face IoT's industry world.

### A. Significant Risks

- Material losses which cause to harming users (Ex, home appliances) by intervening and manipulating their properties.
- The potential of robbery operations due to exploiting location data of those IoT devices (Ex, determining the car Coordinates).
- Monitoring users and privacy issues of sensitive data which might put the user data in a risky position.
- Employing the IoT devices for hacking electronic governments and critical organizations that are fully connected to the Internet [28].

### B. Security Vulnerabilities

In computer security, the vulnerability can be considered as a high weakness point to implement unauthorized actions within the system by attackers. A security vulnerability includes privacy, sabotage and denial of service. Undoubtedly, the effects of sabotage and denial of service can widely be taken into consideration more than concentrating on privacy itself despite its importance. For Instance, "changing the mix ratio of disinfectants at a water treatment plant or stopping the cooling system at a nuclear power plant could potentially place a whole city in instant danger" [23].

### C. Types of IoT Security Gaps

- Weakness in the authentication process [29].
- Vulnerabilities and gaps in communication interfaces between the user and IoT is insecure, where the user can control, access and bypass the device.
- The use of unconfident protocols for data transfer.
- Lack of identification methods where the unauthorized people can log in into most devices easily.
- The simplicity of scanning and knowing the devices linked to the internet.

## VI. Swot Analysis

The issues of IoT are very various and have several aspects that should be taken into consideration, such as business models, enabling technologies, applications, social and environmental effects. Two analyses must be used before launching any service/product into local or globe market. SWOT analysis is one of most important analyses, it will be used in this paper to conclude and summarize the internal factors of IoT as well as the external factors as following below:

### A. Strength Points

- *The possible use of IoT lead to reduce businesses costs and increase the profits over time:* as mentioned above, the earning of IoT use will be up to $123 Billion in 2021 and more with an annual growth rate of 7.3%.
- *Environment-Friendly:* linked appliances to the internet such as smart cars, homes, etc, can be utilized to bring down the harmful emissions and consequently limit the use of energy and help protect the environment.
- *Easiness of Use:* IoT can make the devices connect with each other easily.
- *Innovation:* the studies and sciences conducted, in terms of IoT innovations, have driven the technology industry towards the top.

### B. Weakness Points

- *Security:* which can be considered as the most drawback point in IoT in terms of the possibility of how it can be hacked by some mischievous hackers.
- *Data Challenges:* collect, analyse and store the data are a complex process and not that much simple process as known, where it needs a robust infrastructure that can absorb the amount of data flowing every time and from everywhere.

### C. Opportunities Points

- *Emerging markets:* they are fast-growing zones which enable IoT to swiftly expand.
- *Increase the innovation of wearables devices:* smart-watches and smart-glasses carry the ‘smart’ tag, whereas watches nowadays are not only responsible for knowing time, but also able to record the daily activities and work as small smartphone and more. From this point, it can be transmitted every wearable thing into a smart piece.
- *Infrastructure Management:* as mentioned in weaknesses points that IoT has a weak infrastructure, and by increase the forces and forts on this sector, it may be a strong basis for the IoT.
- *Attractive zone for investors:* IoT brings with it an array of potential investment opportunities.

### D. Threats Points

- *Vulnerability to hackers:* hackers are trying to control the surrounding things; the loopholes of the internet are forming real threats for users through being vulnerable to attack by infiltrators.

- *The possibility of not meeting customers' expectations:* IoT has reached to peak, whereas humans have over-the-top expectations from IoT. These exaggerated hopes put the IoT's products at a risky level if the products defeat to satisfy these expectations.

## VII. Conclusions

The diversity of emerged new devices which connected to the Internet will produce an overflow of data which need to be collected, processed and analysed by the organizations. Despite that the organizations will identify new business opportunities according to this data, new risks will emerge. The IoT has the capability to bring together each aspect of different networks. Hence, security at both levels of networks as well as devices is critical for the IoT's operation. The same intelligence that authorises appliances to perform their tasks has also to enable them to recognize as well as counteract threats.

Safeguarding of the IoT's propagation besides harnessing its economic value at the same time, requires a regular and methodical study of various risk factors. Most of the cyber-attacks are targeting IoT devices, and as observed, the ability of attackers is growing continuously, thus however can predict the severity of attacks in the future and how much these attacks will affect on people’s life, business and the IoT itself.

## References

[1] P. Radanliev et al., "Future developments in cyber risk assessment for the internet of things", Computers in Industry, vol. 102, 2018. Available: 10.1016/j.compind.2018.08.002.

[2] N. Gershenfeld, When things start to think. New York, NY, USA: Henry Holt, 1999.

[3] A. Taivalsaari and T. Mikkonen, "A Taxonomy of IoT Client Architectures", IEEE Software, vol. 35, no. 3, pp. 83-88, 2018. Available: 10.1109/ms.2018.2141019.

[4] A. Celesti et al., "Exploring Container Virtualization in IoT Clouds", Proc. 2016 IEEE Int'l Conf. Smart Computing (SMARTCOMP 16), 2016.

[5] D. Cassel, "JavaScript Popularity Surpasses Java PHP in the Stack Overflow Developer Survey", The New Stack, Mar. 2016, [online] Available: thenewstack.io/javascript-popularity-surpasses-java-php-stack-overflow-developer-survey.

[6] Pallavi Sethi and Smruti R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035.

[7] B. Skrabanek, "Difference Between Vision and Mission Statements: 25 Examples", ClearVoice, 2018. [Online]. Available: https://www.clearvoice.com/blog/difference-between-mission-vision-statement-examples/.

[8] C. ROWLAND, "Tesla, Inc.’s Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2018. [Online]. Available: http://panmore.com/tesla-motors-inc-vision-statement-mission-statement-analysis.

[9] L. GREGORY, "Microsoft’s Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2019. [Online]. Available: http://panmore.com/microsoft-corporation-vision-statement-mission-statement-analysis.

[10] V. MARTIN, "Samsung’s Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2019. [Online]. Available: http://panmore.com/samsung-corporate-vision-statement-corporate-mission-statement-analysis.

[11] R. Sharma, "Top 15 Sensor Types Being Used in IoT - Sensor Types & their IoT use", Finoit Technologies, 2018. [Online]. Available: https://www.finoit.com/blog/top-15-sensor-types-used-iot/.

[12] S. Oh and Y. Kim, "Development of IoT security component for interoperability", Cairo, Egypt, 2017.

[13] DataFlair Team, "How IoT Works - 4 Main Components of IoT System -DataFlair", DataFlair, 2018. [Online]. Available: https://data-flair.training/blogs/how-iot-works/.

[14] Gartner, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", Gartner, 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

[15] L. Columbus, "10 Charts That Will Challenge Your Perspective Of IoT's Growth", Forbes.com, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/#406f0a8c3ecc.

[16] L. Columbus, "The Best IoT Companies To Work For In 2018 Based On Glassdoor", Forbes.com, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/06/19/the-best-iot-companies-to-work-for-in-2018-based-on-glassdoor/#31313d9a3b63.

[17] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization", Wireless Personal Communications, vol. 58, no. 1, pp. 49-69, 2011. Available: 10.1007/s11277-011-0288-5.

[18] C. Sharma and N. Gondhi, "Communication Protocol Stack for Constrained IoT Systems", Bhimtal, India, 2018.

[19] J. A. Stankovic, "Research directions for the Internet of Things", IEEE Internet Things J., vol. 1, no. 1, pp. 3-9, Feb. 2014.

[20] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries, J.Krapelse, RFID Application in Healthcare–Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe, Feb 2009.

[21] R. Porkodi and V. Bhuvaneswari, "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview," 2014 International Conference on Intelligent Computing Applications, Coimbatore, 2014, pp. 324-329.

[22] C. Forsey, "7 Ways IoT Is Changing Retail in 2019", Blog.hubspot.com, 2019. [Online]. Available: https://blog.hubspot.com/marketing/iot-retail.

[23] Peerbits, "Internet of things in healthcare: applications, benefits, and challenges", 2019. [Online]. Available: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html.

[24] W. Nyambi, "The IoT Revolution: challenges and opportunities", Geneva Business News | Actualités: Emploi, RH, économie, entreprises, Genève, Suisse., 2016. [Online]. Available: https://www.gbnews.ch/the-iot-revolution/.

[25] S.-R Oh, Y.-G Kim, "Security Requirements for Internet of Things", IEEE 2017 Platform Technology and Service (PlatCon), pp. 1-6, February 2017.

[26] I.T. Hwang, Y.-G. Kim, "Analysis of Security Standardization for the Internet of Things", IEEE 2017 Platform Technology and Service (PlatCon), pp. 1-6, February 2017.

[27] Jaeseok Yun, Ramnath Chekka Teja, Nan Chen, Nak-Myoung Sung, Jaeho Kim, "Interworking of oneM2M-based IoT Systems and Legacy Systems for Consumer Products", Information and Communication Technology Convergence (ICTC), pp. 423-428, October 2016.

[28] M. Tawfik, A. Almadni and A. Alharbi, "A Review: the Risks And weakness Security on theIoT", IOSR Journal of Computer Engineering, vol. 2278-0661, no. 2278-8727, pp. PP 12-17, 2017.

[29] C. Qiang, G. Quan, B. Yu and L. Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking, vol. 6, no. 6, pp. 1-10, 2013. Available: 10.14257/ijfgcn.2013.6.6.01.

[30] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, A Review on Internet of Things (IoT), International Journal of Computer Applications (0975 8887) Volume 113 -No.1, March 2015.