**Internet of Things**

* Introduction:

The Internet of Things is a novel paradigm shift in the IT arena. The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. While coming to the Things that can be any object or person which can be distinguishable by the real world. Everyday objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but “things” that we do not do normally think of as electronic at all―such as food, clothing; and furniture; materials, parts and equipment, merchandise and specialized items; landmarks, monuments and works of art and all the miscellany of commerce, culture, and sophistication.

The best definition for the Internet of Things would be:

“An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face of situations and changes in the environment”

Internet of Things is maturing and continues to be the latest, the most hyped concept in the IT world. Over the last decade, the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for anyone.

* Opportunities and Scope in IoT:

The IoT will create a huge network of billions or trillions of “Things” communicating with each other. The IoT is not a subversive revolution over the existing technologies, it is comprehensive utilization of existing technologies, and it is the creation of new communication modes. The IoT blends the virtual world and the physical world by bringing different concepts and technical components together: pervasive networks, miniaturization of devices, mobile communication, and a new ecosystem. In IoT, applications, services, middleware components, networks, and end nodes will be structurally organized and used in entirely new ways.

IoT offers a means to look into complex processes and relationships. The IoT implies a symbiotic interaction between the real/physical and the digital/virtual worlds: physical entities have digital counterparts and virtual representation; things become context-aware and they can sense, communicate, interact, and exchange data, information, and knowledge. New opportunities will meet business requirements, and new services will be created based on real-time physical world data.

Everything from the physical or virtual world will possibly be connected by the IoT. Connectivity between the things shall be available to all at a low cost and may not be owned by private entities. For IoT, intelligent learning, fast deployment, best information understanding, and interpreting, against fraud and malicious attacks, and privacy protection are essential requirements.

* The Current Issues in the field of IoT:

The six significant IoT security challenges:

1. Weak password protection
2. Lack of regular patches and updates and weak update mechanism
3. Insecure interfaces
4. Insufficient data protection
5. Poor IoT device management
6. The IoT skills gap

* Bibliography:

1. <https://www.scirp.org/html/56616_56616.htm?pagespeed=noscript>
2. <https://ieeexplore.ieee.org/abstract/document/6851114>
3. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats>