ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol3, Issue 5, May 2016

Future Aspects and Key Challenges of IoT

[1] Bitan Paul, [2] Manik Reshi, [3] Manish Dixit, [4] Drishant Sharma, [5] Dr. B. Shadaksharappa
[1,2,3,4] UG Scholar, Sri Sairam College of Engineering, Bengaluru, India
[5] Professor & HOD (CSE), Sri Sairam College of Engineering, Bengaluru,India

***Abstract*— Embedded industry ensures well laid and efficiently advanced days of transparency in the near future ahead. It's the need as well as call of the hour that we initiate developing IOT configured products, so as to meet the customer needs. The count of people that IoT expects to connect is estimated to be around 28 billion —things to the internet by 2020, having diverse gadgets that range from wearable devices like smart watches to automobiles, embedded appliances, and industrial equipments. Several IoT solutions that have been enlarged so far, functionalities of them and also the technology used. Thereby, we conclude the various challenges that need to be focused on to pave the way to betterment of solutions that will aid the society.**

***Keywords*: Internet of things, RFID, IPv6, Wireless Sensor Network, Smart home.**

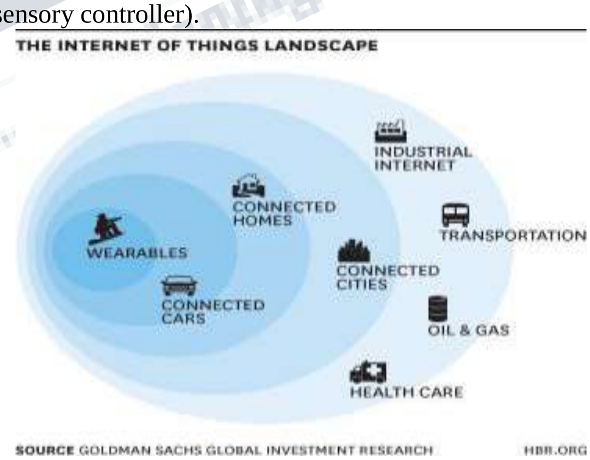
I. AN INTRODUCTION TO THE INTERNET OF THINGS:

The term-Internet of Things (IoT) was primarily coined around 1998 which defines as a network of networks where typically, a large number of objects or sensors are connected via communications and information infrastructure to provide value-added services. It ensured in developing a world where all the objects around us are internet accessible and therefore the communication to each other with redundant human intervention. The utmost goal is to create a better world for humans, where the objects around us acknowledge our desire and hence act accordingly without any external instructions. In a more common manner, it refers to a global, distributed network (or networks) of corporeal objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers. Such 'smart' objects come in a wide range of sizes and capacities, including simple objects with embedded sensors, household Appliances, industrial robots, cars, trains, and wearable objects such as watches, Bracelets or shirts. All these things have certainly changed the entire look of the word connectivity. Internet of Things is on the peak of its existence and it is evident from its benign outcomes. From smart cities, ambience, healthcare, energy, vehicle, transportation, public safety to our day-to-day needs, Internet of Things has completely invigorated these fields.

II. PURPOSE OF IoT OUTCOMES

IoT sometimes is touted as similar to smart systems: smart put-ons, smart houses, smart townships, smart ambience, smart endeavors and the list goes on.

1. Smart Put-ons: Smart puts-on are networked devices that have the capability to collect data, track activities, and advance experiences to user needs and desires. Puts-on solutions are configured for a variety of functions as well as for where on a different of part of body such as the head, eyes, wrist, waist, hands, fingers, legs or embedded into different element of attire. .Puts-on devices are of two types, namely, One standard is based on product forms, including head-mounted (such as glass and helmet), body-dressed (such as coat, underwear, and trousers), hand-worn (such as watch, bracelet, and gloves), and foot-worn (such as shoes and socks). Another standard is based on product functions, including healthy living (such as sport wristband and smart bracelet), information consulting (such as smart glass and smart watch), and somatosensory control (such as somatosensory controller).



2. Smart Houses: Smart House is the technical blend of technology and services through home networking for a better quality of living. A lot of technologies related to Smart House are coming out. Result in this category ensures a complete and contented aura for the occupants as of today. Some smart home solutions also pay interest on giving assistance to the aged people in their day-to-day chores and on healthcare surveillance. Due to the huge market potential, more and more smart home solutions are making their way into the market. Areas of major focuses have been namely on resource management and related phases.

3. Smart Townships: A 'smart township' is a non-rural region that is immensely advanced in terms of overall structural design, maintainable real estate, communications and market viability. It is a city where IT is the principle infrastructure and the core for providing omnipresent services to residents. Many technological aspects are also keenly involved up-to a certain extent. As the need of the hour calls, it will prove to be a benign aspect in the very near future. Urban IOTs, in fact, are designed to support the Smart City vision, which aims at taking advantage of the most customized communication systems to aid added-value services for the admin of the city as well as to its denizens. The application of the IoT exemplar to an urban context is of particular interest, as it responds to the stalwart push of many national governments to adopt IoT solutions in the public affairs management, thus taking into conscience the so-called Smart City concept.

4. Smart Ambience: The Smart Ambience in a city comprises of Smart Governance, Smart Mobility, Smart Utilities, and Smart Buildings. Services enabled by the IOT exemplar in smart city environment might range from Monitoring health building, Management of waste, Monitoring air quality, Monitoring noise, Traffic bottleneck, smart parking , smart lightning, water quality management, natural disaster surveillance ,smart farming and many more.. WNA is a wireless landslide detection system that is capable of releasing alerts about possible landslides caused by torrential rain in the contemporary season. There are many more solutions available providing different ideas in different areas.

5. Smart Endeavors: Enterprise IoT solutions are advanced to support structural design and more general-purpose functionalities in industrial place. Current enterprise strategies already acknowledge a few interfaces to smart items, but because of increased computational as well as communication abilities of these gadgets, the power drifts towards the edges of the network. Intellectual mechanisms for data aggregation, filtering, fusion and conversion can be installed to and executed at the network edge, or within the network, as suitable.

Software is primarily the core innovation driver in many industries and many new business models of the future will heavily rely on the use of such items. Some of the most promising phases are Manufacturing, supply chain integrity, energy and production, health, transportation and logistics. Timely and optimal replacement strategies are determined from context information related to usage patterns.

III. IoT AS A METHODOLOGICAL FORTITUDE

There are three IOT components which enables seamless insidious computing:

a) Hardware - made up of sensors, triggers and embedded communication hardware

b) Middleware – on-demand storage and computing devices for data analytics and

c) Presentation – innovative and easy to understand mental picture and analysis tools which can be widely accessed on diverse podiums and which can be designed for several applications.

The IoT covers a enormous aspect of industries and applications.

1. Radio Frequency Identification (RFID)

RFID can be easily understood as a radio-frequency identification system that makes use of tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers transmit a signal to the tag and acknowledge its response. The readers usually transmit their observations to a computer running RFID software or RFID middleware. RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader. It is more consistent, competent, safe, cheap and precise. RFID has an extensive range of wireless applications.

2. Wireless Sensor Networks (WSN)

A wireless sensor network (WSN) is a collection of distributed sensors that observe corporeal or environmental circumstances, such as temperature, sound, and pressure. Data from each sensor passes through the network in a node-to-node fashion. The parts that sum up the WSN surveillance network consist of:

WSN nodes are inexpensive devices, so they can be developed in high volume. They also operate at low power so that they can run on battery, or even use energy harvesting. A WSN node is an embedded system that typically performs a single function (such as measuring temperature or pressure, or turning on a light or a motor). A WSN edge node is a WSN node that includes Internet Protocol connectivity. It acts as a gateway between the WSN and the IP network. It can also perform local processing, provide local storage, and can have a user interface.

WSN Technologies: There are several candidates that can be selected as WSN technologies. Few of them are discussed here.

Wireless-Fidelity: The first immediate networking technology candidate for an IoT device is Wi-Fi, because it is so necessary. Obviously, Wi-Fi can be a benign solution for many applications. Almost every house that has an Internet connection has a Wi-Fi router. However, Wi-Fi needs a fair amount of power. There are numerous devices that aren't able to afford that level of power: battery operated devices, for example, or sensors situated in locations that are difficult to power from the grid.

IEEE 802.15.4: One of the major IoT enablers is the IEEE 802.15.4 radio standard, released in 2003. Commercial radios meeting this standard provide the basis for low-power systems. This IEEE standard was extended and improved in 2006 and 2011 with the 15.4e and 15.4g amendments. Power consumption of commercial RF devices is now cut in half compared to only a few years ago, and we are expecting another 50% reduction with the next generation of devices.

3. Addressing schemes

[The capability to solely recognize things is critical for the success of IoT. This will not only allow us to uniquely recognize billions of devices but also to monitor remote devices through the Internet. The few most critical features of developing a unique address are: exclusiveness, trustworthiness, perseverance and scalability. Every element that is already connected and those that are going to be connected, must be identified by their unique identification, location and functionalities. The current IPv4 may support to an extent where a group of sharing sensor devices can be identified geographically, but not on individual basis. The Internet Mobility properties in the IPv6 may improve some of the device identification problems; however, the mixed nature of wireless nodes, variable data types, parallel operations and union of data from devices intensifies the problem further IPv6's addressing scheme provides more addresses than there are grains of sand on earth. With IPv6, it is much simpler for an IoT device to obtain a global IP address, which enables efficient peer-to-peer communication.

4. Storage and Data analytics

Primary curb is that this immensely configured world will develop data at an exponential rate, even if not all the data is or ever will be interesting or priced. Storage of data, ownership and termination of the data become grave issues. Hence, data centers which run on harvested energy and which are centralized will assure energy fullness as well as trustworthiness. The data has to be stored and used intelligently for smart surveillance and trigger action. The basic value in an IoT system is in the ability to perform analytics on the gathered data and retrieve useful insights.

IV. CONFORNTATIONS IN BUILDING IoT

The solutions for IoT development confrontation needs to be arrived from methodological, public, legitimate, monetary, and business milieu.

1. Standards and interoperability

Standards are essential in creating markets for new technologies. If devices from diverse manufacturers don't use the similar standards, interoperability will be more difficult, requiring extra gateways to translate from one standard to another. Additionally, a company that observes different phases of a vertical market may overpower a market, stifling competition and creating obstacles for smaller players and entrepreneurs. Diversifying data standards can also tend to lock consumers into one family of products: if consumers can't easily transfer their data when they replace one device with another from a diverse manufacturer, they will in effect lose any advantage from the data they have been gathering over time.

2. Security.

As the IoT conjoins more devices together, it provides more decentralized entry points for malware and spam. Less expensive devices that are in physically compromised locales are more subject to disfigurement. More layers of software, integration middleware, APIs, machine-to-machine communication, etc. create more complexity and new security risks.

3. Trust and Privacy.

With remote sensors and surveillance a core use case for the IoT, there will be heightened sensitivity to controlling access and ownership of data. New compliance frameworks to address the IoT unique issues would be evolved. Social and political concerns in this field may also curb IoT adoption.

4. Complexity, confusion and integration issues.

With several podiums, n-number of protocols and huge numbers of APIs, IoT systems integration and testing will prove to be a key challenge. The confusion around evolving standards is almost sure to slow adoption. The exponential evolution of APIs will likely consume unforeseen development resources that will reduce project teams' abilities to add basic new functionalities. Slower adoption and unforeseen development resource requirements will likely slip schedules and slow time to revenues, which will require additional funding for IoT projects.

5. Evolving configuration, protocol battles and competing standards

There may be several standards that evolve based on diverse requirements checked by device class, power requirements, capabilities and uses. This proposes opportunities for platform vendors and open source advocates to contribute and influence future standards.

6. Concrete use-cases and compelling value propositions.

Lack of clear use-cases will slow down adoption of the IoT. Although technical specifications, theoretical uses and future concepts may do for some early adopters, monotonous adoption of IoT will require well-grounded, customer-oriented communications and messaging around. Detailed explanations of a specific device or technical details of a component won't cut it when buyers are looking for a complete value-added service. IoT providers will have to explain the key pros of their services or face the consequences.

V. POTENTIAL OF IoT IN THE NEAR FUTURE

The advancement of IoT from haughty concept to reality is predicated on the projected advanced growth of smart devices and the joint of cheap infrastructure, connection facility and data. Declining device costs, widespread and persistent connectivity, and an exponential focus on operational efficiency and productivity is leading to widespread deployment of IoT solutions. This fast growth is based on expectations that the IoT will bring malleable pros to businesses and consumers. Those advantages can take different forms for denizens, for businesses and for governments. Consumers can get more personal product or service offers, based on what they actually do or where they are. They can travel more easily by avoiding traffic congestion when their connected car suggests an optional route, based on traffic reported by other vehicles. It can be monetarily beneficial. They can be healthier, safer and more independent due to puts-on devices that provide feedback on health or that monitor the aged in the home. Businesses can provide better products and services by studying how customers behave; they can also explore needs for new products or services. They can protect buildings via far-flung security; secure assets like cars and machinery with location trackers and remote locking devices; and ensure that sensitive products (e.g. pharmaceuticals) are consistently stored in right conditions. They can become more efficient, as in the case of utilities using smart meters to erase waste or loss, or in the case of equipment sellers providing just-in-time preventive maintenance. Farmers can be more productive with smart irrigation that provides water whenever needed. Governments and public authorities can also benefit from the IoT. Road safety can be ameliorated based on data from thousands of drivers. The efficiency of street lighting can be improvised by dimming lights on empty roads. As government works to deliver quality services in increasingly complex environments, devices that have already begun to make life more simpler and more efficient for companies and consumers can also aid create bigger public value.

VI. CONCLUDING REMARKS

The great potential of the IoT appears to be huge, in spite of the range of issues that need to be acknowledged. Section I, reviewed an overview about the IoT concept. Section II reviewed a set of the popular applications which are offered by IoT. Section III focuses on methodological fortitude for the realization of IoT. Section IV and V reviewed a set of challenges faced and future impact of IoT. It can be pondered that new research challenges arise due to the large scale of devices, the connection of the physical and internet worlds, the openness of the systems of systems, and continuing problems of privacy and security.

REFERENCES

[1] IoT for Embedded systems : The new Industrial Revolution. Retrieved from http://www.micrium.com/iot/overview/

[2] R. Davies ―The Internet of things Opportunities and Challenges (May 2015)‖ , European Parliamentary Research Service . Retrieved from www.europarl. europa.eu /RegData/. ../EPRS_BRI(2015)557012_EN.pdf

[3] S. Jankowski, ―The Sectors where the Internet of Things really Matters ― Retrieved from https://hbr.org/2014/10/