ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Getting IoT Ready:From Connected Things to Living in the Data

Jacob Thomas

Assistant Professor, Department of Electronics and Communication Engineering, Believers Church Caarmel Engineering College, Perunad, Pathanamthitta, Kerala, India

Abstract: The Internet of Things (IoT) is rapidly evolving. There is a need to understand challenges in obtaining horizontal and vertical application balance and the key fundamentals required to attain the expected 50 billion connected devices in 2020. The number of Internet-connected devices surpassed the number of human beings on the planet in 2011 and by 2020. Internet-connected devices are expected to number between 26 billion and 50 billion. For every Internet-connected PC or handset there will be 5-10 other types of devices sold with native Internet connectivity. These will include all manner of consumer electronics, machine tools, industrial equipment, cars, appliances, and a number of devices likely not yet invented. The concept of the IoT will disrupt consumer and industrial product markets generating hundreds of billions of dollars in annual revenues, serve as a meaningful growth driver for semiconductor, networking equipment, and service provider end markets globally, and will create new application and product end markets that could generate billions of dollars annually. This paper explores the history of the IoT, some early applications that are already disrupting existing markets, and some interesting applications that have the potential to go mainstream in the next several years. This paper also explain the value chain of companies that creates the IoT in various end markets and attempt to quantify its impact on specific semiconductor, software, device, and service provider end markets.

Keywords: Internet of Things (IoT), RFIDs, Sensors, Machine-to-Machine (M2M) communications.

I. INTRODUCTION

The Internet of Things (IoT) refers to a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers. Connecting physical devices to the Internet is not a new idea, however the rapidly falling cost of sensor and Radio Frequency Identification (RFID) technology and the greater coverage and availability of wireless and mobile networks have opened up new opportunities. The promise of IPV6, cloud computing and also the future social and economic benefits that these developments could offer is stoking current interest in the IoT. The Internet of Things (IoT) is transforming the everyday physical objects that surround us into an ecosystem of information that will enrich our lives. From refrigerators to parking spaces to houses, the IoT is bringing more and more things into the digital fold every day, which will likely make the IoT a multi-trillion dollar industry.

The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics. The Internet of Things is poised to disrupt industries. If it is the next big thing—then getting in soon will be critical to success. In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Cisco forecasts that this figure is expected to double to 25 billion in 2015 as the number of more smart devices per person increases, and to a further 50 billion by 2020.IOT supports the pervasive connectivity of sensors and the need for them to interact with each other i.e., act as both tags and interrogators. In order to support such connectivity and communications, the design and use of low-power chipsets will create a significant impact and consideration on power consumption for future sensors. Ultra-low power designs for chipset circuits have been an ongoing research area, with techniques moving from single gate to multi-gate transistors and to carbon nanotube designs. It is illustrated in fig. 1.

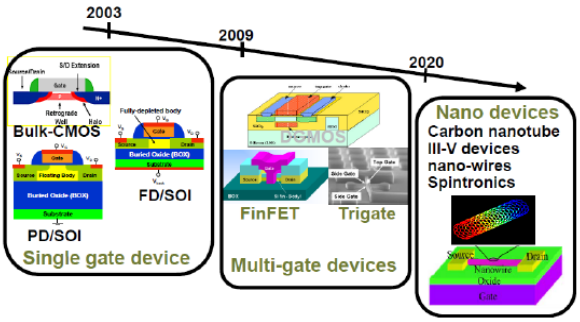

Fig. 1. Low-power chipset designs

The rest of this paper is organized as follows: in Section II the different visions of IoT are reviewed;Section III elaborates the IoT architecture. Section IV describes how the nextevolution ofthe internetis changing everything followed by security and privacy issues of IoT in Section V. Section VI discusses about international activities of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

IoT. Section VII discusses the IoT applications. Finally, Section VIII concludes the paper with future outlook.

II. IoT- Different Visions for a Novel Paradigm

The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. The Internet of Things can enable the next wave of life-enhancing services across several fundamental sectors of the economy. The modern age of business and consumerism is increasingly driven in a global fashion with international brands in many vertical industries. In order to support the development of a viable service ecosystem, i.e. one that meets customer expectations in an economical manner, globally consistent service enablers will be a key requirement. IoT presents an opportunity for new commercial models to support mass global deployments. The majority of revenue is derived from the provision of value added services and operators are building new capabilities to address these new service areas. The IoT will increase the range of services, each requiring varying levels of bandwidth, mobility and latency. For example, services that are related to public safety or personal safety will generally require low latency, but not high bandwidth per se. alternatively, services that provide surveillance might also require high bandwidth. Fig. 2 illustrates some examples of services characterized by their mobility, bandwidth and their sensitivity to latency.

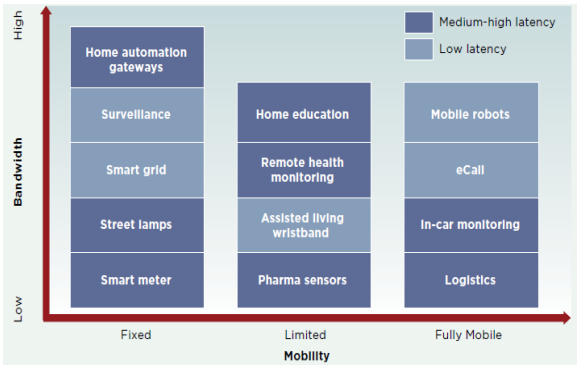

Fig. 2. IoT Service Segmentation

Another important characteristic of IoT services can be the deployment of a large number of the same type of devices and applications. Each device and application performs the same activity and transports information to a service centre at the same time. Regardless of the amount of data transmitted by each device, this simple operation could cause network congestion. Mobile networks need to provide several mechanisms to protect and better utilize their capabilities for delivering such M2M/IoT services. Mechanisms for remotely managing such devices and applications could allow intelligent scheduling, which would facilitate an appropriate application development and reduce the vulnerability of the network to application misbehavior. In today's IT industry, companies are staying competitive by adopting new technologies, streamlining business processes and innovating new services to increase productivity and save costs.In the logistics and supply chain, the traditional supply of goods is based on established agreements between manufacturers and suppliers. Orders are made in advance and tracking is done by various stakeholders in the supply chain, i.e., assembly lines, manufacturers and logistics managers. With the use of smart technologies such as active RFID (executable codes in tag), it is possible to envision that goods may be transported without human intervention from manufacturers to suppliers. Warehouses will become completely automatic with goods moving in and out; forwarding of the goods will be made, using intelligent decisions based on information received via readers and positioning systems to optimize transiting routes. Suppliers will have the flexibility to purchase parts from various manufacturers (possibly from competing manufacturers) and buy them in a sequence of individual orders. Such automation creates a dynamic production and transportation network and provides better asset management to improve the overall efficiency in the supply chain. Several technology trends will help shape IOT. Here are seven identified macro trends: the miniaturization of devices, advances in RFID technologies, Internet Protocol version Six (IPv6), improvements in communication throughput and latency, real-time analytics, adoption of cloud technologies and security. The IPv4 address pool is effectively exhausted, according to industry accepted indicators. The final allocations under the existing framework have now been made, triggering the processes for the Internet Assigned Numbers Authority (IANA) to assign the final five IPv4/8 blocks, one to each of the five regional registries.

With the exhaustion of the IANA pool of IPv4 addresses, no further IPv4 addresses can be issued to the regional registries that provide addresses to organizations.IPv6 is the next Internet addressing protocol that is used to replace IPv4. With IPv6, there are approximately 3.4×1038 (340 trillion trillion trillion) unique IPv6 addresses, allowing the Internet to continue to grow and innovate. Given the huge number of connected devices (50 billion), IPv6 can potentially be used to address all these devices (and systems), eliminating the need of network address translation (NAT) and promoting end-to-end connectivity and control. These features provide seamless integration of physical objects into the Internet world. IoT connects billions of devices and sensors to create new and innovative applications. In order to support these applications, a reliable, elastic and agile platform is essential. Cloud computing is one of the enabling platforms to support IoT.

III.IoT Architecture

IoT architecture consists of different suite of technologies supporting IoT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IoT deployments in different scenarios. The functionality of each layer is described in Fig. 3. The lowest layer is made up of smart objects integrated with sensors. The sensors

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. The miniaturization of hardware has enabled powerful sensors to be produced in much smaller forms which are integrated into objects in the physical world.Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications.

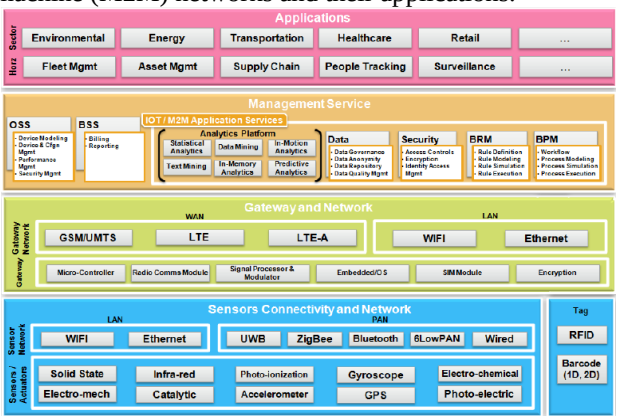

Fig. 3. IOT Architecture

The management service renders the processing of information possible through analytics, security controls, process modelling and management of devices. One of the important features of the management service layer is the business and process rule engines. IoT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to post-processing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IoT system. There are various applications from industry sectors that can leverage on IoT. Applications can be verticalised ones that are specific to a particular industry sector, and other applications such as Fleet Management, Asset Tracking, and Surveillance can cut across multiple industry sectors.

The types of sensing nodes needed for the IoT vary widely, depending on the applications involved. Sensing nodes could include a camera system for image monitoring; water or gas flow meters for smart energy; radar vision when active safety is needed; RFID readers sensing the presence of an object or person; doors and locks with open/close circuits that indicate a building intrusion; or a simple thermometer measuring temperature. The bottom line is that there could be many different types of sensing nodes, depending on the applications. Embedded processing is at the heart of the IoT. Local processing capability is most often provided by MCUs, hybrid microcontrollers/microprocessors (MCUs/MPUs) or integrated MCU devices, which can provide the "real-time" embedded processing that is a key requirement of most IoT applications. Use cases vary significantly, and fully addressing the real-time embedded processing function requires a scalable strategy (using a scalable family of devices), as one size will not fit all. There are a few requirements that make an MCU ideal for use in the IoT such as Energy efficiency, embedded architecture with a rich software ecosystem, Portfolio breadth that enables software scalability, Portfolio breadth that cost-effectively enables different levels of performance and a robust mix of I/O interfaces, Cost-effectiveness, Quality and reliability, Security etc.

IV. How the Next Evolution of the Internet Is Changing Everything?

The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything—including ourselves. This may seem like a bold statement, but consider the impact the Internet already has had on education, communication, business, science, government, and humanity. Clearly, the Internet is one of the most important and powerful creations in all of human history. Now consider that IoT represents the next evolution of the Internet, taking a huge leap in its ability to gather, analyze, and distribute data that we can turn into information, knowledge, and, ultimately, wisdom. In this context, IoT becomes immensely important.

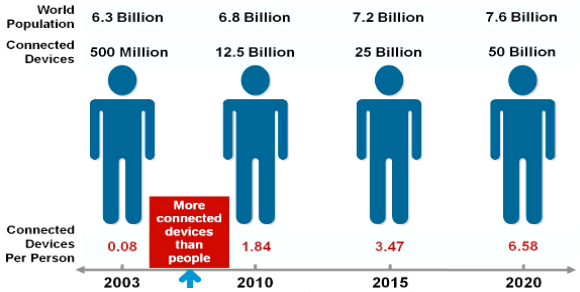

Fig. 4 The Evolution of Internet of Things

Already, IoT projects are under way that promise to close the gap between poor and rich, improve distribution of the world's resources to those who need them most, and help us understand our planet so we can be more proactive and less reactive. Even so, several barriers exist that threaten to slow IoT development, including the transition to IPv6, having a common set of standards, and developing energy sources for millions—even billions—of minute sensors. The Evolution of Internet of Things is shown in Fig. 4. However, as businesses, governments, standards bodies, and academia work together to solve these challenges, IoT will continue to progress. The goal of this paper, therefore, is to educate you in plain and simple terms so you can be

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

well versed in IoT and understand its potential to change everything we know to be true today.

The Internet of Things (IoT) is transforming the everyday physical objects that surround us into an ecosystem of information that will enrich our lives. From refrigerators to parking spaces to houses, the IoT is bringing more and more things into the digital fold every day, which will likely make the IoT a multi-trillion dollar industry in the near future. 20% of companies are investing in sensors, compared to 17% last year. 25% of Top Performers are investing in sensors, up from 18% last year.54% of Top Performers said they will invest more in sensors this year.14% of respondents said sensors would be of the highest strategic importance to their organizations in the next 3–5 years, as compared to other emerging technologies. The IoT can help consumers achieve goals by greatly improving their decision-making capacity via the augmented intelligence of the IoT.For businesses, the Internet of Business Things (IoBT) helps companies achieve enhanced process optimization and efficiencies by collecting and reporting on data collected from the business environment. More and more businesses are adding sensors to people, places, processes and products to gather and analyze information to make better decisions and increase transparency.

V. SECURITY AND PRIVACY

Security and privacy issues should be considered very seriously since IoT deals not only with huge amounts of sensitive data (personal data, business data, etc.) but also has the power of influencing the physical environment with its control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks. In addition, an infrastructure needs to provide support for security and privacy functions including identification, confidentiality, integrity, non-repudiation authentication and authorization. Here the heterogeneity and the need for interoperability among different ICT systems deployed in the infrastructure and the resource limitations of IoT devices (e.g., Nano sensors) have to be taken into account.

While the possible applications and scenarios outlined above may be very interesting, the demands placed on the underlying technology are substantial. Progressing from the Internet of computers to the remote and somewhat fuzzy goal of an Internet of Things is something that must therefore be done one step at a time. In addition to the expectation that the technology must be available at low cost if a large number of objects are actually to be equipped, we are also faced with many other challenges, such as:

Scalability: An Internet of Things potentially has a larger overall scope than the conventional Internet of computers. But then again, things cooperate mainly within a local environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large-scale environments.

Arrive and operate: Smart everyday objects should not be perceived as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and organize and configure themselves to suit their particular environment.

Interoperability: Since the world of physical things is extremely diverse, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Different smart objects would also be subjected to very different conditions such as the energy available and the communications bandwidth required. However, to facilitate communication and cooperation, common practices and standards are required. This is particularly important with regard to object addresses. These should comply with a standardized schema if at all possible, along the lines of the IP standard used in the conventional Internet domain.

Discovery: In dynamic environments, suitable services for things must be automatically identified, which requires appropriate semantic means of describing their functionality. Users will want to receive product-related information, and will want to use search engines that can find things or provide information about an object's state.

Software complexity: Although the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems, a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

Fault tolerance: The world of things is much more dynamic and mobile than the world of computers, with contexts changing rapidly and in unexpected ways. But we would still want to rely on things functioning properly. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.

Power supply: Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. In many scenarios, batteries and power packs are problematic due to their size and weight, and especially because of their maintenance requirements. Unfortunately, battery technology is making relatively slow progress, and "energy harvesting", i.e. generating electricity from the environment (using temperature differences, vibrations, air currents, light, etc.), is not yet powerful enough to meet the energy requirements of current electronic systems in many application scenarios. Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally, not just locally.

For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection. To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyper connected world. In fact, it is increasingly difficult to purchase some devices that are not Internet-connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber-attack, but we can't so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behavior.

This is why security of IoT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact. As we note in the principles that guide our work, ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting trust and use of the Internet. As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don't believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector.

A number of questions have been raised regarding security challenges posed by Internet of Things devices. Many of these questions existed prior to the growth of IoT, but they increase in importance due to the scale of deployment of IoT devices. Some prominent questions include:

a) Good Design Practices. What are the sets of best practices for engineers and developers to use to design IoT devices to make them more secure? How do lessons learned from Internet of Things security problems get captured and conveyed to development communities to improve future generations of devices? What training and educational resources are available to teach engineers and developers more secure IoT design?

b) Cost vs. Security Trade-Offs: How do stakeholders make informed cost-benefit analysis decisions with respect to Internet of Things devices? How do we accurately quantify and assess the security risks? What will motivate device designers and manufacturers to accept additional product design cost to make devices more secure, and, in particular, to take responsibility for the impact of any negative externalities resulting from their security decisions? How will incompatibilities between functionality and usability be reconciled with security? How do we ensure IoT security solutions support opportunities for IoT innovation, social and economic growth?

c) Standards and Metrics: What is the role of technical and operational standards for the development and deployment of secure, well-behaving IoT devices? How do we effectively identify and measure characteristics of IoT device security? How do we measure the effectiveness of Internet of Things security initiatives and countermeasures? How do we ensure security best practices are implemented?

An attacker can use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to a device. A majority of devices along with their cloud and mobile components failed to require passwords of sufficient complexity and length with most allowing passwords such as "1234" or "123456."In fact, many of the accounts we configured with weak passwords were also used on cloud websites as well as the product's mobile application. A strong password policy is Security 101 and most solutions failed. Six of the 10 devices we tested displayed concerns with their Web interface. These concerns were issues such as persistent cross site scripting, poor session management, and weak default credentials. It has identified a majority of devices along with their cloud and mobile counterparts that enable an attacker to determine valid user accounts using mechanisms such as the password reset features. These issues are of particular concern for devices that offer access to devices and data via a cloud website.

VI. INTERNATIONAL ACTIVITIES

Internet of Things activities is gathering momentum around the world, with numerous initiatives underway across industry, academia and various levels of government, as key stakeholders seek to map a way forward for the coordinated realization of this technological evolution. In Europe, substantial effort is underway to consolidate the cross-domain activities of research groups and organizations, spanning M2M, WSN and RFID into a unified IoT framework. Supported by the European Commission 7thFramework program (EU-FP7), this includes the Internet of Things European Research

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Cluster (IERC). Encompassing a number of EU FP7 projects, its objectives are: to establish a cooperation platform and research vision for IoT activities in Europe and become a contact point for IoT research in the world. It includes projects such as CASAGRAS2, a consortium of international partners from Europe, the USA, China, Japan and Korea exploring issues surrounding RFID and its role in realizing the Internet of Things. As well, IERC includes the Internet of Things Architecture (IoT-A) project established to determine an architectural reference model for the interoperability of Internet-of-Things systems and key building blocks to achieve this. At the same time, the IoT Initiative (IoT-i) is a coordinated action established to support the development of the European IoT community.

The IoT-i project brings together a consortium of partners to create a joint strategic and technical vision for the IoT in Europe that encompasses the currently fragmented sectors of the IoT domain holistically. Simultaneously, the SmartSantander project is developing a city scale IoT testbed for research and service provision deployed across the city of Santander, Spain, as well as sites located in the UK, Germany, Serbia and Australia. At the same time large scale initiatives are underway in Japan, Korea, the USA and Australia, where industry, associated organizations and government departments are collaborating on various programs, advancing related capabilities towards an IoT. This includes smart city initiatives, smart grid programs incorporating smart metering technologies and roll-out of high speed broadband infrastructure. A continuing development of RFID related technologies by industry and consortiums such as the Auto-ID lab (founded at MIT and now with satellite labs at leading universities in South Korea, China, Japan, United Kingdom, Australia and Switzerland) dedicated to creating the Internet of Things using RFID and Wireless Sensor Networks are being pursued. Significantly, the need for consensus around IoT technical issues has seen the establishment of the Internet Protocol for Smart Objects (IPSO) Alliance, now with more than 60 member companies from leading technology, communications and energy companies, working with standards bodies, such as IETF, IEEE and ITU to specify new IP-based technologies and promote industry consensus for assembling the parts for the Internet of Things. Substantial IoT development activity is also underway in China, with its 12th Five Year Plan (2011-2015), specifying IoT investment and development to be focused on: smart grid; intelligent transportation; smart logistics; smart home; environment and safety testing; industrial control and automation; health care; fine agriculture; finance and service; military defence. This is being aided by the establishment of an Internet of Things centre in Shanghai (with a total investment over US$ 100million) to study technologies and industrial standards. An industry fund for Internet of Things, and an Internet of Things Union _Sensing China has been founded in Wuxi, initiated by more than 60 telecom operators, institutes and companies who are the primary drivers of the industry.

VII. IoT Applications

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications", see Fig.5. The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth. Smart products have a real business case, can typically provide energy and efficiency savings of up to 30 per cent, and generally deliver a two- to three-year return on investment. This trend will help the deployment of Internet of Things applications and the creation of smart environments and spaces. At the city level, the integration of technology and quicker data analysis will lead to a more coordinated and effective civil response to security and safety (law enforcement and blue light services); higher demand for outsourcing security capabilities.

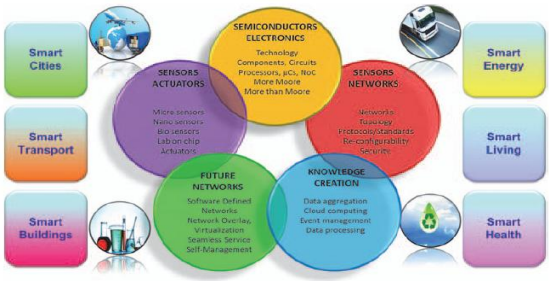

Fig. 5. IOT Applications

At the building level, security technology will be integrated into systems and deliver a return on investment to the end-user through leveraging the technology in multiple applications (HR and time and attendance, customer behaviour in retail applications etc.). There will be an increase in the development of "Smart" vehicles which have low (and possibly zero) emissions. They will also be connected to infrastructure. Additionally, auto manufacturers will adopt more use of "Smart" materials. Let's look at some categories for IoT-related applications. While there are literally hundreds of applications being considered and identified by different industries, they can be categorized in a simple, logical way. Category one encompasses the idea of millions of heterogeneous "aware" and interconnected devices with unique IDs interacting with other machines/objects, infrastructure, and the physical environment. In this category, the IoT largely plays a remote track, command, control and route (TCC&R) role. As with all aspects of the IoT, safety and security are paramount.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

The second category is all about leveraging the data that gets collected by the end nodes (smart devices with sensing and connectivity capability) and data mining for trends and behaviors that can generate useful marketing information to create additional commerce. If needed, command, control and routing functions for tasks and processes today usually done manually, or, if done remotely, that require additional infrastructure. For example, in most homes today, it's a manual process to turn on and off certain lights, set temperature zones and turn on and off a washing machine. In the future, doors, windows, electrical outlets, appliances and many other types of standalone equipment will become "smart" with a unique ID. Those smart devices can then be connected via wired or wireless communication, allowing a user to monitor his or her house remotely, change settings on a refrigerator or washing machine and control household tasks through a laptop or mobile phone. In fact, there are some services offered today by security or Internet service providers to do exactly that, but on a much smaller scale and with fewer capabilities than we expect to see in the future. Energy management is a requirement towards a sustainable environment and the smart grid represents a building block for its realization. Indeed, the spread of renewable energy sources has led to a profound modernization of the traditional electrical distribution system and on the way of distributing energy. The smart grid is defined as an intelligent electrical distribution system that delivers energy flows from producers to consumers in a bidirectional way. Unlike the traditional power grids, where the energy is generated only by a few central power plants and it is ''broadcasted'' to the final customers, via a large networks of cables/ transformers/ substations, in the smart grid the producers may also be the final customers. The energy produced by the customers' micro-grids (e.g., through solar panels, wind turbines) is sent to the grid, which, in turn, manages it appropriately through smart energy control services and stores it in specific energy storages. Monitoring and exchanging information about energy flows are additional applications of the smart grid. Using smart meters, automatic control devices, smart switches, smart appliances, and the grid is able to know in advance the expected demands and to adapt the production and consumption of electricity, consequently avoiding peak loads, eliminating possible blackouts and acting promptly in case of failures/leaks.

VIII. CONCLUSION

The Internet of Things promises to deliver a step change in individuals' quality of life and enterprises' productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks.

REFERENCES

[1] Connectedliving@gsma.com
[2] Ovidiu Vrmesan, Peter Friess-Internet of Things:Converging Technologies for Smart Environments and Integrated Ecosystems.
[3] The Internet of Things Opportunities and challenges: European Parliament, May 2015.
[4] Sensing the future of the Internet of Things, PwC 6th Annual Digital IQ, 2014.
[5] https://connect.innovateuk.org/c/document_library/get_file?folderId=9447195&name=DLFE-102773.pdf
[6] Friedemann Mattern and Christian Floerkemeier: From the Internet of Computers to the Internet of Things, Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich {mattern, floerkem}@inf.ethz.ch
[7] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic,Marimuthu Palaniswamia.
[8] What the Internet of Things (IoT) Needs to Become a Reality, freescale.com / arm.com.
[9] Cisco IBSG, 2010; U.S. Census Bureau, 2010
[10] The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, Dave Evans, April 2011.
[11] Internet of Things-From Research and Innovation to market Deployment, Ovidiu Vrmesan, Peter Friess
[12] Internet of things research study, Hewlett Packard Enterprise.
[13] Reaping the Benefits of the Internet of Things, Cognizant report.
[14] Raymond James, Technology & Communications, U.S. Research Published by Raymond James & Associates.
[15] The Evolution of the Internet of Things, Jim Chase Strategic marketing Texas Instruments.
[16] The Internet of Things vision: Key features, applications and open issues, Eleonora Borgia Institute of Informatics and Telematics (IIT), Italian National Research Council (CNR), via G. Moruzzi 1, 56124 Pisa, Italy.

BIOGRAPHY

Mr. Jacob Thomas received his B. Tech Degree in Electronics & Communication Engineering from St. Joseph's College of Engg. And Technology, Affiliated to Mahatma Gandhi University, in 2007. He got M.Tech in Network and Internet Engineering from Karunya University, Coimbatore, in 2011. At present he is working as Assistant professor in Electronics and Communication Engineering Department, Believers Church Caarmel Engg. College. His research areas include R. F. Communication and Networking.