International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7009(P)
Issue 09, Volume 3 (December 2016) www.ijiris.com ISSN: 2349-7017(O)

SHAPING THE FUTURE OF INTERNET: INTERNET OF THINGS (IOT)

[1]K.H.Anuhya[*], [2]K.John Paul
[1]Department of Electronics, Maris Stella College, Vijayawada, Andhra Pradesh, India
[2]Associate Projects, Cognizant Technology Solutions, Bangalore, Karnataka, India

Abstract-- Internet of Things (IoT) is a new technological revolution of the Internet. IoT is and can be said the expansion of internet services. It is changing the way we work and live by saving time and resources and opening new opportunities for growth, innovation and knowledge creation. Internet of Things is the general idea of things, especially everyday objects that are readable, recognizable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication means .IoT allows everyone to be connected anytime and anywhere. It provides a platform for communication between objects where objects can organize and manage themselves. Objects can be communicated between each other by using radio frequency identification (RFID), wireless sensor network (WSN), Zigbee, etc. IoT is embodied in a wide spectrum of networked products, systems and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible.

Keywords: Internet of Things, RFID, WSN, networked products, sensors

1. INTRODUCTION:

Internet of Things (IoT) refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate exchange and consume data with minimal human intervention. Data can be derived from any number of IoT devices such as sensors and actuators. The data may come in any manner of shape and form ranging from temperature, pressure, motion, and distance. Typically sensors connect through a gateway because they cannot communicate directly over the internet. Getting the connector to communicate over the wide area network or the internet requires connecting in an open interoperable, scalable and secure manner. On the web, when people talk through services they are using a single protocol, HTTP – which is open and interoperable. In the same way, IoT devices need to be connected in an open, a scalable manner, where everything is interoperable and secure.

The Internet of Things (IoT) encompasses many aspects of life from connected homes and cities to connected cars and roads, roads to devices that track individual's behavior and use the data collected for push services. The large-scale implementation of IoT devices promises to transform many aspects of the way we live. New IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving toward a vision of the "smart home'', offering more security and energy efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost. IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors.

Statistics predict one trillion Internet-connected devices by 2025 and define mobile phones as the eyes and ears of the applications connecting all of those connected things. By these internet of things billions objects can communicate over worldwide over a public, private internet protocol network. In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Smart cities, Smart cars, Public safety, Smart Industries and Environmental Protection has been given the high intention for future protection by IoT Ecosystem. Due to internet of things hospitals are shifting to remote self-monitoring for patients. Due self-monitoring it gives the patient greater freedom and independence for their health and free the equipment for emergency purpose for patients.

II. ADVANCEMENTS IN TECHNOLOGIES:

Radio Frequency Identification (RFID) and sensor network technologies will rise to meet the new challenge, in which information and communication systems are invisibly embedded in the environment around us. This result in the generation of enormous amounts of data which have to be stored processed and presented in a seamless, efficient, and easily interpretable form. The advancements and convergence of micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics has resulted in the development of miniature devices having the ability to sense, compute, and communicate wirelessly in short distances. These miniature devices called nodes interconnect to form a wireless sensor networks (WSN) and find wide application in environmental monitoring, infrastructure monitoring, traffic monitoring, retail, etc. For the realization of a complete IoT vision, an efficient, secure, scalable and market oriented computing and storage resourcing is essential. Cloud computing is the most recent paradigm to emerge which promises reliable services delivered through next generation data centers that are based on virtualized storage technologies. This platform acts as a receiver of data from the ubiquitous sensors, as a computer to analyze and interpret the data, as well as providing the user with easy to understand web based visualization. The ubiquitous sensing and processing works in the background, hidden from the user.

III. IOT ELEMENTS:

The aids in defining the components required for Internet of Things from a high level perspective which enables seamless ubiquitous computing are:

a) Hardware - made up of sensors, actuators and embedded communication hardware
b) Middleware - on demand storage and computing tools for data analytics and
c) Presentation - novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

3.1. RADIO FREQUENCY IDENTIFICATION (RFID)

RFID technology is a major breakthrough in the embedded communication paradigm which enables design of microchips for wireless data communication. Radio Frequency identification assigns a unique identification to the objects. RFID is used as more secure identification and for tracking/locating objects, things, vehicles. They help in automatic identification of anything they are attached to acting as an electronic barcode. The passive RFID tags are not battery powered and they use the power of the reader‘s interrogation signal to communicate the ID to the RFID reader. This has resulted in many applications particularly in retail and supply chain management. The applications can be found in transportation (replacement of tickets, registration stickers) and access control applications as well. The passive tags are currently being used in many bank cards and road toll tags which are among the first global deployments. Active RFID readers have their own battery supply and can instantiate the communication. Of the several applications, the main application of active RFID tags is in port containers for monitoring cargo.

3.2. WIRELESS SENSOR NETWORKS (WSN):

Recent technological advances in low power integrated circuits and wireless communications have made available efficient, low cost, low power miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments. Active RFID is nearly the same as the lower end WSN nodes with limited processing capability and storage. Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics. The components that make up the WSN monitoring network include:

a) WSN hardware - Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. Almost always, they comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.

b) WSN communication stack - The nodes are expected to be deployed in an adhoc manner for most applications. Designing an appropriate topology, routing and MAC layer is critical for scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base 8 station. Node drop outs, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.

c) WSN Middleware - A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner. This is based on the idea of isolating resources that can be used by several applications. A platform independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA). OSWA is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE) by the Open Geospatial Consortium (OGC).

d) Secure Data aggregation - An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors.

As node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

IV. APPLICATIONS AND THE FUTURE:

There's already over 29 billion things connected, and recording, and processing data. There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement. We categorize the applications into four application domains: (1) Personal and Home (2) Enterprise (3) Utilities and (4) Mobile. There is a huge crossover in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company which can in turn optimizes the supply and demand in the Utility IoT. Internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities. The sensor information collected is used only by the individuals who directly own the network. Usually Wi-Fi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound).

Ubiquitous healthcare has been envisioned for the past two decades. IoT gives a perfect platform to realize this vision using body area sensors and IoT backend to upload the data to servers. For instance, a Smartphone can be used for communication along with several interfaces like Bluetooth for interfacing sensors measuring physiological parameters. So far, there are several applications available for Apple iOS, Google Android and Windows phone operating system that measure various parameters. However, it is yet to be centralized in the cloud for general physicians to access the same. An extension of the personal body area network is creating a home monitoring system for aged-care, which allows the doctor to monitor patients and elderly in their homes thereby reducing hospitalization costs through early intervention and treatment. Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. This will see consumers become involved in the IoT revolution in the same manner as the Internet revolution itself.

Most of us have interacted with speech recognition with our Smartphone, which often begins with a button press. IoT allows for speech recognition without having to hit a button, and enables ultra-low-power, high-accuracy command sets. The majority ofIoT systems today tend to think of voice recognition being within the cloud, and there are complex speech recognition features that make sense to be there. But there is tremendous value in on-board speech recognition within sensors and devices. This enables better human interface and enables endpoints to communicate amongst themselves and from device-to-cloud. This meshed speech capability concept enables IoT developers to optimize where the speech features are placed.

Social networking is set to undergo another transformation with billions of interconnected objects. An interesting development will be using a Twitter-like concept where individual things in the house can periodically tweet the readings which can be easily followed from anywhere creating a Tweet of Things (ToT). Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized.

V. CONCLUSION:

The Internet of Things is happening now. It's important that we think about it in the same way we think about the Internet itself. Like the Internet, the IoT is a platform, a platform that sends and receives massive amounts of data, from people to devices, from devices to people, and from device to device. That constant exchange of data, that foundation of information, enables powerful new services to be built. Services that connect us to the physical world around us, services that make the world work better. And services that enable entirely new business and revenue streams. It promises to offer a revolutionary, fully connected "smart" world as the relationships between objects, their environment, and people become more tightly intertwined. Yet the issues and challenges associated with IoT need to be considered and addressed in order for the potential benefits for individuals, society, and the economy to be realized.

REFERENCES

[1].Internet of Things (IoT): A vision, architectural elements, and future directions
[2].J Gubbi, R Buyya, S Marusic, M Palaniswami - Future Generation, 2013 – Elsevier
[3].Internet of Things: Challenges and Opportunities
[4].SC Mukhopadhyay, NK Suryadevara - Internet of Things, 2014 – Springer
[5].Internet of Things: An Overview-Internet Society, October, 2015.
[6].Internet of Things-From Research and Innovation to Market Deployment
[7].Dr.Ovidiu Vermesan, SINTEF, Norway and Dr.Peter Friess, EU, Belgium, River Publishers, Aalborg.

