INTERNATIONAL JOURNAL OF
CURRENT MULTIDISCIPLINARY STUDIES
Available Online at http://www.journalijcms.com
Vol. 2, Issue, 6, pp.328-332, June, 2016

IJCMS

RESEARCH ARTICLE

INTERNET OF THINGS (IOT): INTRODUCTION, ARCHITECTURE, TECHNOLOGIES AND APPLICATIONS

Vishal Pawar[1]., Vinay Soni[2] and khusboo pawar[3]

[1,2]Acropolis Technical Campus Indore
[3]Mahakal Institute Of Technolgy ujjain

ARTICLE INFO

Received 18 th, March, 2016,
Received in revised form 27 th,
April, 2016, Accepted 13 th, May, 2016,
Published online 28th,June , 2016

Keywords:

Internet of Things, IoT, RFID, EPC, Barcode, Wi-Fi, Bluetooth, NFC, Sensors, Actuators.

ABSTRACT

One of the popular word in the Information Technology is Internet of Things (IoT). The Internet of Things may be a hot topic in the industry but it's not a new concept. In the early 2000's, Kevin Ashton was laying the groundwork for what would become the Internet of Things (IoT) at MIT's AutoID lab. Ashton was one of the pioneers who conceived this notion as he searched for ways that Proctor & Gamble could improve its business by linking RFID information to the Internet. The concept was simple but powerful. The future is Internet of Things, which will transform the real world objects into intelligent virtual objects. The IoT aims to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things. Although this research paper focuses on definitions, geneses, basic requirements, characteristics and aliases of Internet of Things. The main aim of this paper is to provide an introduction of Internet of Things, architectures, and main technologies and their usages in our daily life. However, this paper will help new researchers, who want to do research in this field of Internet of Things and gives knowledge accumulation in efficiently.

INTRODUCTION

In general, the "Internet of Things" is the networking of physical objects connecting through the Internet. The Internet of Things is not a new concept, as devices have been communicating with each other for a number of years. The difference now is that:

- electronic devices and everyday objects, especially consumer products, are increasingly being built to communicate through sensors and Internet connectivity;
- sensors are becoming more sophisticated;
- objects and devices have the ability to seamlessly connect and communicate a wide range of online and offline information (including location, biometrics, purchases, and online browsing history);
- Internet of Things computing devices are becoming affordable and accessible for individuals and organizations of all sizes, including small- and medium-sized enterprises (SMEs); and cloud computing and Big Data analytics are available for all organizations to store information, share it, and make inferences about their clientele.

If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could be communicate with each other and be managed by computers. In a 1999 article for the RFID Journal Ashton wrote:

"If we had computers that knew everything there was to know about things—using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data."[1]

Challenges

- How would we connect everything on the planet?
- What type of wireless communications could be built into devices?

*✉ ***Corresponding author: Vishal Pawar**
Acropolis Technical Campus Indore

- What changes would need to be made to the existing Internet infrastructure to support billions of new devices communicating?
- What would power these devices?
- What must be developed to make the solutions cost effective?

Definitions

There is no unique definition available for Internet of Things that is acceptable by the world community of users. In fact, there are many different groups including academicians, researchers, practitioners, innovators, developers and corporate people that have defined the term. There are a variety of definitions and graphical representations[2] of the Internet of Things, most of which include the following elements:

- cheap, ubiquitous and uniquely identifiable sensors, devices or “things;”
- the means to react or carry out a command;
- integration into a dynamic global network infrastructure or “network of networks;”
- use of standard and interoperable communication protocols;
- connection of the physical world with the cyber world;
- both physical and virtual “things” that have “identities, physical attributes, and virtual personalities”;
- §devices that communicate without human intervention and are “self-configuring;” and
- devices that generate data stored in the cloud and involve data processing, aggregation and analytics.[3]

The best definition for the Internet of Things would be:

Figure 1 Internet of Things Schematic showing the end users and application areas based on data

“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” .The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [4]. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before.
Architectural view

Main components

Most of us think about “being connected” in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what’s called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. There are three IoT components: 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.

Some of the technologies involved

There are several technologies involved in the Internet of Things, such as radio-frequency identification (RFID), near-field communications (NFC), machine-to-machine communication (M2M) as well as wireless sensor and actuator networks.

RFID is an important enabling technology for the Internet of Things and is used mainly for tracking and tracing objects. It provides the ability to link all manner of inanimate objects from our daily life.[5] RFID technology is a major term in the embedded communication paradigm which enables design of microchips for wireless data communication. They help in automatic identification of anything they are attached to acting as an electronic barcode [6,7].

- 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 is 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.

NFC can be understood as having evolved from RFID and is a short-range, low-power wireless way to transfer small amounts of data between devices. [8]

M2M communication generally refers to the Internet of Things for industrial, business and commercial applications, while the

Internet of Things is discussed more in the context of consumer applications.[9]

Wireless sensors are different from RFID technologies in that they measure features of our physical environment, such as pressure, heat and humidity.[10] Active RFID is nearly the same as the lower end WSN nodes with limited processing capability and storage. The scientific challenges that must be overcome in order to realize the enormous potential of WSNs are substantial and multidisciplinary in nature [11]. 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:

- 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 .
- 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 station.
- 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 [12].
- 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 [13].

Actuators convert information or energy from sensors into action by transmitting it to another power mechanism or system, such as heating or cooling a room.[14] No human intervention need be involved in the decision-making process.[15]

Applications

There are many application areas which will be improved by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact. We classify the applications into four application domains: (1) Personal and Home; (2) Utilities; (3) Mobile.

Personal and Home

Internet of Things technologies are now being made available to consumers who are willingly bringing these technologies into their homes. “Smart,” Internet-connected devices for use in the home.The sensor information collected is used only by the individuals who directly own the network. Usually WiFi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound). 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. Smart fridges can prevent food spoilage, saving consumers money; smart meters can control energy consumption; smart home monitoring can ensure security. However, all of these devices come with a privacy cost which may not be immediately apparent to those who choose to use them.

European Union Agency for Network and Information Security anticipates three likely patterns in the development of smart home technology:

- a fully decentralized smart home where each device is autonomous and which makes use of the existing home network to the Internet and transmits data to the service provider in the cloud;
- a home with an enabled local connectivity between smart devices, without the use of connection to cloud services and without a central getaway; and
- a home with a central hub where a central software system—and accessible from one central device—coordinates.
- 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.
- Smart Meters: connecting homes to the wider grids.

Many homes in Canada, are currently equipped with smart electricity meters which can better manage consumption and find efficiencies. Smart meters measure and record consumption times and levels and transmit this information automatically to the power authority. They make it possible to introduce time-of-use pricing to encourage ratepayers to shift their electricity use to times of lower demand[16] and are growing in popularity largely to address the challenges of an aging electrical grid.[17] An added advantage is that billing can be much more accurate when use is measured and transmitted in small increments – usually hourly but sometimes as small as every 10 minutes. Early versions of smart meters communicated only one way: from the meter to the utility company. Newer models also allow the users to learn about their energy consumption. The Green Button Initiative pilot launched in 2013 in Ontario enables users to share their electricity data with a third party through an app to help them monitor their consumption and find efficiencies.[18] This common data standard is being implemented in other North American jurisdictions.[19] A feature related to smart meters is the utility company installing, with the consent of the user, a device which allows the utility to remotely adjust home energy consumption during peak consumption periods, such as setting a higher thermostat temperature during a heat wave, to ease pressure on the electrical grid.[20]

Utilities

A smart TV is any television that can be connected to the Internet to access streaming media services and that can run entertainment apps, such as on-demand video-rental services, Internet music stations or Web browsers. Higher-end models have built-in video cameras, microphones, and voice and gesture recognition. Smart TVs can be inherently smart if they have an internal microprocessor and Internet access capability, or they can be regular TVs made smart by being connected to a set-top box like Roku, Apple TV or Fire TV, which enables Internet access and streaming. In 2013, it was estimated that 25% of Canadian households, a full one in four, already had a smart TV; this number was projected to increase to 40% by 2015.104 The level of market penetration for these new smart TVs or smart options has accelerated to the point where fewer and fewer “dumb” TVs are even available anymore.

The fact that smart TVs can connect to many other devices wirelessly, such as laptops, wireless keyboards, mice, smartphones and tablets to facilitate text entry, navigation, web browsing and content sharing is considered a major step towards a convergence of computing and entertainment. It also provides the consumer with the capacity to have content literally at the touch of his or her many devices — for instance, seamlessly moving from watching a movie on one device to another, starting from where the user left off, or wirelessly displaying pictures from a smartphone onto the TV screen. As smart TV interconnectivity continues to develop, a smart TV could potentially take content from any source (TV, movie, podcast, social media), observe consumption and viewing habits and make intelligent recommendations or serve ads based on the analysis of the content being consumed across media and platforms.[21]

Ubiquitous healthcare [22] 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.

Mobile

Another smart home technology that is gaining a significant foothold in consumers’ homes is security systems. While established home security companies are updating their products, new entrants, such as local telecommunications providers, independent developers and giants such as Google and (soon) Apple,[23] are all leveling the playing field and competing for a share of this growing market. In years past, surveillance systems were limited to commercial enterprises such as banks, warehouses and airports.smartphone apps. Notwithstanding the selected device or system, they usually provide features such as: smart door locks; garage openers; video cameras; night vision; door and window sensors; and movement, fire and temperature sensors. Security systems can be self-monitored or monitored by a third party—for instance, by a telecommunication or home security company. Self-monitored systems have a two-way communication between the system and the user and the data being collected can also be stored in the cloud. Monitored systems, on the other hand, are installed by a security or telecommunication company and will additionally stream back certain data to the company. Certain companies are teaming up with data analytics providers to offer more tailored advice or solutions to a given user.As technology evolved and prices dropped, it became feasible to set up a network of real-time, high-definition surveillance cameras in the home to be monitored either by third parties (including security firms and telecommunications companies). In the US, those who opt to install such systems can be rewarded with lower home insurance rates as a reward for minimizing the attractiveness of their home to criminals.nanny-cam,” a small camera typically installed inside a doll, named for monitoring child care providers. Another is the “peep-hole camera,” which can photograph anyone who comes within a certain distance, be they visitors, couriers, vandals or thieves. Newer cameras can be motion activated, and set to send an e-mail or text alert to a smartphone upon activation.[24]

CONCLUSION

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.The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps. 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 *TweetOT*. Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized . The framework allows networking, computation, storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment.

References

1. Digital Life in 2025, Pew Research Internet Project, March 11, 2014. Retrieved: May 12, 2015.
2. See the European Research Cluster on the Internet of Things web site.
3. See, for example, the Internet of Things: From Research and Innovation to Market Deployment report of the European Research Cluster on the Internet of Things (IERC), 2014. Retrieved: May 12, 2015.
4. Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of “Internet of Things”. *First International*

Conferenc on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435

5. For more detail, see Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*. Wiley-ISTE, 2010, p.18: mechanical (e.g. position, force, pressure, etc), thermal (e.g. temperature), electrostatic or magnetic fields, radiation (e.g. electromagnetic, nuclear), chemical (e.g. humidity, ion, gas concentration), biological (e.g toxicity), military (enemy tracking or battlefield surveillance).
6. E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, et al., Building the Internet of Things Using RFID The RFIDEcosystem Experience, IEEE Internet Computing 13 (2009) 48–55.
7. A. Juels, RFID security and privacy: A research survey, IEEE Journal of Selected Areas in Communication 24 (2006) 381–394.
8. Jamie Carter, “What is NFC? Everything you need to know” *Tech Radar*, January 16, 2013. Retrieved: May 12, 2015.
9. For more detail, see Alain Louchez, “The Internet of things — Machines, businesses, people, everything.” *ITU News*, No. 6, 2013. Retrieved: May 12, 2015.
10. For more detail, see Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*. Wiley-ISTE, 2010, p.18.: mechanical (e.g. position, force, pressure, etc.), thermal (e.g. temperature), electrostatic or magnetic fields, radiation (e.g. electromagnetic, nuclear), chemical (e.g. humidity, ion, gas concentration), biological (e.g. toxicity), military (enemy tracking or battlefield surveillance).
11. Butler, D. (2020) Computing: Everything, Everywhere. *Nature*,**440**, 402-405. http://dx.doi.org/10.1038/440402a
12. A. Ghosh, S.K. Das, Coverage and connectivity issues in wireless sensor networks: A survey, Pervasive and Mobile Computing. 4 (2008) 303–334.
13. Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, N. Xiong, Secure Data Aggregation in Wireless Sensor Networks: A Survey, in: 2006: pp. 315–320.
14. Ángel Asensio, Álvaro Marco, Rubén Blasco, and Roberto Casas. Protocol and Architecture to Bring Things into Internet of Things, *International Journal of Distributed Sensor Networks*, [15] April 2014. Retrieved: May 12, 2015.
15. Melanie Swan, Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensors and Actuator Networks*, 2012, 1(3), 217-253. Retrieved: May 12, 2015. 2014 Report of the Office of the Auditor General of Ontario, p.362, Retrieved: April 1, 2015. The Report also concludes that estimated benefits related to smart meter implementation were higher than those of the actual current results.
16. More information is available from Hydro One’s Smart Meter site, Retrieved: April 2015. [18]“Ontario’s Green Button: Providing You with Access to Your Energy Data,” Retrieved: April 1, 2015.
17. Green Button: Helping You Find and Use Your Energy Data,” Retrieved April 1, 2015.
18. “Save on Energy,” Retrieved: April 1, 2015.
19. Dan Shust, Vice President of the RI Lab at Resource Interactive, quoted by Jay Donovan in “Smart TVs: How Do They Work?,” *TechCrunch*, January 13, 2012, Retrieved: April 2, 2015.
20. Dodson, S. (2008) The Net Shapes up to Get Physical. Guardian.
21. Google and Apple are both positioning themselves to be key leaders in smart home security; Google is acquiring startups such as Nest, a smart thermostat and Dropcom, a closed circuit camera developer so as to combine the two devices. Apple has launched HomeKit, a software framework that can be used by app and hardware developers for communicating with and controlling connected accessories in a user’s home. For more details, see “Smart homes: ‘My home, my comfort’, say readers,” Open Roboethics Initiative, October 28, 2014, Retrieved: April 2, 2015.
22. Richard Davis, “How surveillance systems save money on insurance,” January 24, 2014, Retrieved: April 2, 2015. While it is unclear whether this is currently the case in Canada, it is highly likely Canadian Insurance companies will be following suite. See also the Financial Services Commission of Ontario’s Fact Sheet on Home Insurance Tips, Retrieved: April 2, 2015.
23. This capacity is increasingly available in many cameras including Vue Zone, Belkin’s netcams, and others.

****