

Current Trends in IoT Technologies, Challenges and Applications

M. Pradeep¹, M.Vasanthakumar²
Assistant Professor¹, UG Scholar²

Department of ECE, Sasurie Academy of Engineering, Coimbatore, India

Abstract:

We are entering in a new era of computing technology i.e. Internet of Things (IoT). IOT is a sort of “universal global neural network” in the cloud which connects various things. The IoT is a intelligently connected devices and systems which comprised of smart machines interacting and communicating with other machines, environments, objects and infrastructures and the Radio Frequency Identification (RFID) and sensor network technologies will rise to meet this new challenge. As a result, a enormous amount of data are being generated, stored, and that data is being processed into useful actions that can “command and control” the things to make our lives much easier and safer—and to reduce our impact on the environment. As a measure of internet of things serious concerns are elevated over access of individual privacy and personal data pertaining device .This survey summaries the elements, challenges, evolution, application, security and privacy concerns of internet of things.

Keywords: Internet of Things, Privacy and Security, Sensors

I. INTRODUCTION

The Internet of Things (IoT), also called Internet of Everything or Network of Everything, is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the production, operator and or other connected devices based on the infrastructure of International Telecommunication Union's Global Standards Initiative. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

With the quick development of communication technology and internet technology, survives are progressively led into unreal space of virtual world. People can shop, chat, work, keeps plants and pets in the virtual would provide by the network. Though, human being lives in an actual world, human action cannot be entirely applied through the services in the imaginary space. It is the restraint of imaginary space that restricts the development of internet to give better services. To eliminate these constraints, a

technology is essential to integrate real world on a same platform and imaginary space. Based on a maximum number of low-cost wireless communication sensors, the sensor networks forward new demands to the internet technology. It will carry changes to the upcoming society; change our business model and way of life.

The internet of things permit things and people to be connected anyplace, anytime, with anyone ,anything perfectly using any network/path and any service. They are material objects connected to material objects in the internet. For illustration, through laser scanners, RFID, infrared sensors, global writing system and further information sensing devices are connected to several object for data exchange and communication services. At last, to reach the smart devices to be tracked, monitored and to handle the network functions and located, to make the physical infrastructure consolidation internet of things is the most needed one.



Fig.1 Internet of things Example

II EMPOWERING TECHNOLOGIES IN IoT

A. Communication and Sensing Technology

i. Radio Frequency Identification

It is a technology which electronically records the presence of an object using radio signals. Radio frequency identification system is collected of one or more radio frequency identification reader and radio frequency identification tags. Each RFTD (radio frequency identification) has its sole identification number. Radio frequency identification readers, query to radio frequency identification tag by triggering it with suitable signals. Radio frequency identification tag is response sends its tag unique identification number. There is passive radio frequency identification which harvests the power from incoming signals from radio frequency identification readers. Active radio frequency identification has own battery power and can instantiate the communication. Merits of radio frequency identification is that it is of very low cost, small in size and can be operated without line of sight, but at the similar time, the biggest demerits is that it has limited battery power.

ii. Wireless Sensor Networks

It contains of large number of spatially distributed intelligent sensor nodes, having the capabilities of processing, analyzing, collecting the raw data and can issue the processed information. Wireless sensor networks can be verified better as compared to radio

frequency identification while tracking the moving object, as it traces location along with its surrounding atmosphere parameter like temperature and humidity etc. Most of the wireless sensor networks can be applied through various IEEE 802.15.4 standard wireless technologies; Wireless local area network, Wireless personal area network, Wireless metropolitan area network, Satellite network and Wireless wide area network. Wireless sensor networks works on two major types of protocol such as IP-based protocols (PhyNet, NanoStack and IPv6) and non-IP based (Sensor-Net and Zigbee). The best part of wireless sensor networks is that it has high radio coverage range so no special device like radio frequency identification is required.

Here are some of the standards groups involved in IoT:

3GPP: Handles cellular standards from 2G to LTE and beyond, including development of LTE Cat-M and to handle the network functions and to located, to make the physical infrastructure and IT infrastructure consolidation internet of things is the most needed one and narrowband IoT standards.

IEEE: Home for Wi-Fi, the 802.15.4 standard for low-rate personal-area networks and dozens of other and to handle the network functions and to located, to make the physical infrastructure and IT infrastructure consolidation internet of things is the most needed one standards relating to the function and communication of wireless devices;

A. Communication and Sensing Technology

i. Radio Frequency Identification

It is a technology which electronically records the presence of an object using radio signals. Radio frequency identification system is collected of one or more radio frequency identification reader and radio frequency identification

low cost, small in size and can be operated without line of sight, but at the similar time, the biggest demerits is that it has limited battery power.

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

amended for specific machine-to-machine support.

Bluetooth Special Interest Group:

Responsible for standards development and certification for Bluetooth technology, used by an estimated 8.2 billion devices today. Bluetooth SIG announced earlier this year its newest release, Bluetooth 5, will have increased range and speed as well as broadcast messaging capabilities. Bluetooth 5 is expected to be released late this year or in early 2017.

Thread: A format built on open standards including IEEE's 802.15.4 standard and Ipv6/6LoWPAN protocols for mesh networking of up to 300 wireless devices in the home, focused on security and low power. Google, a backer of Thread, open-sourced Thread earlier this year so the protocol could be used by developers for free, though certification from Thread is still required for products.

NFC Forum: Certification body for near field communications, commonly used for contactless payments and increasingly used for smart access to connected vehicles.

ZigBee Alliance: Another IEEE 802.15.4-based wireless solution, this certification group includes more than 400 companies and says more than 200 ZigBee products have achieved its certification so far this year. ZigBee Alliance recently added a fifth accredited test lab group (UL), and its president and CEO, Tobin Richardson, said "we're on pace in 2016 to have our biggest year yet as an industry alliance" due to surging demand in IoT.

Z-Wave Alliance: Responsible for interoperability/certification testing for this ISM-band mesh technology. Often used in home automation products, Z-Wave's application layer specification was also made public earlier this year to encourage its use.

OneM2M: A global consortium for IoT standards that includes collaboration among the All Seen Alliance, Open Connectivity Foundation and Open Mobile Alliance for basic connectivity and interworking among their IoT systems.

LoRa Alliance: Certification and specification group for the low-power wide-area network technology LoRaWAN that relies on spread-spectrum technology

in unlicensed bands for bidirectional communications for IoT.

SigFox: A LP-WAN network provider that relies on ultra-narrowband, sub-1 GHz bands similar to LoRa's approach, but licenses its technology for radio module development and is the primary core technology operator for networks across 22 countries.

iii. Two Dimensional Barcode

It is a technology which uses optical resources for representing data that can be read by a special bar code reader machine to achieve the data. It shelters several inches to few feet distance but bar code and reader should be in line of site. The tear and wear is more in two dimension code as compares to radio frequency identification but at the similar time it is low-cost technology compare to radio frequency identification.

B. Middleware

Middleware is a software layer which offer abstraction by interfacing underlying technologies of internet of things and its application level. It permits the application running through multiple platforms that hides the heterogeneity, location of sensing devices and delivers interoperability between the heterogeneous devices.

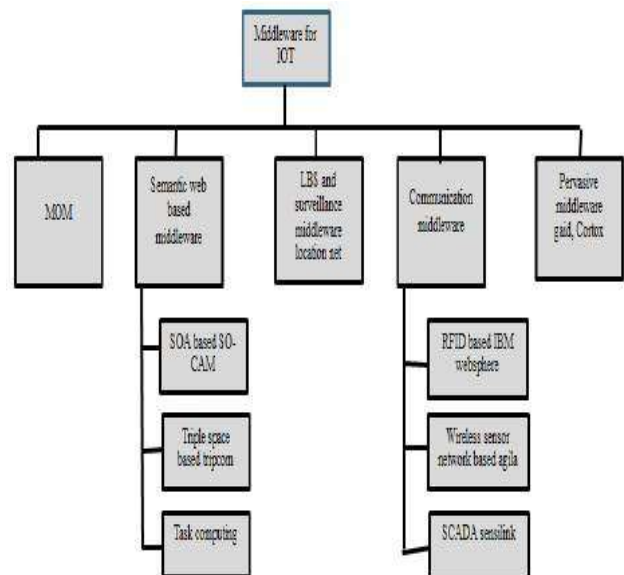


Fig.2 Classification of Middleware

C. Protocols

Internet of things essentials various protocol for diverse operations. Like it involves a protocol for collecting the information from sensors, communication protocol to send the data to server infrastructure, protocols for device to people communication, protocol for D2D and M2M communication.

- ▮ Message queue telemetry transport MQTT [5,6]
- ▮ Constrained application protocols-COAP [5,11]
- ▮ Extensible messaging and presence protocol-XMPP [5,6]
- ▮ Data distribution service-DDS [5,6]
- ▮ Zigbee [7,8]
- ▮ Zwave[7,8]
- ▮ 6LowPAN[9,10]

CHALLENGES	
Challenges in sensing and communication technology	Standardization Interoperability Noisy data Massive data issue Scalability
Challenges in communication protocol	Power consumption Special gateway REQUIRED Security challenge in 6LowPAN Routing
Challenges in middleware	Standardization Abstraction Scalability Heterogeneity and zero infrastructure
Challenges in QOS	Resource constraints Dynamic infrastructure Scalability Heterogeneous Traffic

Fig.3 Open Challenges in Internet of Things

III CHALLENGES IN IoT

Major challenges while IOT involves:

A. Scalability

One more main challenge is the scalability of the internet of things, as daily new devices and objects are getting connected with the network. It includes issues like naming and addressing conventions, service management and information management etc.

B. Device Heterogeneity

As internet of things is almost connecting several smart devices, connecting heterogeneous devices is main challenge while building internet of things. Such device runs on dissimilar platforms, they usages different protocols to communicate. So it is essential to do unification of such devices.

C. Energy Optimized Solution

This is main constraint of internet of things. As numerous devices are connected via networks, energy spent for data communication between different devices.

D. Ubiquitous Data Exchange Through Wireless Technology

In internet of things, wireless technologies are used to connect smart devices. Include issues like network delays, congestion and availability etc.

E. Self-Organization Capabilities

In internet of things, it is necessary that the smart objects should sense the environment and autonomously respond to real world situations, without abundant human intervention.

F. Localization and Tracking Capabilities

The smart objects required be tracking and identified of them is necessary.

G. Semantic Interoperability and Data Management

Internet of things interchange data between different smart objects, it is essential that there should be a standardized format for data exchange in order to make sure the interoperability among applications.

IV EVOLUTION

Earlier the investigation of the internet of things in depth, it is valuable to look at the evolution of the internet. In the late 1960s, communication among two computers was made possible through a computer network. In the initial 1980s, the TCP and IP stack was introduced. Then, commercial use of the internet started in the late 1980s. Late, the world wide web because presented in 1991 which made the internet extra popular and stimulate the rapid growth.

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

Then, mobile devices connected to the internet and formed the mobile internet. With the appearance of social networking, users taking place to become connected organized over the internet. The next step in the internet of things is where objects around us will be capable to connect to each other and communicate via the internet. What we want, and what we need and act accordingly without explicit instructions.

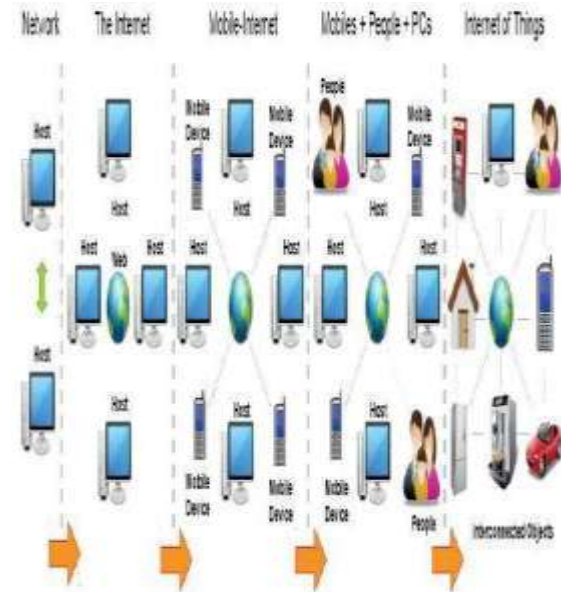


Fig.2 Evolution of the Internet of Things

V. APPLICATIONS OF IoT

A. Internet of Things in Smart Home

At the present, smart homes are becoming additional cost effective and intellectualized with continued progress and cost decrease in communication technology, electronics and information technology, which connects the internet with sensor and normal devices for connecting physical and virtual objects through the data capture and communication capabilities development. Reading of remote meters can be achieved through these smart home systems. That indicates, the data linked with home power, gas, water and telecommunication can be sent automatically to their corresponding value company to improve the efficiency of the work. In adding, by virtue of smart home system, home ventilation, windows, lighting, doors, air conditioning etc., can be controlled remotely. Every electronics devices such as washing machine, refrigerator and oven etc., can be manipulated by remote program or platforms.

Entertainment equipment like television and radio can be connected to common channels which are in remote. In adding healthcare and home security are also significant aspects of smart homes. For example, health aid devices can help an elder single to send alarm or request to a professional medical center or a family member. In smart home design the home and various electronic appliances have been prepared with sensors and actuator.

B. Internet of Things in Health Care

The internet of things technologies such as radio frequency identification, wireless sensor networks etc., could deliver various benefits in the healthcare domain.

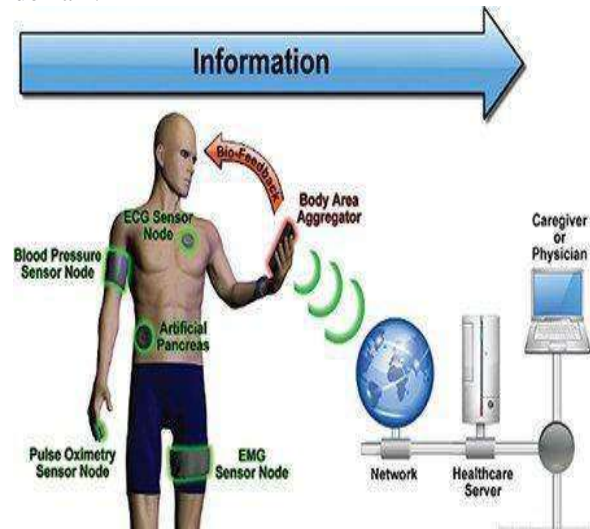


Fig.3 Internet of Things in Healthcare

For illustration, a person health status could be inferred from the radio frequency identification tags on clothes or from discovering wearable medical devices. And the application can be categorized in to tracking of patients and hospital staff, authentication and identification of people, remote healthcare and automatic data sensing and collection In the remote health system, each day blood glucose level, human blood oxygen concentration are collected automatically by the sensor nodes, transmitted wirelessly to the base station and displayed compared to time on the screen. Moreover by connecting the base station with a networked home person computer, doctors may check the data to see if the results are normal or not. The data can be transferred to doctor mobile devices through the gsm short message from the home base station. This system gives benefits to hospital or remote healthcare at homes.

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

C. Intelligent Community Security System

The ICSS (intelligent community security system) embraces various subsystems, such as surrounding security subsystem (SSS), vehicle management subsystem (VMS), property management subsystem (PMS), central information processing system (CIPS) and fire and theft prevention subsystem (FIPS) etc.

i. Vehicle Management Subsystem

The VMS in intelligent community security system accepts intellectual property rights, radio frequency identification and sensor network technologies. Image registration can be taken by video camera and radio frequency identification which is given to the vehicle. The vehicle license data will be messaged to the central information processing system, when enter the communities. The visitor is assigned with the short-term parking places. The record information and the data of the driver radio frequency identification card must be coherent when the car leaves. This assurance the security of the car and prevents theft occurrences. In the garages video system will check damage or stealing to assure the vehicle security.

ii. Surrounding Security Subsystem

As per the essentials of security surroundings to create an intelligent and enclosed community, sensing terminals such as Unicode infrared laser, power network and sensor optical fibre rare installed. WSN collect the valuable feedback and information to the central information processing system at regular time intervals. The surrounding security subsystem surrounds electronic access controls electronic fences and rotatable watching cameras. It can be applied to escape illegal intrusive behaviour or enter in to communities.

VI. SECURITY CONCERNS IN INTERNET OF THINGS

Internet of things nearly is a network of actual world system with actual time interaction. The development of the original stage of internet of things is machine to machine (M2M) having single characteristics, subscription and deployment contexts. Unattended operation without human intervention is possible from extended periods of time by the WAN (wireless area network) or wireless local area network. Though given that improvements in social effectiveness if makes an array of new

problems concerning information security and that breach of privacy

A. Front end sensors and equipment

Front end sensors and equipment collect data through the built in sensors. They then transfer the information using machine to machine or module devices, thus attaining networking services of multiple services sensors. This method includes the security of machines with node connectivity and business implementation . Perception nodes or machine are mostly dispersed in the nonappearance of monitoring scenario. As invader can easily access these devices which implies damage or illegal actions on these nodes can be done. Potential threats are examined and are categorized to illegal access to information, threats to the denial of service attack and internet.

B. Networks

Networks acting a significant role providing a more comprehensive effect, interconnection capability and thriftiness of connection, as healthy as authentic quality of service in internet of things. Later a maximum number of machines transfer data to large number of nodes, network congestion and group exist in internet of things may be produced in denial of service attacks.

C. Backend of its System

Back end it system form the middleware, gateway, which has gathering and high security requirements, pseudo real time to increase business intelligence or examining sensor data in real time. The security of internet of things system has seven main standard; data integrity, privacy protection, communication layer security, data confidentiality, access control, user authentication and comfort of use at any time.

VII. PRIVACY CONCERNS IN INTERNET OF THINGS

The internet security glossary defines privacy as the right of entity acting in its own to define the degree to which it will interact with its environment, as well as the degree to which the object is willing to share data about itself with others. Typically in internet of things, the environment is detected by connected devices. Then they broadcasts the collected information's and detailed events to the server which carrier out of the applications logic. This is achieved by fixed communication or mobile which take responsibility. Privacy should be safe in

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

the device, in processing which helps to disclose the sensitive information and at storage during communication. The privacy of data protection and users has been recognized as one of the significant challenges which need to be addressed in the internet of things.

VIII. CONCLUSION

We studied that Internet of things (IOT) is a wide network having various application area for making city smart. Each application of IOT can be implemented using different standards and different protocols. In this paper, we state the current trends of art on the internet of things, including the elements, evolution, applications, challenges, security and privacy. It is held that in the new future the reaching of the vision of anyplace, anytime connectivity for anyone, we will currently have connectivity for anything should determine on cooperative efforts and cross discipline in related field.

REFERENCES

- [1] C. Perera., A. Zaslavsky., P. Christen., and D. Georgakopoulos., "Context Aware Computing of the Internet of Things: A Survey," IEEE Communications Survey & Tutorials, 2013, pp.1-41.
- [2] L. Atzori., A. Iera., and G.Morabito., " The Internet of Things: Survey," Computer Networks Journal 54(2010), pp.2787-2805.
- [3] S. Schneider (2013, October 9) "Understanding the Protocol Behind the Internet of Things [Online]," Available:<http://electronicdesign.com/embedded/understanding-protocols-behindinternet-things>.
- [4] M. Chaqfeh., and N. Mohamed., "Challenges in Middleware Solution for the Internet of Things," IEEE 2012 International Conference on Collaboration Technologies and System (CTS), pp. 21-26.
- [5] "IOT/M2M Protocols [online]," Available: <http://IOT.eclipse.org/protocols.html>.
- [6] S. Schneider.,(2013,October 9) "Understanding the Protocol behind the Internet of Things [online]," Available: <http://electronicdesign.com/embedded/understanding-protocols-behindinternet-things>.
- [7] M. Shiuan., and Y.Chee. (no date) "Zigbee Wireless Sensor Networks and Their Applications [online]," Available: <http://people.cs.nctu.edu.tw/~yctseng/papers.pub/book-zigbee.pdf>.
- [8] J. Tan., G. Simon., and M. Koo., "A Survey of Technologies Internet of Things," 2014 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 269 – 274.
- [9] Z. Shelby., and C.Bormaen., "6LoWPAN: The Wireless Embedded Internet Companion," Welly Publication 2009.
- [10] N. Kushalnagar., G. Montenegro., and C. Schumacher., " IPv6 over Low- Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goal [Online]" Available:http://datatracker.ietf.org/doc/rfc4919/?include_text=1.
- [11] Z. Shelby., K. Hartke., and C. Bormann., "The Constrained Application Protocol [Online]," Available: <https://tools.ietf.org/html/rfc7252>.
- [12] A. Vilamovska., E. Hattziandreu., R. Schindler., C. Van Oranje., H. De Vries., and J. Krapelse., "RFID Application in Healthcare-Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery." RAND Europe, February 2009.