WWJMRD 2018; 4(7): 11-15
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
Impact Factor MJIF: 4.25
E-ISSN: 2454-6615

G. Umarani
Guest Lecturer, Dept of computer Science K.N.Govt Arts College for Women (A), Thanjavur, TamilNadu,India

K.Sharmila
Guest Lecturer, Dept of computer Science K.N.Govt Arts College for Women (A), Thanjavur, TamilNadu, India

Correspondence:
G. Umarani
Guest Lecturer, Dept of computer Science K.N.Govt Arts College for Women (A), Thanjavur, TamilNadu,India

IoT: The Next Evolution of Internet

G. Umarani, K.Sharmila

Abstract
Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction. The basic idea of IoT is to allow 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. This article reports the various technologies of IoT, Applications and discuss the challenges shall be faced by the research community.

Keywords: Internet of Things- IoT- Defy-RFID- Actuator-NFC

I Introduction

The Internet of Things is a network of physical objects or "things" embedded with electronics, software, sensors and network connectivity which enables to interact with each object to collect and exchange data.

Internet of Things (IoT) is not a result of single novel technology; instead several complementary and technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities includes: Communication and Cooperation, Addressability, Identification, Sensing, Actuation, Embedded information processing, Localization and user interfaces. The IoT can be viewed as a gigantic network (shown in Fig 1) consisting of network of devices and computers connected through series of intermediate technologies; where numerous technologies like RFIDs (Radio Frequency Identification), Wireless connections may act as enablers of this connectivity.

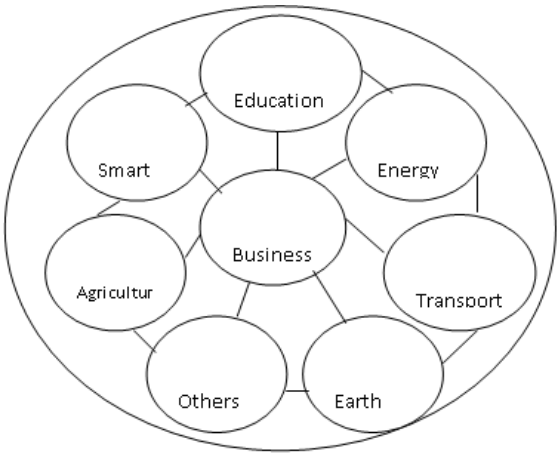


Fig.1: Internet of Things

Radio Frequency Identification (RFIDs) uses electromagnetic fields tom automatically identifies and track tags attached to object. The tag contains electronically stored

information. RFIDs were seen as a prerequisite for the IoT at that point. If all objects and people in daily life where equipped with identifiers. Computer could manage and inventory them. Besides using RFIDs, the tagging of things may be achieved through such technologies and Near Field Communication (NFC), Bar codes, QR Codes, Bluetooth and Digital watermarking.

Tagging Thing
Real-time item traceability and addressability by RFIDs

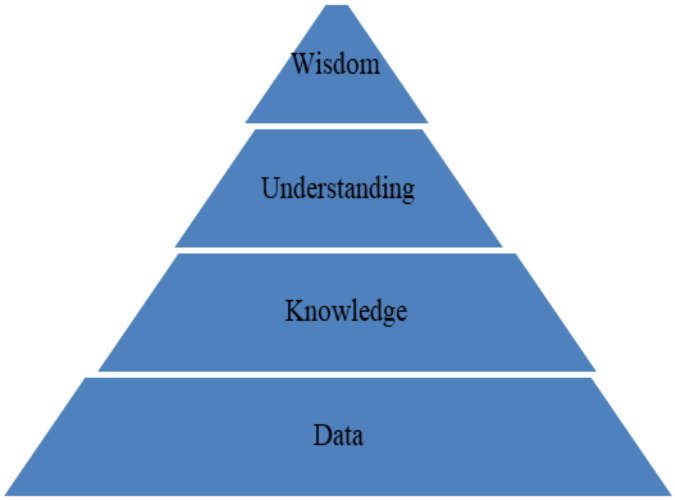
Feeling Things
Sensors act as a primary device to collect data from the environment.

Shrinking Things
Miniaturization and Nanotechnology has provoked the ability of small things to interact and connect within the "Things" or smart devices.

Thinking Things
Embedded intelligent in devices through sensors has formed the network connection to the internet. It can make the things realizing the intelligent control.

Tracking Behavior
Product with sensor is able to track by companies through their movements and monitor interaction with them. Sensor-driven decision analytics can support longer range of complex human planning and decision making such as Oil and Gas industry, retailing, healthcare.
The network connected with added security analytics and management capabilities. This will allow IoT to become even more powerful in what it can help people achieve. The Data transformation process can be illustrated using the well-known "Knowledge Hierarchy" (shown in Fig 2). We adopt the meaning of layers to context of IOT.

More important



Less important

Fig. 2: Knowledge Hierarchy

IoT is increasing the connectedness of people and things on a scale that once is unimaginable. Connected devices outnumber the world's population by 1.5 to 1. The pace of IoT market adoption is accelerating because of increasing interconnectivity of machines and personal smart devices.

II Technologies of IoT
IoT primarily exploits standard protocols and networking technologies. However the major enabling technologies and protocols of IoT are RFIDs, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A and Wi-Fi Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common system.

A. Protocols
1) NFC and RFID.
RFID (Radio Frequency Identification and Near Filed Communication (NFC) provide simple, low-energy and versatile options for identity and access tokens, connection bootstrapping and payments. RFID technology employs 2-way radio transmitter-receivers to identity and track tags associated with objects.
NFC consists of communication protocol for electronic devices, typically a mobile device and a standard device.

2) Low-energy Bluetooth.
This technology supports the low-power, long-use need of IoT function while exploiting a standard technology with native support across systems.

3) Low-energy Wireless.
This technology replaces the most power hungry aspect of an IoT system.
Though sensors and other elements can power down over long periods, communication links (i.e. wireless) must remain in listening mode. Low-energy wireless not only reduces consumption, but also extends the life of the device through less use.

4) Radio Protocols.
ZigBee, Z-wave and Thread are radio protocols for creating low-rate private area networks. These technologies are low-power, but offer high throughput unlike many similar options. This increases the power of small local devices networks without the typical costs.

5) LTE-A.
LTE-A or LTE Advanced, delivers an important upgrade to LTE technology by increasing not only its coverage, but also reducing its latency and raising its throughput. It gives IoT a tremendous power through expanding its range, with its most significant applications being vehicle, UAV, and similar communication.

6) Wi-Fi Direct.
Wi-Fi Direct eliminates the need for an access point. It allows P2P (Peer-to-Peer) connections with the speed of Wi-Fi, but with lower latency.
Wi-Fi Direct eliminates an element of a network that often bogs it down, and it does not compromise an speed or throughput.

B. Hardware
The Hardware utilized in IoT Systems includes device for a remote dashboard, devices for control servers, a routing and bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication and detection to support specific goals and actions.

1) IoT-Sensors.

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, Radio Frequency (RF) modules, and sensing modules. RF modules manage communications through their signal processing, Wi-Fi, ZigBee, Bluetooth, radio transceiver, duplexer and BAW.

The sensing module manages sensing through assorted active and passive measurement devices. Here is a list of some of the measurement devices and used in IoT(shown in Table 1).

Table 1: Hardware Devices

S.No.	DEVICES	
1.	Accelerometers	Temperature Sensors
2.	Magnetometers	Proximity Sensors
3.	Gyroscopes	Image Sensors
4.	Acoustic Sensors	Light Sensors
5.	Pressure Sensors	Gas RFID Sensors
6.	Humidity Sensors	Micro flow Sensors

2) Wearable Electronics.

Wearable electronic devices are small devices worn on the head, neck, arms, and feet. Current smart wearable devices includes

Head – Helmet, glasses
Neck – Jewelry, Collars
Arm – Watches, Wristbands, rings
Feet – Socks,

3) Standard devices.

The desktop, tablet and cell phone remain integral parts of IoT as the command center and remotes.

The desktop provides the user with the highest level of control over the system and its settings. The tablets provide access to the key features of the system in a way resembling the desktop, and also acts as a remote. The cell phone allows some essential settings modification and also provides remote functionality.

Other key connected devices include standard network devices like routers and switches.

C. Software

1) Protocols.

A list of IoT protocols including 6LOWPAN, MQTT, COAP and others.

2) Platforms.

A list of IoT platforms like Tfing worx, ioBridge, sense and others.

3) Embedded Operating System.

TinyOS is an open source operating system designed for low–power wireless devices. TinyOS is written in nesC is a programming language for Deeply Networked systems.

Contiki is designed for micro controllers with small amount of memory.

Mantis OS (MOS) is an open source multithread OS written in C for wireless sensor networking platform.

Nano-RK supports fixed-priority preemptive multitasking-LiteOS is an open source interactive UNIX-like OS. FreeRTOS ported to several microcontroller.

D. Middleware

Many researchers have proposed the use semantic middlewahre to interoperate the different communication formats. Semantic middleware seeks to create a common framework that enables data sharing and exchange across distributed devices, applications and locations.

E. Architecture

The IoT requires huge Scalability in the network space to handle the surge of devices.Billions of devices being added to the internet space. Ipv6 will play a major role in handling network layer scalability.

Fog computing is a viable alternative to prevent such large burst of data flow through internet. The edge devices computation power can be used to analyse and process data, thus providing easy real time.

III Applications

While IoT applications are limitless, several key vertical markets are emerging as areas where it is likely to scale first, offering major benefits for people and businesses. Various application are: Education, Smart Home, Connected Cars, Industrial internet, Smart cities, Agriculture, Health care.

A. Education

IoT learning Environment support educators can influence how we communicate and operate. There are two aspect, firstly how students are taught and finally how educational institutions can being in IoT to improve campuses.

B. Smart Home

Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicated smart home will become as common as smart phones.

C. Connected Car

The automotive digital Technology has focused on optimizing vehicles internal functions. A connected car is a vehicle which is able to optimize its own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity. Major brands like Tesla, Apple, and Google are working on bringing the next revolution in automobiles.

D. Industrial Internet

Industrial Internet is also termed as industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and Big Data analysis to create brilliant machines. The driving philosophy behind IIoT is that, Smart machines are more accurate and consistent than humans in communicating through data.

Applications for tracking goods, real-time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain

efficiency.

E. Smart Cities

Smart cities are another powerful application of IoT generating curiosity among world's population. Smart surveillance, automated transportation, Smart energy management System, water distribution monitoring for smart cities. IoT will solve major problems faced by the people.

Smart energy management System, water distribution monitoring for smart cities. IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies.

F. Agriculture

IoT contributes significantly towards innovative farming methods. The integration of wireless sensors with agriculture mobile apps and cloud platform helps in collecting vital information pertaining to the environment conditions: temperature, rainfall, humidity, wind speed, pest infestation can be used to improve and automate farming techniques, take informed decisions and improved quality and quantity and minimize risks and waste.

G. Health Care

IoT devices can be used to enable remote health monitoring and emergency notification systems. The health monitoring devices can range from Blood pressure and Heart rate monitors to advanced devices capable of monitoring specialized implants such as parameters, Fibit electronics wrist bands, or advanced hearing aids. ensuring the proper treatment is being administred and assisting people regain lost mobility via therapy.

IV Challenges

For the IoT industry to thrive there are three categories of challenges to overcome and this is true for any trend in technology not only IoT; technology, business and society.

A. Technology

There are many technological challenges, including, security, connectivity, compatibility and longevity standards and intelligent analysis and action.

1) Security.

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world internet has possibility to carry ever deeds, especially since a considerable number of them suffer from security holes.

2) Connectivity.

Connecting so many devices will be one of the biggest challenges of future of IoT, and it will defy the very structure of current communication models and the underlying technologies. Centralized system will turn into bottleneck. The future of IoT will very much have to depend on decentralizing IoT networks.

3) Compatibility and Longevity.

IoT is growing in many different directions, with many different directions, with many different technologies competing to become the standard. This will cause difficulties and require the deployment of extra hardware and software when connecting devices. Some of these technologies will eventually become obsolete in the next few years. IoT tend to remain in service for much longer and should be able to function even if their manufacturer goes out of service.

4) Standards

Technology standards which include network protocol, communication protocol, and data-aggreation standards, are the sum of all activities of handling, processing and storing the data collected from the sensors.

B. Business

A sound and solid business model must satisfy all the requirements for all kinds of e-commerce vertical markets, horizontal markets and business markets. But this category is always a victim of regulatory and legal scrutiny.

C. Society

Understanding IoT from the customers and regulators prospective is not an easy task for the following reason: Customers demands and requirement change constantly, new uses of devices, consumer confidence, lack of understanding and education.

D. Privacy

The IoT creates unique challenges to privacy, many that go beyond the data privacy issues. The collection of IoT information exposes legal and regulatory challenges facing data protection and privacy law.

V Conclusion

In this article we have reported several technologies and applications of IoT and outlined the challenges. Multi-disciplinary nature of the IoT domain requires synergetic efforts from other fields such as service computing, data mining and social science to enchance the processing and utilization of data in IoT domain. One question that remains is whether or not the IoT is to be an eduring technology, whether it will fail to materialize, or whether it is a stepping stone to another paradigm. Only time will ultimately answer that question. However, by bringing existing technologies together in a novel way. The IoT has the potential to reshape our world.

References

1. Andrew Whitmore, Anurag Agarwal, Li Daxu, "The Internet of Things-A Survey of Topics and trends", Springer, 2015.
2. Luigi AtZori, Antonio lora, Giacomo,Morabito, "The Internet of Things: A Survey", Elsevier,2010.
3. Payam Barnaghi, Wei wang, Cory Hensor and Kerry Taylor, "Semantics for the Internet of Things: A early progress and back to the future".
4. Rowley, Jennifer (2010) "The wisdom hierarchy: representations of DIKW hierarchy" Journal of information Science.
5. Meyer.S, et.al) (2011) "Towards modeling real-world aware business processes", In proceeding of web of Things.
6. Akyildiz. I.F. & Jornet,J.M. (2010). "The Internet of Nano Things." IEEE Wireless Communications.
7. Ma.H (2011), "The Internet of Things: Objectives and Scientific Challenges", Journal of Computer Science and Technology.

8. Aggarwal, C. C.,Ashish, N., & Sheth, A. (2013). The Internet of Things: A Survey from the data-centric perspective. In C. C. Aggarwal(Ed.), Managing and mining sensor data (pp.383-428). US: Springer.
9. [Bandyopadhyay, D., & Sen, J. (2011). Internet of Things:applications and challenges in technology and standardization. Wireless Personal communications, 58(1), 49-69.
10. [Castellani, A. P., Gheda, M., Bui, N.,Rossi, M., & Zorzi, M. (2011). Web Services for the Internet of Things through CoAp and EXI. Proceedings of the IEEE International Conference on Communication Workshops (ICC).