International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

Evolution of the Internet of Things

Dipak R. Nemade
Assistant Professor, Department of Computer Science, J. T. Mahajan College of Engineering, Faizpur, India

***Abstract*: The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. We see the IoT as billions of smart, connected "things" (a sort of "universal global neural network" in the cloud) that will encompass every aspect of our lives, and its foundation is the intelligence that embedded processing provides. The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. As a result, huge volumes of data are being generated, and that data is being processed into useful actions that can "command and control" things to make our lives much easier and safer—and to reduce our impact on the environment. The creativity of this new era is boundless, with amazing potential to improve our lives. The following thesis is an extensive reference to the possibilities, utility, applications and the evolution of the Internet of Things. We're entering a new era of computing technology that many are calling the Internet of Things (IoT). Machine to machine, machine to infrastructure, machine to environment, the Internet of Everything, the Internet of Intelligent Things, intelligent systems—call it what you want, but it's happening, and its potential is huge.**

***Keywords*: IoT, Network, Internet, Evolution, Communication, objects, embedded, machine**

1. Introduction

The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure .IoT is made up of a loose collection of disparate, purpose-built networks. Today's cars, for example, have multiple networks to control engine function, safety features, communications systems, and so on. Commercial and residential buildings also have various control systems for heating, venting, and air conditioning (HVAC); telephone service; security; and lighting. As IoT evolves, these networks, and many others, will be connected with added security, analytics, and management capabilities.

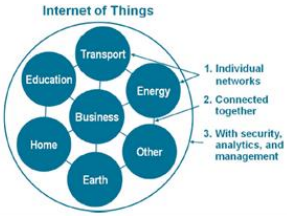

Fig. 1. Internet of Things

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure,[creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. The Internet and the World Wide Web (or web)—terms that are often used interchangeably. The Internet is the physical layer or network made up of switches, routers, and other equipment. Its primary function is to transport information from one point to another quickly, reliably, and securely. The web, on the other hand, is an application layer that operates on top of the Internet. Its primary role is to provide an interface that makes the information flowing across the Internet usable.

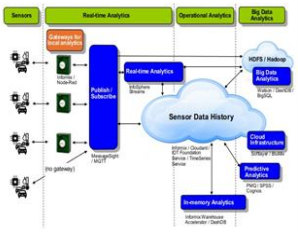

Fig. 2. Architecture of IoT

The integration of wireless sensors with agricultural mobile apps and cloud platforms helps in collecting vital information pertaining to the environmental conditions – temperature, rainfall, humidity, wind speed, pest infestation, soil humus

content or nutrients, besides others linked with a farmland, can be used to improve and automate farming techniques, take informed decisions to improve quality and quantity, and minimize risks and wastes. The app-based field or crop monitoring also lowers the hassles of managing crops at multiple locations. For example, farmers can now detect which areas have been fertilized (or mistakenly missed), if the land is too dry and predict future yields. Information technologies are getting smarter by the day. In the near future, users may able to send a message to a friend by typing something on their sleeve, or their purse may remind them not to leave their keys in the house. In fact, keys may soon be a thing of the past, if biometric recognition sensors in smart homes replace them. Current definitions of "smart" are very broad. Any conventional material or thing that can react to external stimuli may be called a "smart thing". In other words, not only are our devices, such as PDAs and mobile phones, getting "smarter", but so too are the clothes we wear, the containers we use and the houses we live in. This section examines some of the most interesting developments in this area.

2. IOT smart sensors

A. What is a sensor?

A sensor is a device that detects and responds to some type of input from the physical environment. A sensor is an electronic device, which detects senses or measures physical stimuli – for instance, motion, heat or pressure – and responds in a specific way. It converts signals from stimuli into an analogue or digital form, so that the raw data about detected parameters are readable by machines and human The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena.

The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing. Sensors are used to measure physical quantities such as temperature, light, pressure, sound, and humidity. They send signals to the processor. For example: A security alarm system may have an infrared sensor which sends a signal when the beam is broken. Why might one require the use of sensors? One of the first questions people ask over a mobile phone is: "Where are you?" They do this to get information about the location and situation a person is in. This information is needed for more effective decision-making. Much is gained from applying a similar logic to computers: even more so, when computers become ubiquitous. It is extremely important to gather knowledge about the environment, situation or context surrounding an object (computing element) or user, so that decisions taken by the computing element are as relevant to the user's task or status as possible. However, computers communicate in other ways than people. In a ubiquitous network society, where human-computer interactions should be as simple and effortless as possible, some of the most important sources of information for a computer are its sensors.

B. Wireless sensor networks

The intelligence of a single sensor increases exponentially when used in a network. When a sensor forms part of a sensor network, it is known as a sensor "node". While it is now easy to deploy single sensors, ensuring connectivity between multiple nodes is a more challenging task. In simple terms, sensor nodes can be connected to each other in two ways: wire line and wireless. Wire line communication protocols provide high levels of security and reliability, and are appropriate "whenever time-critical and mission-critical data and closed-loop control are required". However, laying cables and relocating them at a later date can be costly and time-consuming. Taking these factors into consideration, together with advances in miniaturization and low-cost alternatives, wireless links are being increasingly explored for the development of sensor networks. Wireless sensor networks are generally less costly, less visible and more flexible.

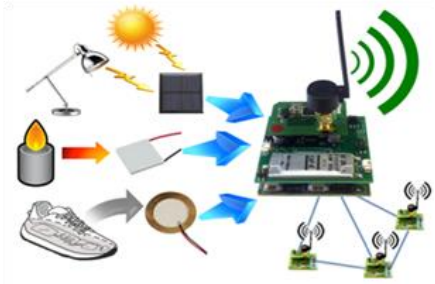

Fig. 3. Wireless Sensor Network

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on. Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location.

C. Webbing the sensors

While software, machine-to-machine learning and other technologies work together to analyze data from physical objects – the sensors are key to gathering the information. If software is the brains of the IoT, sensors are the nervous system collecting continuous streams of data to be processed. Industrial systems rely on sensors for reliable, consistent and accurate data in all aspects of automation. One could even argue the IoT is nothing without sensors to measure parameters such as strain, temperature, position, and pressure. The Internet of Things (IoT), also sometimes referred to as the Internet of Everything (IoE), consists of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. These devices, often called

"connected" or "smart" devices, can sometimes talk to other related devices, a process called machine-to-machine (M2M) communication, and act on the information they get from one another. Humans can interact with the gadgets to set them up, give them instructions or access the data, but the devices do most of the work on their own without human intervention. Their existence has been made possible by all the tiny mobile components that are available these days, as well as the always-online nature of our home and business networks. Connected devices also generate massive amounts of Internet traffic, including loads of data that can be used to make the devices useful, but can also be mined for other purposes. All this new data, and the Internet-accessible nature of the devices, raises both privacy and security concerns. An IoT system consists of sensors/devices which "talk" to the cloud through some kind of connectivity. Once the data gets to the cloud, software processes it and then might decide to perform an action, such as sending an alert or automatically adjusting the sensors/devices without the need for the user. But if the user input is needed or if the user simply wants to check in on the system, a user interface allows them to do so. Any adjustments or actions that the user makes are then sent in the opposite direction through the system: from the user interface, to the cloud, and back to the sensors/devices to make some kind of change.

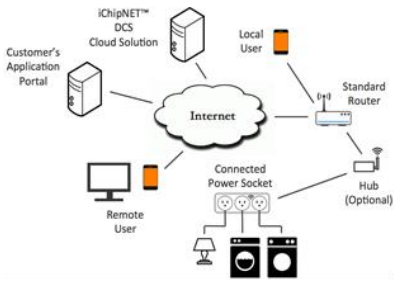

Fig. 4. Block Diagram of IoT

Internet of Things (IoT) is a rapidly developing technology today and most likely everyday thing in the future. Numerous devices, computing machines and build-in sensors connected in a single dynamic network continuously receive and exchange information from the outer environment. Huge data clusters are collected and put to use in handmade applications that scrupulously manage and control given objectives. In this way, an interactive technical infrastructure is created, which can oversee and infiltrate any person's vital processes. Though separately every device and technological solution in the IoT can be known for many years, each architecture is unique and provides new challenges for the network owner. This research aims to investigate IoT general structure and management aspects with the knowledge of which the authors will try to answer a trivial question whether it is possible to comprehensively control.

3. IoT security

IoT security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things (IoT). The Internet of Things involves the increasing prevalence of objects and entities – known, in this context as things -- provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices. The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. IoT products are often sold with old and unpatched embedded operating systems and software. Furthermore, purchasers often fail to change the default passwords on smart devices or if they do change them, fail to select sufficiently strong passwords. To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be monitored to identify potential anomalous traffic, and action should be taken if there is a problem.

A. IoT network security

IoT network security is Protecting and securing the network connecting IoT devices to back-end systems on the internet. IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity. Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems.

B. IoT authentication

Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics. Unlike most enterprise networks where the authentication processes involve a human being entering a credential, many IoT authentication scenarios (such as embedded sensors) are machine-to-machine based without any human intervention.

C. IoT encryption

Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers. The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes, since poor key management will reduce overall security.

D. IoT PKI

Providing complete X.509 digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation. The hardware specs for some IoT devices may limit or prevent their ability to utilize PKI. Digital certificates can be securely loaded onto IoT devices at the time of manufacture and then activated/enabled by third-party PKI software suites; the certificates could also be installed post-manufacture.

E. IoT security analytics

Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies. These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging. IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls.

F. IoT API security

Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs.

G. Firewalling and IPS

The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. Why a host-based firewall or IPS is required if network-based appliances are in place? Deeply embedded devices have unique protocols, distinct from enterprise IT protocols. For instance, the smart energy grid has its own set of protocols governing how devices talk to each other. That is why industry-specific protocol filtering and deep packet inspection capabilities are needed to identify malicious payloads hiding in non-IT protocols. The device needn't concern itself with filtering higher-level, common Internet traffic—the network appliances should take care of that—but it does need to filter the specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.

H. Secure booting

When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. In much the same way that a person signs a check or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded. The foundation of trust has been established, but the device still needs protection from various run-time threats and malicious intentions.

4. IoT applications

A. Smart home

Definition of connected home is different for different people. In simple words a smart home is the one in which the devices have the capability to communicate with each other as well as to their intangible environment. A smart home gives owner the capability to customize and control home environment for increased security and efficient energy management. There are hundreds of IoT technologies available for monitoring and building smart homes.

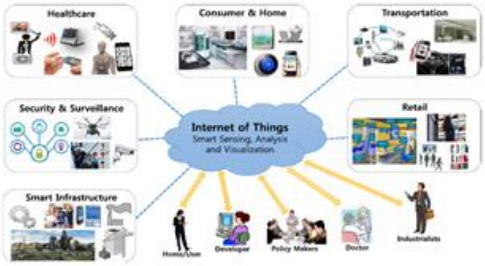

Fig. 5. IoT Applications

B. Variables

Variables are one of the hottest trends in IoT currently. Apple, Samsung, Jawbone and plenty of others all are surviving in a cut throat competition. Wearable IoT tech is a very large domain and consists of an array of devices. These devices broadly cover the fitness, health and entertainment requirements. The prerequisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized. Here are some top examples of wearable IoT devices that fulfill these requirements.

C. Retail

The potential of IoT in the retail sector is enormous. Imagine the scenario when your home appliances will be able to notify you about shortage of supplies or even order them all on their own. This proximity-based advertising model of smart retailing has started to become a reality. We already have internet of things application examples as part of smart supply chains. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery all existing but with a limited reach.

D. Smart Cities

Smart surveillance, safer and automated transportation, smarter energy management systems and environmental

monitoring all are examples of internet of things applications for smart cities. Smart cities are the real substantial solutions for the troubles people usually face due to population outburst, pollution, poor infrastructure and shortage of energy supplies. Here are some examples of IoT devices at work.

E. Healthcare

Healthcare is one sector which is supposed to be highly boosted with advent of internet of things applications. IoT examples in this domain are many. TI is shaping technology to improve the quality and accessibility of digital products that are revolutionizing the health and fitness industries.

F. Agriculture

Reduce time to market in your precision agriculture design with TI devices and reference designs.

5. Conclusion

Internet of Things is a new revolution of the Internet & it is a key research topic for researcher in embedded, computer science & information technology area due to its very diverse area of application and heterogeneous mixture of various communications and embedded technology in its architecture.

References

[1] D. D. Guinard and V. M. Trifa, “Comparing IoT and WoT,” Building the Web of Things, 2016, p. 8.
[2] Ovidiu Vermesan SINTEF, Norway, Peter FriessEU, Belgium, “Internet of Things–From Research and Innovation to Market Deployment”, river publishers’ series in communications, 2014
[3] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., “Internet of Things Strategic Research Agenda”, Chapter 2 in Internet of Things - Global Technological and Societal Trends, River Publishers, 2011.
[4] Martin Serrano, Insight Centre for Data Analytics, Ireland ,Omar Elloumi, Alcatel Lucent, France, Paul Murdock, Landis Gyr, Switzerland, “Alliance for Internet of Things Innovation, Semantic Interoperability” , Release 2.0, AIOTI WG03 – loT Standardisation,2015.
[5] IoT:https://dzone.com/articles/the-internet-of-things-gateways-and-next-generation.
[6] http://www.reloade.com/blog/2013/12/6characteristics-within-internet-things-iot.php
[7] Martín Serrano, Payam Barnaghi, Francois Carrez Philippe Cousin, Ovidiu Vermesan, Peter Friess, “Internet of Things Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps”, European research cluster on the internet of things, IERC, 2015.
[8] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World”, The Internet Society (ISOC), 2015.
[9] H. van der Veer, A.Wiles, “Achiveing Technical Interoperability —the ETSI Approach”, ETSI White Paper No.3, 3rd edition, April 2008.
[10] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[11] http://tblocks.com/internet-of-things
[12] https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology.
[13] Ovidiu Vermesan SINTEF, Peter Friess EU, Belgium, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, river publishers’ series in communications, 2013.
[14] L. Tan and N. Wang, “Future internet: The Internet of Things,” in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, 2010, pp. 376–380.
[15] Christophe B, “Semantic profiles to model the “Web of things”. In: Proceedings of the 7th international conference on semantics, knowledge and grid (SKG), pp. 51–58, 2011.