ELK ASIA PACIFIC JOURNAL OF COMPUTER SCIENCE AND INFORMATION SYSTEM

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

ELK
Asia Pacific Journals
www.elkjournals.com

TOWARDS A SMARTER WORLD: INTERNET OF THINGS

Harshvardhan Pandey	Rahul Palaria
B Tech Undergraduate, Amrapali Group of Institutes, Haldwani	Asst. Professor, Dept. of Comp. Sc. & Engg., Amrapali Group of Institutes, Haldwani
harshvardhanpandeycse@gmail.com	rahulpalaria@yahoo.com

Abstract

The Internet of Things (IoT) has grown immensely as a promising technology. IoT represents a continuum consisting of all types of devices and products which are connected to the Internet through network archictectures. The sensor technology provides the backbone to this system which can use various types of connections such as RFID, Wi-Fi, Bluetooth, ZigBee, 3G, LTE, etc. All such component devices share data of all sorts with each other making the world smarter. In this paper, we attempt to review the many popular applications of IoT. Also we discuss some of the possible related technologies and the hurdles we may face in implementing them.

Keywords - Internet, RFID, IEEE-SA, PKI, homomorphic encryption

I. INTRODUCTION

The Internet is, undoubtedly one of the most prosperous inventions of all times. With the advent of The Internet of Things (IoT) or the Internet of Objects, mankind attempts to change the environment in which we live. The Internet has had a very profound influence on our lives ranging from education, communication, business, to science, government healthcare, and humanity [1].

IoT takes the significance of the Internet to the next level. Objects, referring to all IoT enabled devices, are able to identify themselves. They learn about their environment by the virtue of the fact that they can communicate information about themselves. Such objects can access information that has been aggregated[2], or they can augment the services provided by other similar devices.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

The concept of IoT was first born when a heuristic coke machine was made Internet enabled in 1982. It was able to report the drinks it contained and that whether the drinks were cold or not. In 1999, Bill Joy hinted about Device to Device communication and Kevin Ashton proposed the term ”Internet of Things” to describe a system of interconnected devices. IoT was defined to allow independent exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us with the

help of leading technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSNs)[3]. **(Ref Figure- 1)**

Computing services are becoming pervasive and distributed leading to decentralized resources. We need a strong interconnection among them by a dynamic network of networks . The IoT technology makes possible the testing and deployment of such products. The medium for communication in such a heterogeneous environment is based on interoperable protocols.

2. STANDARDS

It is estimated that by the year 2020 around 100 billion objects will be connected by the Internet. We will definitely need a common standard for these objects to extend their routine behavior. The success of IoT depends on standardization to provide interoperability, compatibility, reliability, and effective operations on a global scale. As the Internet evolves, it may be necessary to review such constraints and investigate ways to ensure sufficient capacity for expansion[4].

IEEE Standards Association (IEEE-SA) develops a number of standards that are related to environment need for an IoT. The main focus of the IEEE standardization activities are on the Physical and MAC layers. The IEEE provides an early foundation for the IoT with the IEEE802.15.4 standard for short range low power radios,

typically operating in the industrial, scientific and medical band in addition to using ZigBee technology. The IEEE-SA has over 900 active standards and more than 500 standards under development. The base project related to IoT is IEEE P2413 which is currently considering the architecture of IoT.

It produces globally applicable standards forinformation and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies, discusses a similar concept under the label of “machine to machine **(Ref Figure- 2)**

(M2M) communication” . These standards are considered as one of the basic standards of IoT.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

The Internet Engineering Task Force (IETF) is concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF provides its own description of IoT including a major recognizable enhancement to support IPv6, with the 6LoWPAN. The 6TiSCH Working Group is being formed at the IETF to address the networking piece of that unifying standard[5]. Based on open standards, 6TiSCH will provide a complete suite of protocols for distributed and centralized routing operation over the IEEE802.15.4e TSCH MAC.

III. APPLICATIONS

A. Home

Wi-Fi technologies in home automation have been used primarily due to the networked nature of deployed electronics. Wi-Fi has started becoming part of the home IP network due to the increasing rate of adoption of mobile computing devices like smart phones, tablets, etc. All types of WiFi enabled devices can be used as gateways for IoT applications. Many companies are considering to develop platforms that integrate the building automation with entertainment, healthcare monitoring, energy monitoring and wireless sensor monitoring in the home and building environments [6]. The Internet together with energy management systems also offers an opportunity to access the accomodations' energy information and control systems which can be from a laptop or a smartphone placed anywhere in the world.

B. Energy

A smart grid that integrates the information and communications technologies (ICTs) to the electricity network will enable a real time, two way communication between suppliers and consumers, creating more dynamic interaction on energy flow, which will help deliver electricity more efficiently and sustainability. This will primarily include sensing and monitoring technologies for power flows; digital communications infrastructure to transmit data across the grid; smart meters with in home display to inform energy usage; coordination, control and automation systems to aggregate and process various data, and to create a highly interactive, responsive electricity [7].

C. Health Care

Health sensors can be used to collect comprehensive physiological information. Internet gateways and the cloud cn then be used to analyze and store the information and send the analyzed data wirelessly to caregivers for further analysis and review. It will replace the process of having a health professional coming at regular intervals to check the patient's

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

vphysiological signs. In this way, it simultaneously improves the quality of care through constant attention and lowers the cost of care by overcoming conventional methods.

D. Urban Agglomerates

Major cities like New York, Tokyo, London, Singapore, Amsterdam, and Dubai are built upon smart projects. IoT can help in improving infrastructure, enhancing public transportation, reducing traffic congestion, and keeping citizens safe, healthy and more engaged in the community by the integration of all management and monitoring systems.

E. Transportation

A road condition monitoring and alert application is one of the most important IoT applications. The main idea of the concept of smart transportation and mobility is to apply the principles of crowd sourcing and participatory sensing. The process begins with the user identifying the desired route and marking some points as pothole in the smart phone's application. The transportation analytic represents the analysis of demand prediction and anomaly detection.[8] The routing of vehicles and speed control in addition to traffic management comes under transportation control which is related to vehicles connectivity (V2X communication), and overall governed by multi-technology dissemination. IoT also finds application in electric vehicles for monitoring and management of the Li ion batteries.

IV. CHALLENGES

The Internet of Things, its applications and scenarios outlined above are very interesting, but there are some challenges to its implementation and associated costs. Some of them include: **(Ref Figure- 3)**

- *Self-Organizing*: Smart things should not be managed as computers that require their users to configure and adapt them to particular situations.
- *Data Volumes*: Some application scenarios of the Internet Of Things will involve infrequent communication, and gathering information form sensor networks, or from logistics and large scale networks, will collect huge volumes of data on central network nodes or servers.
- *Data Interpretation:* To support the users of smart things, there is a need to interpret the local context determined by sensors as accurately as possible.
- *Interoperability*: Each type of smart objects in Internet of Things have different information, processing and communication capabilities.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

- *Automatic Discovery*: In dynamic environments, suitable services for things must be automatically identified[9], which requires appropriate semantic means of describing their functionality.
- *Software complexity:* A more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

V. RELATED FUTURE TECHNOLOGIES

Many new technologies are related to IoT which will provide the integration of wired as well as wireless control, communication and IT technologies. Such a coherent system shall be responsible for connecting several subsystems and things which operate under a unified platform and are controlled and managed smartly.

A. Cloud Computing

The two worlds of Cloud and IoT have seen a rapid and independent evolution. These worlds are very different from each other, but their characteristics are often complementary. In general, in which IoT can benefit from the virtually unlimited capabilities and resources of cloud to compensate its technological constraints[10]. For example: storage, processing, and communication. Cloud can offer an effective solution for IoT service management and composition as well as for implementing applications and services that exploit the things or the data produced by them .On the other hand, cloud can benefit from IoT by extending its scope to deal with real world things in a more distributed and dynamic manner, and for delivering new services in a large number of real life scenarios. In many cases, Cloud can provide the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement the latter. This will impact future application development, where information gathering, processing, and transmission will generate new challenges, especially in a multi cloud environment or in fog cloud. Cloud facilitates IoT applications to enable data collection and data processing, in addition to rapid setup and integration of new things, while maintaining low costs for deployment and for complex data processing. It is the most convenient and cost effective solution to deal with data produced by IoT and, in this respect, it generates new opportunities for data aggregation, integration, and sharing with third parties. Once into Cloud, data can be treated as homogeneous through well-defined APIs and can be protected by applying top level security so that it can be directly accessed and visualized from any place.

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

B. Big Data

The expectations in the next years show that around 50 billion devices will generate large volumes of data from many applications and services in a variety of areas such as smart grids, smart homes, healthcare, automotive, transport, logistics and environmental monitoring. The related technologies and solutions that enable integration of real world data and services into the current information networking technologies are often described under the terms of the Internet of Things[11].

The volume of data on the Internet and the Web is still growing, and everyday around 2.5 quintillion bytes of data is created and it is estimated that 90% of the data today was generated in the past two years. Collected data from sensors related to different events and occurrences can be analyzed and turned into real information to give us better understanding about our physical world and to create more value added products and services. Such sensory data are: data of predicted and balanced power consumption in smart grids, analyzed data of pollution, weather and congestion , data recorded to provide better traffic control and management, and monitoring and processing health signals data[12]. In addition, the information available from social media such as Facebook, Twitter, WhatsApp and user submitted physical world observations and measurements also provide a huge amount of data (Big Data). Integration of data from various physical, cyber, and social resources with the IoT enables developing applications and services that can incorporate situation and context awareness into the decision making mechanisms and can create smarter applications and enhanced services. With large volumes of distributed and heterogeneous IoT data, issues related to interoperability, automation, and data analytics will require common description and data representation frameworks.

C. Security and Privacy

Due to the fact that IoT applications are able to access the administrative domains and involve multiple ownership, there is a need for a security framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. The security framework needs to be able to deal with humans and machines as users, for it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. The development of trust frameworks that address this requirement will require advances in areas such as lightweight public key infrastructures (PKI) as a basis for trust management. Lightweight key management systems is used to enable trust encryption materials using minimum communications and

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

processing resources, as is consistent with the resource constrained nature of many IoT devices.

IoT based systems require quality of information for metadata which can be used to provide an assessment of their liability. A novel method is required for IoT based systems for assessing trust in people, devices and data. One of the most common methods used are trust negotiation that allows two parties to automatically negotiate on the basis of a chain of trust policies and a certain minimum level of trust required to grant access to a service or to a piece of information. Internet of Things uses methods for access control to prevent untrusted data breaches by controlling the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted.

Since the IoT has become a key element of the future Internet, the need to provide adequate security for its infrastructure has become ever more important. Large scale applications and services based on the IoT are increasingly becoming vulnerable to disruption from attack or information theft. Many advanced security methods are required in several areas to make the IoT secure from attacks, thefts and many other security problems such as DoS/DDOS attacks, compromised nodes, and malicious code hacking attacks.

The IoT requires a variety of access control and associated accounting schemes to support the various authorization and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed [13]. The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches for example Machine Learning, are required to lead a self-managed IoT. Cryptographic techniques are also very important in IoT based systems for enabling a means of protection for data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.

D. Distributed Computing

Distributed Computing uses groups of networked computers for the same computational goal. It has several common issues with concurrent and parallel computing, as all these three fall in the scientific computing field. A large amount of distributed computing technologies coupled with hardware virtualization, service oriented architecture, and autonomic and utility computing have led to cloud computing. Internet of Things with distributed

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

computing represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be remotely controlled and can act as physical access points to Internet services.

E. Fog Computing

Fog computing is related to the edge computing in the cloud. In contrast to the cloud, fog platforms have been described as dense computational architectures at the network's edge. Characteristics of such platforms reportedly include low latency, location awareness and use of wireless access. While edge computing or edge analytics may exclusively refer to performing analytics at devices that are on, or close to, the network's edge, a fog computing architecture would perform analytics on anything from the network center to the edge. IoT may more likely be supported by fog computing in which computing, storage, control and networking power may exist anywhere along the architecture, either in data centers, the cloud, edge devices such as gateways or routers, edge equipment itself such as a machine, or in sensors.

VI. CONCLUSION

As is evident from the discussions in our paper, the future of the computing world lies in the Internet of Things. Its applications to various fields and the numerous services which will be available through it certainly prove to be beneficiary to us. Active research is being carried out to implement it in the most optimum manner. We foresee a near future having a Mega Internet at our service all the time making us more connected than ever before.

REFERENCES

[1] Guicheng Shen and Bingwu Liu, "The visions, technologies, applications and security issues of Internet of Things," in E-Business and E -Government (ICEE)

[2] H.D. Ma, "Internet of things: Objectives and scientific challenge,"Journal of Computer Science and Technology

[3] Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 3

[4] S. Misra et al., Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering

[5] Adam D. Thierer. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation.

[6] Farheen Fatima, at el., Internet of things: A Survey on Architecture, Applications, Security, Enabling

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

Technologies, Advantages & Disadvantages. *International Journal of Advanced Research in Computer and Communication Engineering*

[7] Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*

[8] Sapandeep Kaur, Ikvinderpal Singh. A Survey Report on Internet of Things Applications. *International Journal of Computer Science Trends and Technology*

[9] S. Misra et al., Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering

[10] Suwimon Vongsingthong and Sucha Smanchat. A Review of Data Management in Internet of Things. *KKU Res. J.*

[11] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*

[12] Grandinetti, Lucio. Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives: Future Outlooks and Interdisciplinary Perspectives. IGI Global

[13] Patrick Guillemin, et al., Internet of Things Position Paper on Standardization for IoT technologies. European research cluster on the internet of things

LIST OF FIGURES

Figure- 1 : IoT Architecture

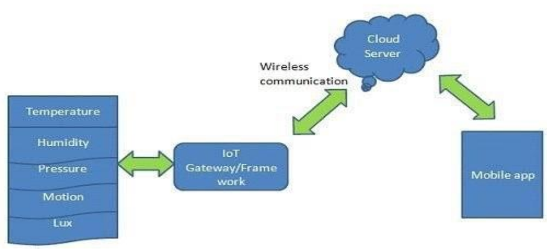

Figure- 2: Growth of devices (*Source:www.hackernoon.com)*

ISSN 2349-9392 (Online); DOI: 10.16962/EAPJMRM/issn. 2349-9392/2015; Volume 4 Issue 2 (2018)

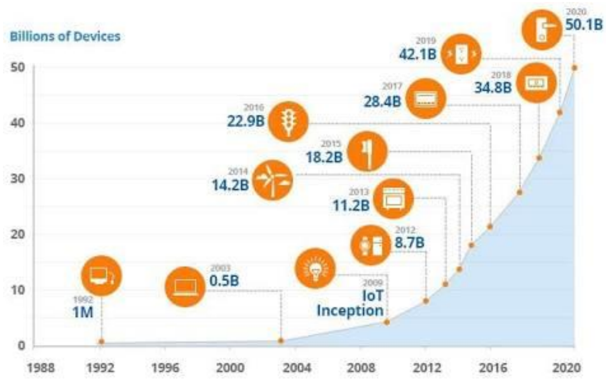

Figure- 3: Applications of IoT (*Source: www.quora.com)*