A Literature survey on Internet of Things (IOT), with its Evolution

Sudhir Shukla[1], Narendra K. Chaurasia[2], Satyendra K. Vishwakarma[3]

1, 2(Assistant Professor, ECE Department, BIT GIDA Gorakhpur)

3(3rd Year, ECE Department, BIT GIDA Gorakhpur)

ABSTRACT

Internet of Things (IoT) is a rapidly growing technology with a wide range of applications in various fields. IOT is a sort of "universal global neural network" in the cloud which connects various things. The IoT is an 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. In other words "IoT" connects heterogeneous devices that provide sensing, control, actuation, and monitoring activities for smarter environments. Smart IoT devices or objects are characterized with a unique identifier to transfer data over the network without human intervention. Every organization such as companies and civil institutions needs up-to-date information about people. In this regard, most establishments either use websites, emails or notice boards. However, in most of countries internet access is available to people on systems and their mobile devices, so that the transferring of the information can be much easier and less costly through the internet IoT is expected to further extend the boundaries of the autonomous world with advanced connectivity of physical entities, systems, and services.

Keywords: CNS, Constrained Application Protocol, Internet of Things (IoT), IOT Cloud.

I.INTRODUCTION

During the last decade, Internet of Things (IoT) has attracted intensive attention due to a wide range of applications in industrial, biomedical observation, agriculture, smart cities, environmental monitoring and other fields (Fig. 1) [1]. IoT is the internetworking of physical devices used in our daily lives that use standard communications architectures to provide new services to end users [13]. From a conceptual standpoint, the elements of IoT summarized into a simple equation below:

IOT = HUMAN + Physical Objects (sensors, controllers, devices, storage) + Internet

It is envisioned that by 2020 the future Internet will include tens of billions of smart objects/devices [13]. IoT technology provides better services to end users via real-time data processing, communications and visualization. IoT can be extended to almost everything from refrigerator to washing machine, wristwatches to smart phones, home security to alarm system, etc [14]. For example, smart refrigerators can tell us the end of the validity of food using bar-codes or which items to buy during our shopping in the market. On the other hand, imagine that we can control our house from anywhere. By using smart phones or tablets with just simple touch we can set a desired temperature or turn lights on or off before getting home. These are examples of just a few applications out of thousands being currently developed every day in the field of IoT. The massive growth in the number of devices connected to the internet (up to 100 billion devices), poses a huge range of challenges. In the future IoT will not be islands of isolated systems, but will be an integration of many islands of connected systems, applications, services and underlying devices. At the moment, each of these devices and services work on their own architectures, data format, and own existing protocol stacks. They are all still at early stages of development. Hence, the communication between these objects is insecure, suffers from interoperability and integration issues. Furthermore, the sources of energy required to power these devices are very precious due to the fact that most of them are powered by battery or by means harvested energy. Therefore, there is a need for comprehensive review of existing unconstrained and constrained devices protocols with the view of developing unified, dynamic, standardized, energy efficient and intelligent protocol stacks with recourse to node identity (both capacity and capability). So far, most of these new challenges and concerns have started to attract the attention of academic researchers and companies. The organization of the paper is as follows: Section 2 presents briefly IoT applications challenges and summarizes the related works. We conclude the paper in section 3.

II.IOT OVERVIEW

Basically Internet of Things (IOT) allows people and things to be connected anytime, anyplace with anyone and anything, ideally using any path/network any of any services. They are material objects which are connected with that of material objects available in the market. Likewise for the purpose of data exchange laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object.

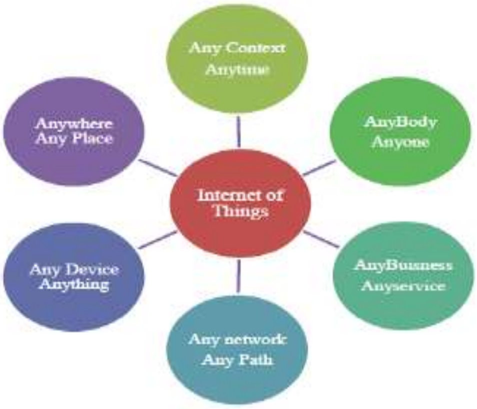

Fig1. Simple connected modules with Internet via IOT [13]

2.1. Evolution:

Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in Fig. 2, in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and formed the mobile Internet. With the emergence of social networking, users started to become connected together over the Internet. The next step in the IoTs is where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via the Internet. IoT promises to create a world where all the objects (also called smart objects) around us are connected to the Internet and communicate with each other with minimum human intervention. The ultimate goal is to create “a better world for human beings”, where objects around us know what we like, what we want, and what we need and act accordingly without explicit instructions [13].

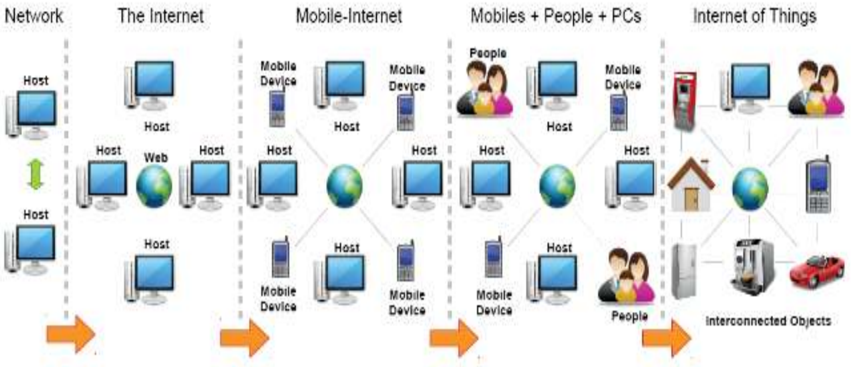

Fig2. Evolution of Internet of Things [13]

2.1.1. Architecture:

IoTs can be divided into three important layers Viz; Perception, Network and Application. As shown in Fig., perception layer (also called as recognition layer) gathers data/information and identifies the physical world. Network layer is the middle one (also called as wireless sensor networks), which accountable for the initial processing of data, broadcasting of data, assortment and polymerization. The topmost application layer offers these overhauls for all industries. Among these layers, the middle one network layer is also a "Central Nervous System" that takes care of global services in the IoTs, since it acts the part of aggregating with upward application layer and makes the link. Downward of perceptual layer.

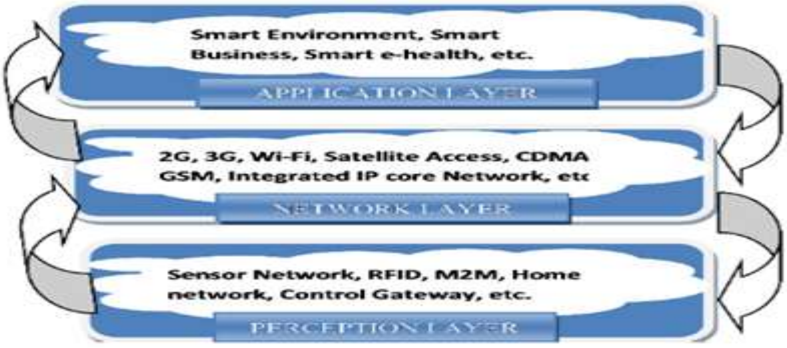
Smart Environment, Smart Business, Smart e-health, etc.
APPLICATION LAYER
2G, 3G, Wi-Fi, Satellite Access, CDMA GSM, Integrated IP core Network, etc
NETWORK LAYER
Sensor Network, RFID, M2M, Home network, Control Gateway, etc.
PERCEPTION LAYER

Fig3. Architectures of IOT (Internet of Things)

2.1.2. Applications:

It is obvious that that there are many more platforms present in the market, but due to tech-specific and time limits few of them are chosen to provide a precise ideas about how they work, what are their strengths, what are their weaknesses, in which domain they are appropriate. While, studying these IoT platforms, each of these was tested in reality to disseminate their strengths and weaknesses. Further, based on applicability and suitability preferences in several domains the IoT cloud platforms have been revisited. 10 different domains are selected based on which most of IoT cloud platforms are currently evolving into the IT market. Management wise few technological sectors are envisioned where these platforms do best fit into such as: Device, System, Heterogeneity, Data, Deployment, and Monitoring. Similarly, Analytics, Research and Visualization fields are chosen where rest of the platforms may be accommodated. While describing the selected cloud platforms following parameters such as real time data capture capability, data visualization, cloud model type, data analytics, device configuration, API protocols, and usage cost are chosen as the key selective features. This section also provides Table 1 that compares IoT clouds according to their suitability and appropriateness in the prescribed division of application domains [1].

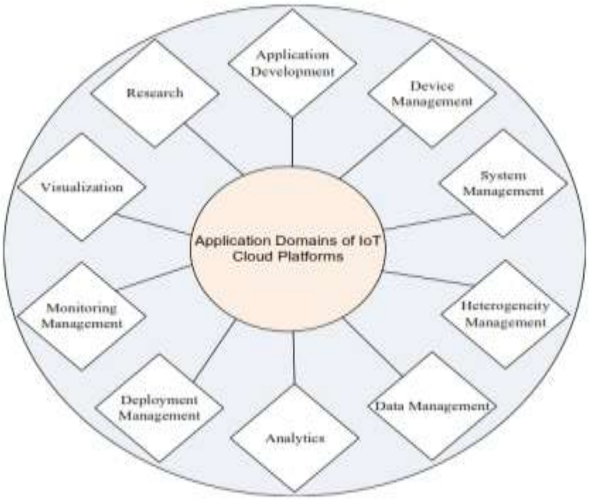

Fig4. Application domains of cloud platform

The main applications or the scenarios attracting the most interest were: smart home, smart city, transportation and health care [14].In this paper, the focus will be briefly on the IOTs applications in medical (health care) [9], smart home[11], intelligent community security system (smart city) [9].

1. IoT in Smart Home
2. Intelligent community security system (ICSS)
3. IoTs in Medical Application
4. Smart agriculture
5. Industrial Control

III.LITERATURE SURVEY

This section prescribes the works done so far by the scientists around the globe (Intel research). Various domain specific architectures based on the broad areas, such as: RFID (Marrocco et al., 2009), service oriented architecture, wireless sensor network, supply chain management, industry, healthcare, smart city, logistics, connected living, big data, cloud computing, social computing, and security are described in this section. The selection of theses domains depends upon current scenario of IoT applicability. It is has been tried to incorporate as much directions into this article, but due to the size constraints, present limitations have been made. The key methodology behind the survey depends on few factors of importance where earlier mentioned domains are deeply investigated based on their respective sub domains. This survey is performed to know the present scenario of internet of things, so may that scope of IOT can be visualized in a proper manner. As being the latest technology it is widely used everywhere to make the connectivity advanced i.e. things will be looked in a drastic manner.

1. P.P. Ray: In this author introduce, Firstly the background and definition of IoT. Secondly, thorough discussions on fundamentals behind IoT architectures are elaborated. Next, several key domains where IoT based research works are currently going on are visited. Afterward, detailed analyses of the research challenges are mentioned. Resulting graph attains the state of-the-art research based motives on the aforementioned domains. A novel concept-‘‘Io<*>” is also proposed that is based on various theoretical nomenclature and external inputs. Different from other IoT survey papers, a main contribution of this paper is that it focuses on area specific architectures of IoT applications and highlights the challenges and possible research opportunities for future IoT researchers who would work in architectural as well as in IoT as a whole.[1]

2. Sinan T. Shukur et al: In this paper the author summarizes, the emergence of IoT, new regulatory approaches to ensure its energy, scalability, security and privacy, human-in-the-loop, big data, etc. become necessary. The IoT revolution is expanding connectivity via the internet and a wide range of applications (e.g. actuators, sensors and other embedded systems). This will have an effect on the quality, different life styles and the way we behave and interact with humans, machines and devices in the future. Therefore, new research challenges and problems will emerge due to the large scale device proliferation and their inter-communication. This paper gives an overview of the key issues related to the IOT services and technologies. A number of researcher challenges have been described, which are expected to become a major research trends in the next decade. A number of previous works have been analyzed, and most relevant WSN and IOT applications were presented. [11]

3. J. Sathish Kumar et al: In this author presented Internet of Things with architecture and design goals. They surveyed security and privacy concerns at different layers in IoTs. In addition, they identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. It was also discussed the applications of IoTs in real life. In future, research on the IoTs will remain a hot issue. Lot of knotty problems is waiting for researchers to deal with [3].

4. Pallavi Sethi et al : In this survey paper Author's presented a survey of the current technologies used in the IoT domain as of 2016. Currently, this field is in a very nascent stage. The technologies in the core infrastructure layers are showing signs of maturity. However, a lot more needs to happen in the areas of IoT applications and communication technologies. These fields will definitely mature and impact human life in inconceivable ways over the next decade [9].

5. Mayra Samaniego et al: In this paper basically discussion is on the study and development of Internet of Things (IoT) applications, web and mobile, is on the increase. Applications, working with data obtained from different areas such as transportation, smart homes, health care, public services, industry and many others. Previous studies have focused on managing the obtained data. However, managing the heterogeneous resources that get that data is an area that demands more attention. This work addresses the management of resources in the Internet of Things. This is achieved by proposing a virtual-resource edge layer, which enables access and configuration to constrained physical resources. The architecture presented focuses on the use of virtual resources as a management concept and identifies different approaches in the performance evaluation on edge computing devices. Using the IoT protocol CoAP, virtual resources are exposed in the edge network. An evaluation of a Go CoAP virtual resource is presented [11].

6. Tuhin Borgohain et al: In this paper they have surveyed all the security flaws existing in the Internet of Things that may prove to be very detrimental in the development and implementation of IoT in the different fields. So adoption of sound security measures countering the above detailed security flaw as well as implementation of various intrusion detection systems cryptographic and stenographic security measures in the information exchange process and using of efficient methods for communication will result in a more secure and robust IoT infrastructure. In conclusion, they would like to suggest that more effort on development of secured measures for the existing IoT infrastructure before going for further development of new implementation methods of IoT in daily life would prove to be a more fruitful and systematic method[13].

7. Arbia Riahi Sfar et al: The Author discuss about the technology i.e. the IoT is a new disruptive technology that can be expected to bring about an evolution in usage and in the surrounding technological ecosystem. In this paper they had shown that this major evolution will create its own security and privacy challenges. Most of these challenges result from the inherent vulnerabilities of IoT objects and the tight coupling of the physical world to the virtual world through intelligent objects. This tight interaction highlights a systemic dimension of IoT security that they proposed to use as a roadmap overview in this work. They then surveyed security related interactions and solutions: Privacy, Trust, Identification and Access Control. In addition to highlighting scientific and technological locks they have shed light on the main standardization activities and the open issues. They showed that the evolution of objects towards greater autonomy intensifies the issues of security and privacy. Finally, we concluded that the autonomy of objects to perceive and act on their environment will cause IoT security to move towards greater perceptive and actionable autonomy based on a cognitive and systemic approach [14].

8. Feifei Shi et al: The Author discuss about the current tendency which shows that data semantization in IoT has become an essential part of daily life. It provides possibilities for knowledge interaction and sharing. Ontology modeling stands out a lot in adding semantics with the standardized description formats which give great ability to merge and exchange heterogonous information. The contribution of this survey consists of a general description of data semantization in IoT, including related concepts, general architectures, key techniques, applications and challenges. Techniques involved in data semantization have been introduced, and it is true that ontology modeling has become the most pervasive technique until now. Every entity, context, user and activity can be modeled through ontologies, with strong expressivity, expansibility and reasoning ability. This paper provides a general overview of data semantization, and makes a comparison between different ontology models and automatic tools. Finally, the survey analyzes challenges and open issues including the standardization and generalization, complexity and dynamicity as well as security and privacy. This is a valuable area which will show great influence on future industry [14].

IV.CONCLUSION

The emerging idea of the Internet of Things (IoT) is rapidly finding its path throughout our modern life, aiming to improve the quality of life by connecting many smart devices, technologies, and applications**.** In this survey paper various aspects regarding internet of things has being discussed. Internet of Thing (IOT) has unified a plethora of devices and infrastructure under the same umbrella and is considered by many technologies leaders as the network of the future (NoF). We also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. With the overview background and architecture is being discussed. As the applications mentioned in this paper have its own research going through. This survey paper helps out to find the future scope in this domain.

REFERENCES

Journals Papers:

[1]. P.P. Ray, "A survey on Internet of Things architectures" Journal of King Saud University Computer and Information Sciences (2016).

[2]. J. Sathish Kumar, Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues" International Journal of Computer Applications (0975 – 8887), Volume 90 – No 11, March 2014, pp-20-26.

[3]. J. Sathish Kumar, Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014.

[4]. Arbia Riahi Sfar, Enrico Natalizio, Yacine Challalc, Zied Chtourou, "A roadmap for security challenges in the Internet of Things", Elseveir, Digital Communications and Networks (2017).

[5]. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Hindawi Publishing Corporation Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, 25 pages.

[6]. Feifei Shi, Qingjuan Li, Tao Zhu and Huansheng Ning, "A Survey of Data Semantization in Internet of Things", Sensors 2018, 18, 313; doi:10.3390/s18010313, www.mdpi.com/journal/sensors.

Conference Papers:

[7]. W. Zhao, C. Wang, and Y. Nakahira, "Medical Application On IoT," International Conference on Computer Theory and Applications (ICCTA), 2011, pp. 660-665.

[8]. K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of Things-based Smart Home System," 2nd International Conference on Intelligent Control and Information Processing, 2011, pp. 921-924.

[9]. J. Liu, and L. Yang, "Application of Internet of Things in the Community Security Management," Computational Intelligence, Communication Systems and Networks, Third International Conference on IEEE, 2011, pp. 314-318.

[10]. Laith Farhan,Sinan T. Shukur, Ali E. Alissa et al, "A Survey on the Challenges and Opportunities of the Internet of Things (IoT)", Eleventh International Conference on Sensing Technology (ICST) 2017.

[11]. Mayra Samaniego, Ralph Deters, "Management and Internet of Things", The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016), Vol-94 (2016) pp137 – 143.

Books:

[12]. C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey" IEEE Communications Surveys & Tutorials, 2013, pp. 1-41.

[13]. Tuhin Borgohain, Uday Kumar, Sugata Sanyal, "Survey of Security and Privacy Issues of Internet of Things", pp 1-6.

Website Link:

[14]. O. Vermesan, P. Friess,and A. Furness, The Internet of Things 2012, By New Horizons, 2012. [Online].Available:http://www.internet-of-things-research.eu/pdf/IERC_Cluster_ Book_2012_WEB.pdf.