International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Future Internet for Service Oriented Applications

Prathyusha Kanakam, ASN Chakravarthy

Abstract*: As with growing internet, the objects in the system need to implant with the external environment. Every object is resided in distinct place and works in an interoperable way. This process of Smart living which involves various smart devices – Smart phones, Sensors, Actuators, Radio Frequency Identification (RFID) tags, etc., evolving in this modern era is coined as Future Internet or Internet of Things (IOT). This IOT associated with distinguished services and visions through which it can be identified among various domains. A distributed intelligence needs to be employed to the application specific machine in order to serve the human perception for the sake of smart forensics. This paper explores and interprets the next generation internet, its components, standards and services along with their applications in diversified fields. Authors provide a systematic exploration of existing IoT products in the marketplace and highlights several possibly meaningful research objectives and drifts.

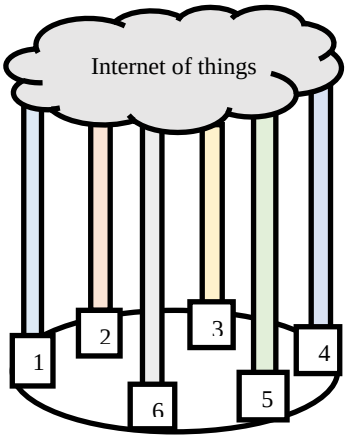
Keywords: Future Internet, Internet of things, IOT Integrals, IOT Standards, RFID.

I. INTRODUCTION

Over the past 40 years, internet has to cope up with lots of changes. In the earlier days, it is mainly utilized for the purpose of communication and now a little bit forward to those communicating virtual world entities with real world entities. There exists ubiquitous infrastructure for this type of internet that connects people, smart physical objects with technologies. It has changed several aspects of individual life and their behaviours. All the physical objects along with existing service provider make their full presence in forming the modern world. Thus, it becomes the future internet or internet of things (IOT), which is the blend of sensors, RFID, smart objects connected through sensor networks via the internet. Due to the massive usage rate of these smart devices, the raw data produced from them are collected, processed and distributed over the internet via traditional communication protocols.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Prathyusha Kanakam*, Assistant Professor, Department of Computer Science Engineering, MVGR College of Engineering, Vizianagaram, Andhra Pradesh, India.
Dr. A. S. N Chakravarthy, Associate Professor, Department of Computer Science Engineering, JNTUK- University College of Engineering Vizianagaram, Andhra Pradesh, India.

Internet of Things (IOT) [1-3] is the Future Internet that focuses on physical things that are in discrete places and their connection to one another. It is a novel paradigm responsible for wireless communications that make use of all the smart devices used in this modern smart era. It unites all objects in this world under a common platform that controls and monitors the state of objects.



6 pillars of IOT
1. Internetwork Connection
2. Fog Computing
3. Data Analytics
4. Cyber and Physical Security
5. Automotive Management
6. Application platform

Fig. 1.Pillars of IoT

A potential user views this next generation internet in various applications specific issues that come under both working and domestic fields. IOT is an extension of traditional networks for the interconnection of every object/thing to every other object/thing with all the underlying process and protocols that enable and support these inter connections. Its shafts include Internetwork Connection; Fog computing, Data Analytics, Cyber and Physical Security, Automotive Management, Application Platform as in Fig. 1. The network of networks connectivity includes gateways to route the data packets between various networks that entirely formed as the Internet. Fog computing provides various services of computing, storage and networking between both the end devices and cloud computing data centers. Data Analytics used to make predictions for future data,

analyzing historical data based on the statistical and logical approaches. Cyber and physical security though they relate to the same domain and there is slight variation in their roles of performing tasks. As Internet of things connects various physical objects in the same platform, there is a lot of scope for the cyber hacks as the objects remotely located and connected to one another. So these physical objects are extremely prone to all types of unauthorized access.

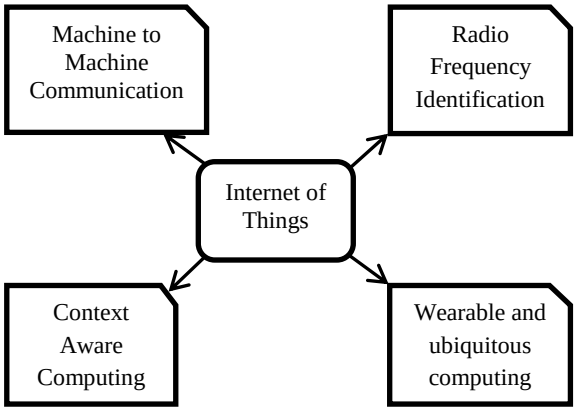


Fig. 2.Distinct Fields of IoT

IOT in the automotive industry is used to give real-time traffic alerts, it offer roadside assistance in the emergency by touching a button, and so on. Thus the automotive industry serves the link to information streams to track all type of records. Cloud-based, connected and driven by data are the three main components of IOT application platform. Thus all type of application platforms can be connected virtually and also provided with solutions from anywhere. The data will be driven from the cloud and transform into a meaningful context by connecting various devices over the internet. 0.3 Million devices are connected in the year 1990, 9.0 billion in 2013 and 1.0 trillion devices are estimated to be connected by the year 2025.

II. INTEGRALS OF FUTURE INTERNET

IOT [3] contributes to different types of knowledgeable fields like telecommunications, informatics, electronics and social science and arise interoperability among them. All these technology developments create awareness of smart things that are emerging out and how to utilise these smart objects to make the world as ubiquitous infrastructure as shown in Fig. 2. The main advantage of IOT is to create a user-defined smart application as it doesn't have a unique structure to model this modern smart world.IOT is the combination of all type of physical objects includes RFID, sensors, smart devices and smart phones which are connected by the internet from numerous places. The system or devices that make uses of internet and distributed over networks transforms the raw data collected into meaningful references.

A. Machine2Machine Communication

Machine2Machine (M2M) Communication [4] is a necessary and essential aspect in IOT where it can be applied to many applications both used for industrial and non-industrial purposes. It is one form of data communication that does not involve any human interaction. It plays a critical role in 3GPP (3rd Generation Partnership Project) under mobile networks and annotated as Machine Type Communication (MTC). This type of communication uniquely challenges as well as provides various applications when millions of computing devices are connected and communicated via internet service provider. M2M Framework consists of 5 modules in its architecture represented in Fig. 3.

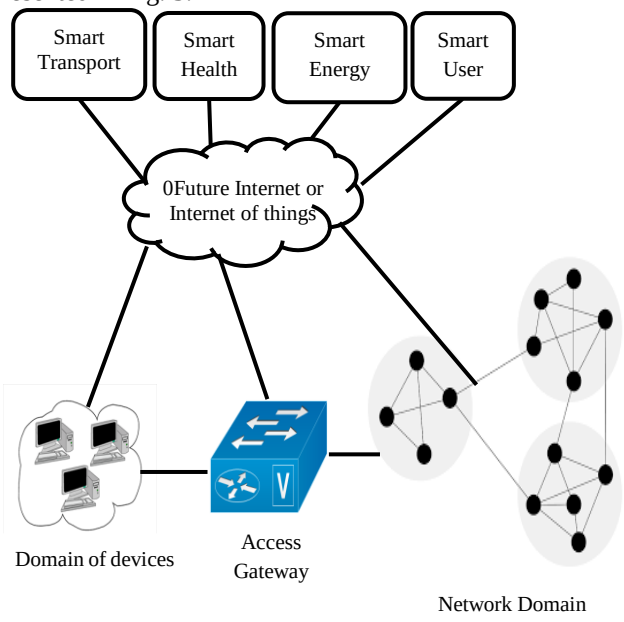


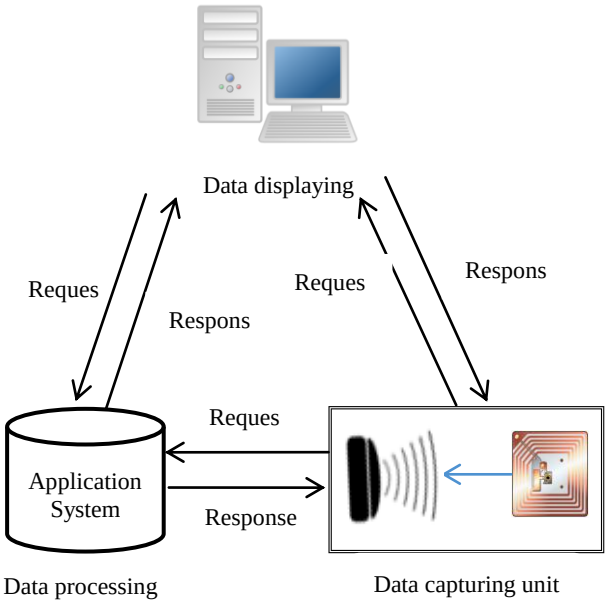
Fig. 3.Components of M2M Communication

1) Devices in M2M: Computing devices which are responsible for M2M communication are capable of transmitting data and responds to the request for providing data on its own. All the communication devices including sensors will act as terminals for M2M communication.
2) Device domain (M2M Area Network): M2M Devices are inter connected via Wireless Personal Area Network or the operator's networks. WPANs are acts as a domain to connect various computing devices which are located at different places. It is also responsible to provide connectivity between gateways and devices.
3) Gateway: It possesses hardware to ensure M2M capabilities in order to adopt inter-working culture among devices by providing connectivity between inter networks for communication. Gateways and routers are the end points of operator's networks when sensors do not connect directly to a network.
4) Network domain (M2M communication Network): It accounts the communication between M2M gateways and applications of M2M. Eg. WLAN.
5) M2M applications: Some of the business processing engines rely on the data and platforms that assist in data collection and processing techniques of discrete service oriented applications. These M2M applications exploit the operator contributed infrastructural resources.

Some of the M2M applications are Smart user, Smart health, Smart transport, and Smart energy.

B. Radio Frequency Identification (RFID)

RFID system [5] is an automated technology that acts as a pre-requisite for IOT used to identify, track and monitor an object with their digital barcode by various computing (devices) terminals of the internet at a real time. This paradigm uses radio waves to trace the objects in order to provide the metadata of the object and also controls it from remote places.



RFID system designed as data capturing unit, data displaying unit and data processing unit as shown in Fig. 4, and they mainly associated with three system peripherals.

Fig. 4.Architecture of RFID system

1) RFID metadata of the object electronically. They can be acts tags: Tags are the microchips embedded in the objects to provide as transceivers used for both transmission and receiving of data about the objects on which it is incorporated.
2) RFID scanners: Scanners are the computing devices that read the information of objects using their tags. They manage the communication with this RFID tag using radio waves. Both the RFID tags and RFID Scanners are merged in data capturing unit.
3) Application system: Either it may be a database or application to acquire metadata related to the object which has a RFID tag and after data capturing from the reader, it is stored in data processing system.

C. Context Aware Computing

The market is turning towards the future internet that involves the deployment of sensors to a greater extent. The data driven out from these sensors appears in huge amount. So the challenge exists in both the acquiring and understanding of this sensor data. Context aware computing [6] gives a novel scenario to provide the semantics of sensor data used for specific business IOT applications.

D. Ubiquitous Computing

It is the standard to operate the devices from anywhere and in any format. Pervasive computing is also having a similar meaning to that of ubiquitous computing [7]. It demands human computer interaction where a user interacts with the computer located far away and also able to access the data which is in unsupervised format connected over the internet. Thus the physical things can be accessed from everywhere and can process the data in undefined fashion.

III. FUTURE INTERNET STANDARDS

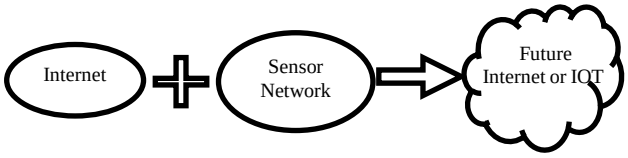


Fig. 5.Future Internet

IOT is a future vision which is in beginning stages and many organizations are interested in implementing the customer-defined products. These products involve the processes of data collection, data management, and data mining driven from various sensors along with World Wide Web to meet their needs. All the smart objects like Radio Frequency Identification tags, sensors, actuators and smart mobiles etc. have unique mechanisms for their interoperability interaction from remote places. Based on the technology usage, there are three types of standards [8] with respect to internet, physical things and semantics and it is annotated as trait of IOT represented in Fig. 5.

A. Standard with Respect to Things

It includes all the physical things like sensors and also pervasive technologies using RFID. It depends on the specific electronic code through which a product can be identified (Commonly known as Barcode) and sensed using sensors. This concept is fulfilled by sensors' capabilities. These sensors and sensor embedded systems collect the data and present the data in meaningful references.

B. Standard with Respect to Internet

All the physical things used for generating data by sensing and computing processes performed on real world objects or entities are connected to one another through the internet which follows the regularities of internet protocol for their communication from a remote place in an interoperable way. By continues monitoring, the sensor based embedded system is capable of presenting the data in an understandable format and also identifying their unique attributes.

C. Standard with Respect to Semantics

The data gathered need to be processed and organized in a meaningful manner. Semantic technologies not only represent data in understandable format but also manage the huge collection of data from the sensors. These semantic technologies also categorize the collected data into homogeneous and heterogeneous formats.

This paradigm is mainly responsible to convert the raw data into meaningful data and a marked separation of data for their interpretation.

IV. SERVICE ORIENTED APPLICATIONS OF IOT

Technologies include identification related tracking and communication problems along with their solutions which involve all the sensors, actuators in both wired and wireless networks possess various factors to form a state-of art paradigm to the future internet. These factors extend their hands in choosing the protocols used in smart communications (communication through smart devices).

Distributed intelligence applied on the machine to train about a particular application. There is a wide range of applications with IOT from household purposes to production line for retail product tracing. Each application specific service provided by IOT [9] is controlled in developing aspects of that product and along with their applications projected in Table 1.

Table- I: Product and along with their applications

Services	Respective Applications
Authentication Services with RFID	• Production and shipping • Supply chain management • Supply chain information transmission
Acquisition Services	• Energy monitoring in house and in enterprises • Monitoring and control system in an agriculture greenhouse production environment. • Measures and records critical temperature, humidity and soil signals.
Decision-making services	• IPV6 (new version of IP protocol) possess a huge number of addressable devices connected to the internet.
Wide spread services	• Ubiquitous computing of devices or terminals.

A. Authenticated Services

The services related to identity [10] of a product or an object concerns about 2 classes (operative and inoperative) for authentication. They can be applied to either individuals or enterprises with respect to the domain of applications. It is mainly correlated with the peripherals of RFID paradigm – RFID tags and RFID Scanners. They categorized as operative and inoperative aspects. Operative authentication services continuously process the information of the object and transmit that metadata to a concerned device by maintaining all the resources (constant power consumption, battery power) whereas In-operative breaks their work and need an external source to perform their services.

B. Acquisition Services

Information aggregation is the critical task performed by these type of services. They follow the procedure of receiving data through a network and transmit through an application. Gateways yield a direction towards data collection from numerous sources like sensors, network devices and share their data via a common service to the application.

C. Decision-Making Services

After the data acquisition, the appropriate actions need to be performed by making the decisions. Responds to the request for data which is collected is one of the complicated decision-making services. So it requires communication between two different devices or one device and one user. They are responsible for not only retrieving of data but also respond to the data collected from sensor networks to perform actions.

D. Wide Spread Services

They are generally ubiquitous in fashion and connect to things from anywhere in the world. Each network uniqueness and the difference in usage of protocols for discrete technologies are the key challenges. The main idea is to reuse and share the loosely coupled real world things that are widely spread over the internet as IOT lacks the centralized infrastructure and non-architectural. IOT is the extended version of current internet services, which is the huge repository of data and upcoming real world objects. With respect to a user, social and environmental contexts, the defined things of the future internet will be identified uniquely and perform interoperability among them that are located in smart spaces and connected through intelligent interfaces.

V. RESULTS AND DISCUSSIONS

When the web services like internet integrated with a network of all types of smart objects – sensors, actuators, Mobile Phones, RFID (Radio Frequency Identification) tags, that are used for sensing and processing the data represented is coined as Future Internet or Internet of things as shown in Fig. 5. It is elaborated in service oriented architecture (SOA) to design smart applications feasible to the user.

Of all these services concerned, there is wide range of IOT applications in various platforms. IOT deals with 'operating from anywhere' concept. So the smart devices are used to control the home appliances in support with various functionalities. Table 2 shows the support and capabilities of some IOT applications in various areas for the given fields like, industry, e-health and etc.

The fuzziness of IOT lies in the separation of words-Internet and things where the internet provides interconnection between computer networks based on the communication standard protocol and thing is an object not precisely identifiable. A critical field of complexity anticipating the IoT market is the optimal direction and use of the information emerging from numerous sources, including connected appliances and sensors. IOT devices improvised their version in various domains - Industrial and household to project themselves as smart devices as shown in Fig. 6.

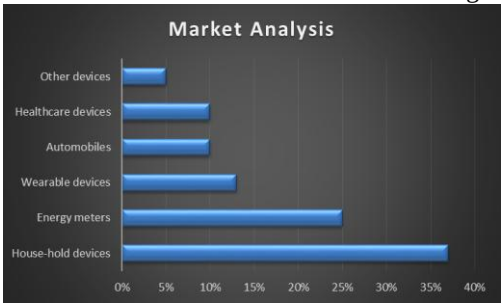


Fig. 6.Market Growth with IoT Device

The initial automobiles are switched to self-driven cars and guiding mentors for routing to the destination. All the Household appliances are enhanced with technologies and operate on the principle "from anywhere". Smart jewelry like bracelets and necklaces entered the technological market to track a person when they are in helping hands. Among most of the future Internet devices, the home appliances with smartness added are in high demand and IOT market growth turns towards these devices to make feasible to users. This complexity exhibits itself in seven essential sections of data utilization like data security, data volume, data diversity, data velocity, data analytics, data economics, data logistics.

Table-II: Summary of IOT applications and capabilities (Source from [11])

Area	Applications	Environment sensing	Location sensing and sharing	Ad hoc network	Remote controlling	Secure communication
Industry	Process Monitoring	✓			✓	✓
	Logistic Management		✓			✓
e-Health	Monitoring	✓	✓	✓		✓
	Home care	✓	✓			✓
ITS	Smart fleet	✓	✓			✓
	Automotive	✓	✓	✓	✓	✓
Smart city	Environment monitoring	✓	✓			✓
	Safety	✓	✓			✓
	Food traceability	✓	✓			✓
	Smart Agriculture	✓			✓	✓

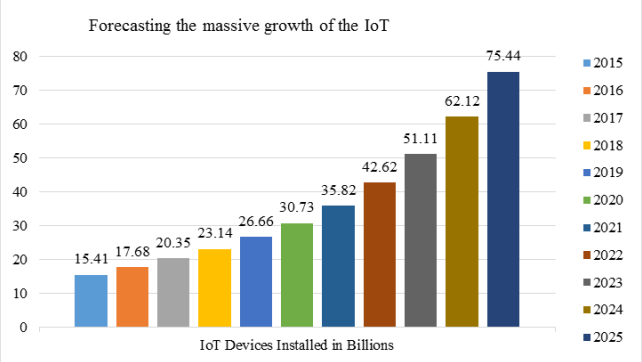


Fig. 7. Forecasst of growth of IoT in billions till 2025

IHS determines that the IoT business will grow from a connected base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025, as seen in Fig 7 as well as the no of devices installed in the year from 2015 to 2025.

Table-III: IoT Devices installation during 2015-2025

Year	IoT Devices Installed in Billions
2015	15.41
2016	17.68
2017	20.35
2018	23.14
2019	26.66
2020	30.73
2021	35.82
2022	42.62
2023	51.11
2024	62.12
2025	75.44

VI. CONCLUSION

The next generation internet grabs all the types of web services offered by internet service provider or current internet. Along with new technologies and emerging electronic computing devices, Future Internet proves that its attempt to present a user convenient system so that the operations can be performed from anywhere in this world.

This remote access needs to trace, identify, authenticate and monitor the objects in these physical systems.
This paper explores the Future Internet and the backbone pillar to implement it, the integral parts of IOT, discrete paradigms associated with IOT and various services oriented applications distributed among various fields.

In future, the work extends in such a way that how this future internet used to track, distinguish and identify people located at different places and also to recognize intruders entered into the network by providing cognition to the machine. Along with the security algorithm, a machine should be equipped with sensors which take their biological traits as inputs.

REFERENCES

1. Dhillon, Parwinder Kaur, and Sheetal Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services, " *Journal of Information Security and Applications*,2017.
2. Nguyen, Kim Thuat, Maryline Laurent, and Nouha Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, 32 2015, pp. 17-31.
3. Atzori, Luigi, Antonio Iera, and Giacomo Morabito, "The internet of things: A survey" *Computer networks*, 2010, pp. 2787-2805.
4. Yi Cheng, Mats Naslund, Goran Selander, and Eva Fogelstrom, "Privacy in Machine-to-Machine Communications", *IEEE International Conference on Communication Systems* (ICCS), 2012
5. X. Jia, Q. Feng, T. Fan and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, 2012, pp. 1282-1285.

6. C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414-454, First Quarter 2014.
7. Ebling, Maria R, "Pervasive computing and the Internet of things," *IEEE Pervasive Computing*, Vol 15, no. 1, 2016, pp. 2-4
8. Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services" *Internet of things (WF-IoT), 2014 IEEE world forum on. IEEE*, 2014.
9. Gigli, Matthew, and Simon Koo, "Internet of things: services and applications categorization," *Advances in Internet of Things*, Vol 1, no. 02, 201, pp. 27
10. Hussain, S. Mahaboob, Prathyusha Kanakam, and A. S. N. Chakravarthy, "Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT," *International Journal of Control Theory and Applications*, Vol 10, no. 4, 2017, pp. 251-255.
11. C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414-454, First Quarter 2014.

AUTHORS PROFILE

Prathyusha Kanakam pursuing her Doctoral Studies in Computer Science Engineering from JNTU Kakinada. She received her Master of Technology in Computer Science Engineering from JNTUK- University College of Engineering Vizianagaram. Currently, she is working as Assistant Professor at MVGR College of Engineering. Her research interests are Biometrics Securities and Semantic Web. She currently serves as Editorial Board Member, Technical Committee Member, Organizing Committee Member and Reviewer for several reputed International Journals and Conferences. She is well recognized in research with 30 research publications, certifications. She received One Research Excellence Award, One Young Woman award and Four Best Paper Awards in research so far.

Dr. A. S. N Chakravarthy received his Doctoral degree from Acharya Nagarjuna University. Currently he is working as Associate Professor in CSE, JNTUK-University College of Engineering Vizianagaram University and coordinator for MOOCs in JNTUK Kakinada. He has several publications in National, International Journals and conferences. He received various awards in his career like Best Professor and Best Faculty in Computer Science by Association of Scientists, Developers and Faculties [ASDF]. His research interests are Forensics science, Network securities and Biometrics having with more than 60 research publications.