Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 123-128
Received 15 April 2021; Accepted 05 May 2021.

A Critiqueon Internet of Things Architecture, Applications and Challenges

K.Kowsalyadevi[1], Dr.N.V.Balaji[2],
[1]Research Scholar, [2]Dean,
[1,2]Faculty of Arts, Science and Humanities, Karpagam Academy of Higher Education, Coimbatore.

Abstract

IoT is now vital role and up to date research trends in today world. It's a set of Multiple Sensors an Actuators Network together which gathers information and those they are altogether having sensors. It's a bunch of Components which each have sensors they're network and that they collect data, the information is getting processed within the cloud or within the local server and every one the connections everything happen in Internet. In this paper comprises the Evolution and Applications of IoT in respect of layers architecture, Applications and key challenges.

Keywords: Internet of Things, IoT Architecture, IoT Applications

INTRODUCTION

A Network is defined to be the interconnection of two or more autonomous computer to be communicated. One certainty is that Internet of Things changes our life styles, it's for commonweal, and also the need is that the input and support of technologies and ordinary people to create it good for people and therefore the society. An IoT model involves numerous actors which include mobile operators, software developers, access technology providers, and so on. E application[1] domains of IoT are very broad and such networks are often deployed in manufacturing, utility management, agriculture, and healthcare. IoT are often seen because the next generation interconnection paradigm which can enable connectivity among people's devices and machines enabling actions to happen without human intervention. Success of the IoT world requires a merger of a distinct communication infrastructure. It's has cause the planning of smart gateways to attach IoT devices with the normal Internet. Most up-to-date efforts are directed to interconnect IoT infrastructure8 and cloud computing which supplements the potentials of IoT.

The Internet of things (IoT) gives a combination of different sensors and articles that can discuss straightforwardly with each other without human intercession. The "things" in the IoT incorporate physical Gadgets, like sensor gadgets, which screen and assemble a wide range of information on machines and human public activity. The appearance of the IoT has prompted the steady general association of individuals, articles, sensors, and administrations. The principle objective of the IoT is to give an organization, foundation, interoperable, correspondence, conventions and programming to permit the association and joining of physical/virtual sensors, (PCs), keen gadgets, vehicles, and things, like ice chest, dishwasher, microwave, food, and meds, whenever and on any organization.

The advancement of cell phone innovation permits incalculable items to be a piece of the IoT through various cell phone sensors. Notwithstanding, the prerequisites for the huge scope organization of the IoT are quickly expanding, which at that point brings about a significant security concern. Security issues, like protection, approval, confirmation, access control, and framework design, data stockpiling, and the executives, are the principle challenges in an IoT climate. For example, IoT applications[19], for example, cell phone and implanted gadgets, help give an advanced climate to worldwide network that streamlines lives by being touchy, versatile, and receptive to human needs. Be that as it may, security isn't ensured. The protection of clients may be undermined and the data on clients might be spilled when client signal is hindered or caught. To broadly receive the IoT, this issue ought to be routed to give client trust regarding protection and control of individual data. The advancement of IoT significantly relies upon tending to security concerns.

A research published by Transform a Insights revealed that the quantity of active IoT devices globally is anticipated to growth from 7.6 billion in 2019 to 24.1 billion in 2030, thereby generating revenue of quite $1.5 trillion, at 11% CAGR. North America, China, and Europe will dominate the IoT market in 2030, with 26%, 24% and 23% respectively of the entire value (Figure 1).

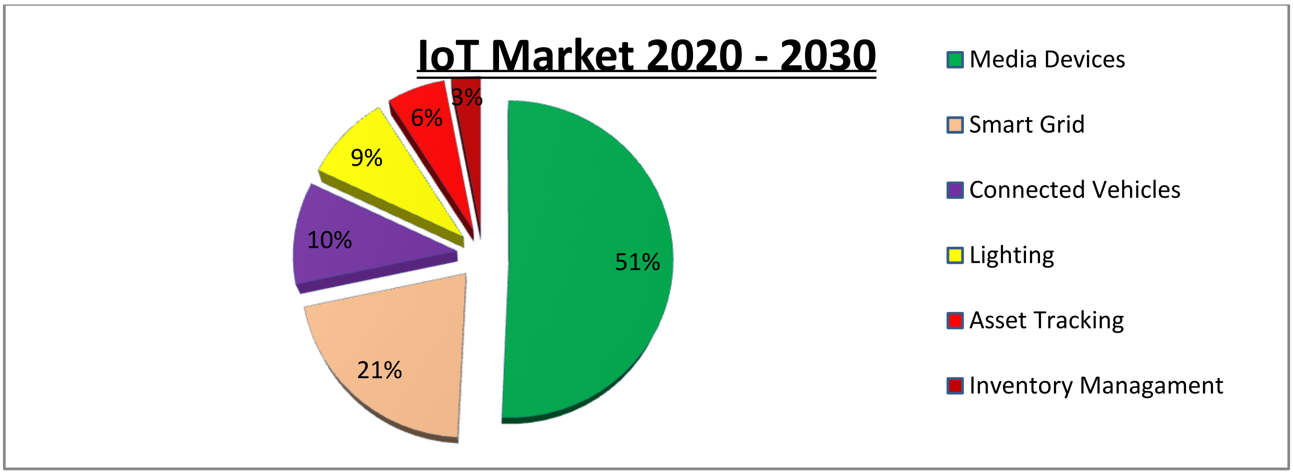

Figure 1: IoT in the era of 2030

This paper addresses the existing development trends, thegeneric architecture of IoT, IoT distinguishing features andpossible future applications. The IoT is a hot research topicthat is getting increasing popularity for academia, industry aswell as government. Many European and American organizationsand multinational companies are involved in the designand development of IoT to achieve different type of useful and powerful automated services[1]. The IoT has to face manychallenges in its deployment especially in the field of security.
The rest of the paper is organized as follows. Section II describes briefly the evolution of Internet of Things. Section III presents the generic architecture of IoT. Section IV forecasts possiblefuture application of IoT. Section V describes key challengesin the design and implementation of IoT. Finally, Section VI concludes the paper.

EVOLUTION OF IoT

The Internet of Things (IoT) is the network of physical objects of “things” embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. In 1999 Kevin Ashton, co-founder of the Auto-ID (for Automatic Identification) Center at MIT introduced the term “Internet of things” shown in Figure 2. IoT was supported reinventing RFID[2] as a networking technology by linking objects to the web using the RFID[19] tag. In 2008, Different industry stakeholders close to make the IPSO Alliance to market connected devices. This was an enormous leap towards having the IoT implemented for big scale business in real production setups. 2008 and beyond: we've got connected home, connected cars, IoT enabled manufacturing plants, and IoT based solar trackers. Internet of Things has spread its wings across the industries and a more recent term “Enterprise IoT (EIoT)” has been established that has devices utilized in business and company setups .

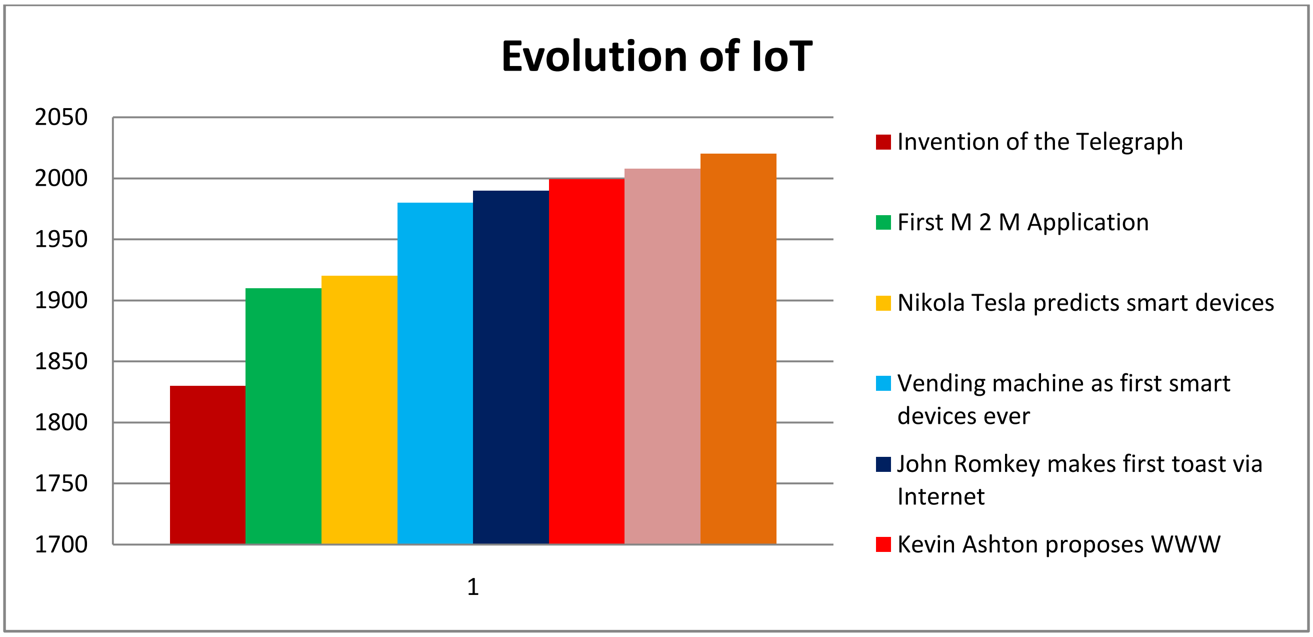

Figure 2: It depicts the Evolution of Internet of Things

IOT ARCHITECTURE

There are four significant layers in the IoT architecture that describes all the functionality of IoT system. The Perception layer, Network Layer, Support or Middle Layer and Application Layer.

Table1: IoT layers and its protocols

Layers	Objects	Protocols
Application Layer	Smart Applications and Management	HTTP(HyperText Transfer Protocol), CoAP(Constrained Application Protocol), SSH(Secure Shell), DNS (Domain Name System), NTP (Network Time Protocol),DLMS (Device Language Message Specification), DNP (Distributed Network Protocol).
Support or Middle Layer	Service Management, Database	
Network Layer	3G, UMTS, Wifi, Bluetooth, Infrared, Zig Bee.	IPV4/IPV6, RPL(Routing ProtocoL), TCP/UDP(Transmission Control Protocol/ User Datagram Protocol), ulP (Upper layer Protocol), SLIC (Subscribe Line Interface Circuit), 6loWPAN
Perception Layer	RFID, QR code, Barcode, Infrared, Sensors	IEEE 802.11 Series, 802.15 series, 802.3, 802.16, Wireless HART (Highway Addressable Remote Transducer), Z-WAVE, UWB (Ultra Wide Band), IrDA(Infrared Data Association), PLC(Programmable Logic Controller), Lornworks, KNX(Konnex).

STAGE 1: Perception Layer

It's also called as Recognition Layer[3]. It consists of networked things typically wireless sensors and actuators. Information gathered with the assistance of Physical equipment shown Figure 3 (RFID reader, GPS and every one types of sensor), like temperature sensors, humidity sensors, pressure sensors, flow sensors or ultrasonic sensors or sound, video etc. This layer converts data into signals and transfer to the Network Layer through secure channels. The following protocols are used in that layer IEEE 802.11 Series[18], 802.15 series, 802.3, 802.16, Wireless HART, Z-WAVE,UWB,IrDA,PLC,Lornworks,KNX…etc.

STAGE 2: Network Layer

Internet gateways and data acquisition that features sensor data aggregation systems and analog to digital conversion. This layer securely transfers the info from sensor device to the information processing system. Protocols are used in that layer such as IPV4/IPV6, RPL[17], TCP/UDP, ulP, SLIC, 6loWPANetc.The transmission mediums[4] are often wired or wireless technology will be 3G, UMTS, Wifi, Bluetooth, infrared, Zigbee, etc. Thus the Network layer transfers the data from perception layer to Middle layer.

STAGE 3: Support Layer or Middle Layer

The system performs[9] pre processing at the information before it moves to the information center or cloud. This layer is accountable for the service management and should link with the database. It receives the info from Upper layer and store within the database[13]. It performs processing a ubiquitous computations and takes automatic decision supported the results.

STAGE 4: Application Layer

Data center and cloud is where the information is analyzed, managed and stored on traditional rear data center systems. This layer answerable for applications management supported the processed information within the middle layer. The applications are often smart health[5], smart car, smart glasses, smart transportations etc.HTTP, CoAP, SSH, DNS, NTP,DLMS, COSEM, DNP, MODBUS protocols are used in that application layer.

IoT APPLICATIONS

The IoT ability allows various applications to be developed based on it, which only a few are currently deployed. Some of the essential IoT applications shown Figure 4 are briefly discussed in the following section;

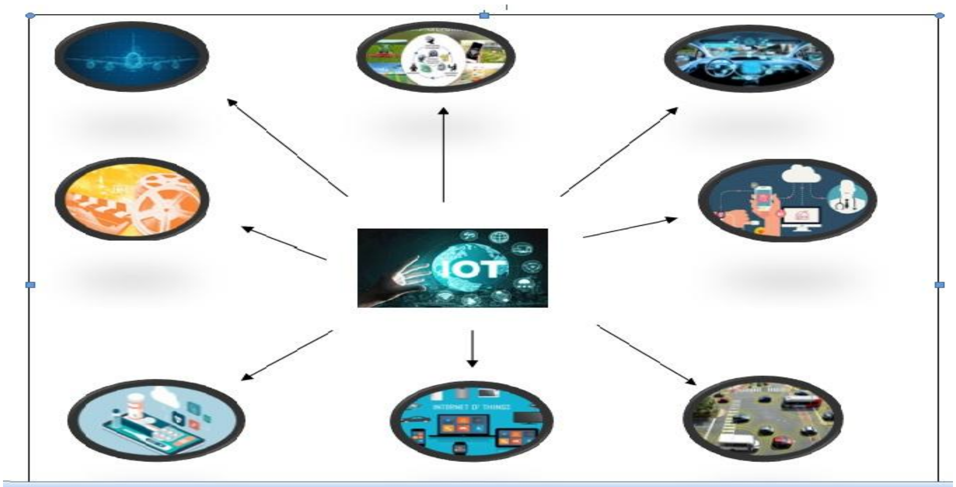

Figure 3: Applications of IoT

1. **Aerospace and Aviation**

IoT adoption in the aerospace industry is transforming both ground and air operations[14]. In order to develop and deploy robust analytical strategies to improve operational efficiency, aerospace producers use IoT. Extensive IoT connectivity [11] allows devices to come together and allows effective coordination, cooperation, communication and interoperability between human-to-human and human-to-machine. These are the primary ingredients in efficient and profitable activities in this area.

2. **Automobile**

IoT has allowed greater transportation efficiency and management capabilities in the automotive sector and is leading us to a smart, autonomous vehicle future. The global automotive IoT[12] market is anticipated to hit USD 100 billion, according to market research by Netscribes, increasing need to save time and optimize efficiency in the fast paced world.

3. **Telecommunication**

Telecom companies are well positioned to be one of the largest IoT players as they allow most internet device connectivity while their current investment is mainly on tracking, they will utilize IoT to expand their B2B contracts and provide customers with new services.

4. **Medical and Healthcare**

Remote monitoring[7] in the healthcare sector has been made possible by IoT enabled devices, unleashing the ability to keep patients safe and secure, and inspiring doctors to provide superlative treatment as interactions with doctors have become simpler and more effective, it has also increased patient involvement and satisfaction. Remote[19] patient health monitoring tends to reduce the duration of hospital stay and avoids re-admissions.

5. **Transportation[3]**

Enhanced communication, control and data distribution are provided by IoT[15]. Personal cars, commercial vehicles, trains, UAVs and other equipment are included in these applications. It extends throughout the entire system of all transportation elements such as traffic control, parking, fuel consumption and more.

6. **Agriculture**

In IoT based smart farming[9], with the aid of sensors (light, humidity, temperature, soil moisture, etc and the automation of the irrigation system, a system is constructed to monitor the crop field. From anywhere, farmers can monitor the field conditions. In comparison with the convention approach, IoT based smart farming is highly efficient.

IOT KEY CHALLENGES

Workflows will be categorized by cross organizational interaction in the field of business, home, workplace and other smart spaces in the future. There are following main challenges:

Security/ Personal Safety:

User data cloud is vulnerable for theft, If one device is getting attacked, Cloud[8] also attacked. It means attacker's damage the whole Network.

Privacy
In cloud, tracked and Monitored by everyone. Extract information and Measure the data from complex Environment.There has been no research in security vulnerabilities[9] and its improvements. It should ensure Confidentiality, Integrity[11] and Availability of non-public data of patient.

Scalability
Billions of internet-enabled devices[9] get connected in a very huge network, large volumes of knowledge are needed to be processed. The system that stores, analyses the information from these IoT devices must be scalable. In present, the age of IoT evolution[7] everyday objects are connected with one another via Internet. The information obtained from these devices need big data analytics and cloud storage for interpretation of useful data.

Connectivity; With the event in technology design challenges[6] are increasing at a faster rate. There are issues regarding design like limited computation power, limited energy and limited memory which require to be sorted out.

Interoperability
IOT maturity comes with several challenges specifically pertaining to interoperability[10] and interfacing the reasons is coexistence of multifactor's systems. That interchange[16] location time dependent information in varied data formats languages data models constructs data quality and complex[21].

CONCLUSION

This paper surveyed a number of the foremost important aspects of IoT Evolution, Architecture and Applications and at last addressed a number of the key challenges keep company with the IoT technology. This can be IoT based and should include smartphone and smartwatches compatibility, since today these devices are used as an integral part of everyday life and are viewed as highly relevant and effective resources for the provision of updates and constructive coaching in order to enhance the health of their consumers and therefore public health. It ends up in the vision of "anytime, anywhere, any media, anything "communication.

REFERENCES

1. Sachin Kumar, Prayag Tiwari and MikhaliZymbler," Internet of things is a revolutionary approach for future technology enhancement: A Review", Journal of Big data, 2019, https://doi.org/10.1186/s40537-019-0268-2
2. A.Prasanth, S.Jayachitra, 'A Novel Multi-Objective Optimization Strategy for Enhancing Quality of Service in IoT enabled WSN Applications', Peer-to-Peer Networking and Applications, Vol.13, 2020, pp.1905–1920
3. SuraponKraijak, PanwitTuwanut, "A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real World Implementation and Future Trends", IEEE, 2005.
4. Mohsen HallajAsghar, NasibehMohammadzadeh and AtulNegi, "Principle Application and Vision in Internet of Things", ISBN: 978 – 1 – 4799 – 8890 – 7, IEEE, 2015.
5. Rafiullah Khan, SarmadUllahKhan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", IEEE Computer Society, 2016.
6. A.Prasanth, 'Certain Investigations on Energy-Efficient Fault Detection and Recovery Management in Underwater Wireless Sensor Networks', Journal of Circuits, Systems, and Computers, Vol. 30, 2020.
7. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt. Inf. J. 2017, 18, 113–122.
8. A.Prasanth, S.Pavalarajan, 'Implementation of Efficient Intra- and Inter-Zone Routing for Extending Network Consistency in Wireless Sensor Networks', Journal of Circuits, Systems, and Computers, Vol.29, 2020.
9. Muhammad A. Iqbal, OladiranG.Olaleye&Magdy A. Bayoumi, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches", Global Journal of Computer Science and Technology: E Network, Web & Security, Volume 16 Issue 7 Version 1.0 Year 2016.
10. S. UshaKiruthika, S. KanagaSubaRaja, R. Jaichandran, 'IOT based Automation of Fish Farming', Journal of Advanced Research in Dynamical and Control Systems, ISSN: 1943-023X, Volume 09, Issue 1, 2017
11. NargesYousefnezhad, AvleenMalhi, KaryFrämling, "Security in product lifecycle of IoT devices: A survey", Journal of Network and Computer Applications 171 (2020).
12. Gianna Reggio, Maurizio Leottaa, et.al. "What Are IoT Systems for Real? An Experts' Survey on Software Engineering Aspects", https://doi.org/10.1016/j.iot.2020.100313.
13. Abbas, N., Asim, M., Tariq, N., Baker, T., Abbas, S., 2019,"A mechanism for securing iot-enabled applications at the fog layer", J. Sens. Actuator Netw. 8 (1), 16, https://doi.org/10.3390/jsan8010016.

14. Ding, S., Cao, J., Li, C., Fan, K., Li, H., 2019.,"A novel attribute-based access control scheme using blockchain for IoT", IEEE Access 7, 38431–38441, https://doi.org/10.1109/ACCESS.2019.2905846.
15. Dinh, N., Kim, Y., 2018.,"An efficient availability guaranteed deployment scheme for iot service chains over fog-core cloud networks", Sensors 18 (11), 3970, https://doi.org/10.3390/s18113970.
16. Eugster, P., Kumar, S., Savvides, S., Stephen, J.J., 2019,"Ensuring confidentiality in the cloud of things", IEEE Perv. Comput. 18 (1), 10–18, https://doi.org/10.1109/MPRV.
17. Suk Kyu Lee, Mungyu Bae and Hwangnam Kim, "Future of IoT Networks: A Survey", 2017, Applied Science, https://doi:10.3390/app7101072.
18. Dhillon, P.K.; Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments", Int. J. Commun. Syst. 2017, doi:10.1002/dac.3323.
19. Happ, D.; Karowski, N.; Menzel, T.; Handziski, V.; Wolisz,"A Meeting IoT platform requirements with open pub/sub solutions", Ann. Telecommun. 2017, 72, 41–52.
20. A.Prasanth, S.Pavalarajan, 'Zone-Based Sink Mobility in Wireless Sensor Networks', Sensor Review, Vol.39, pp.874–880, 2019
21. Murugan, S., Jeyalaksshmi, S., Mahalakshmi, B., Suseendran, G., Jabeen, T. N., & Manikandan, R. (2020). Comparison of ACO and PSO algorithm using energy consumption and load balancing in emerging MANET and VANET infrastructure. *Journal of Critical Reviews*, *7*(9), 2020.