A Comprehensive Review on Internet of Things (IoT)

Pawan Kumar[1], Satvir Singh[2], Lavish Kansal[3]
[1]*Deptt. of Electronics &Communication Engg., I.K. Gujral Punjab Technical University, Kapurthala, Punjab, India*
[2]*Deptt. of Electronics &Communication Engg., I.K. Gujral Punjab Technical University, Kapurthala, Punjab, India*
[3] *Deptt. of Electronics & Electrical Engg., Lovely Professional University,Jalandhar, India*
Email: [1]Pawankumar945@gmail.com, [2]drsatvir.in@gmail.com
[3]lavish.15911@lpu.co.in

***Abstract*—In the near future, the interconnection of physical devices going to bring revolution in Internet, mobile and Machine to Machine (M2M) technologies. This paper presents an overview of the Internet of Things (IoT) and its architectures. Compared with survey papers in the related field this paper overviewed the challenges and applications of IoT. The challenges described helps to explore the future scopes of IoT.**

Keywords: Architecture, Challenges, GPS, Internet of Things (IoT), M2M, RFID.

I. Introduction

The collection of "things" included with sensors, actuators, software, electronics connected via Internet to gather and tansfer data with each other is termed as Internet of Things (IoT). It is the resultant of unprecedented increase in networking of appliances, machines and home appliances. These devices are eqipped with processing power and sensors that enable them to be deployed in many enivironments. This is posing many threats/opportunities for the researchers to make them versatile and secure. HVAC (Heating, Ventilation, and AirConditioning) monitoring and control systems are most common instances of these objects for smart homes. Few others domains are also there that can enhance the quality of life we live. All other applications includes emergency response to natural and man-made disasters, healthcare and transportation. Part 2 and 3 introduces the IoT and its architecture. Part 4 and 5 shows the challenges faced in the IoT and application areas in field.

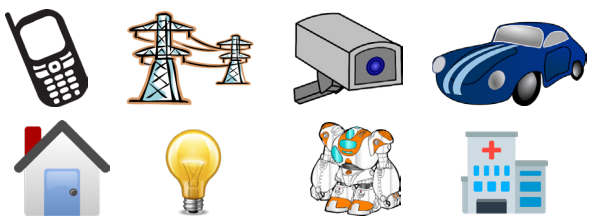


Fig. 1: Application Areas of IoT

II. Internet of Things (IoT)

Internet of things (IoT) is the integration of various sensors and objects that make communication with one another without the intervention of humans. Oladayo Bello [1] et al. tells that although most of the standards discussed are geared toward application domains within the IoT.J. Lin et al. [2] presented a comprehensive review of IoT including enabling technologies. Yongfeng Cui et al.[3] says that IoT is the new revolution in the world of information industry after internet and mobile communication. The IoT word itself consists of two words - "Internet" and "Things". The term "things" represents various physical devices like sensors that collects and monitors data related to human social life and "Internet" characterizes various physical devices that are connected over internet. Overall, it is the connections of physical devices over the Internet. A.L. Sangeetha et al. [4] tells that internet architecture described in the paper is safer than Internet mediated direct remote control establishment. K. Sha et al. [5] describes that with increasing deployments of the IoT systems, security becomes a key component to protect both the cyber and the physical world.With the advancement in the smartphone technology it enables numerous devices to be the part of IoT with the sensors presents[5].S. Sıngh et al. [6] tried to shows various security challenges, vulnerabilities, attacks and threats that hampers the adoption of cloud computing. J. M. Talavera et al. [7] reviewed the agro-industrial and environmental applications that are using the IoT. A. Tewari et al. [8] described the security issues among all the other challenges of the IoT. A.J. C. Trappey et al. [9] provides the formal overview of standards and patents for IoT as a key enabler for the next generation advanced manufacturing. S. Verma et al.[10] tells that the requirements of real time IoT analytics is not taken into account by the existing IoT systems. M. Weyrich et al. [11] advised that the countries of the world should start on the digitized IoT network as it has become the most disruptive technology changing software and society. A.

ISBN: 978-93-91355-11-1

Makkar et al. [12] proposes scheme that enhances the ability of search engine to detect the link spam.

Table 1: IoT Market in Across Globe and in India[34]

S.No.	IoT Global	IoT India
1.	IoT market will raise from 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025	IoT market expected to grow $ 15 billion with 2.7 billion units from current $ 5.6 billion and 200 million connected units by 2020
2.	Global expenses on IoT based products and services by initiatives are projected to reach $120 billion-$253 billion attaining a 16% CAGR during 2016-2021	IoT market in india is expected to grow more than 28% at a CAGR during 2015-2020 and business is expected to touch $300 billion by 2020
3.	IoT market will increase to $15 trillion from $10 trillion to global GDP in the next 20 years	Indian government is objective to generate an IoT production in india of $15 billion by 2020
4.	Automated driving and IoT enable vechile will increase globally by 2020	Utility sector and oil sector will slowly reach on top 5 sector like electronics and telecom.

III. IoT Architecture

Since the IoT is going to connect billions of different devices, so there is a requirement of flexible architecture. From a collection of several models, the basic model is 3-layerarchitecture. M. Saadeh et al. [13] presented a hierarchical architecture for IoT mobile object authentication in the context of smart cities. P. Asghari et al. [14] presented a SLR-based research for the IoT service composition approaches. J. Massana et al. [15] tells about an ongoing work to embed various services under the Smart city architecture for attaining sustainable development. C.M.Sosa-Reyna et al. [16] provided a methodology for development of software applications for IoT. R.Mehta et al. [17] tells that the day to day life can be improved by interconnecting the smart objects, technologies and applications. O. Salman et al. [18] described that the challenges of IoT such as the high scalability and management complexity produces problems in IoT applications implementation. The architecture is divided into three layers-Perception layer, Network Layer and Application layer.

A. Perception Layer

Perception layer is also known as sensory layer whose primary functioning is to interacts with the physical devices and components through smart devices like RFID, sensors and actuators etc. The objective of sensory layer is to connect thing into IoT network and thereon collect, measure and process the state information associated with these things via smartly deployed devices. It transfers the processed information into the upper layers via layer interfaces.

B. Network Layer

The middle layer of IoT architecture is also named as transmission layer. This network layer receives the processed information from perception layer and further it determines the route of data and information transmission to the IoT hub. It is important layer in IoT architecture because devices like switches, gateway etc. and various communication technologies like WiFi, Long Term Evolution (LTE) and Bluetooth are integrated in this.

C. Application Layer

Application layer, also called the business layer is the top layer of the IoT architecture. It receives the data transmitted from the network layer and uses it for various services and operations. For example, this layer can provide the storage service to backup received data into a database. Further it can help for predicting future states of physical devices.

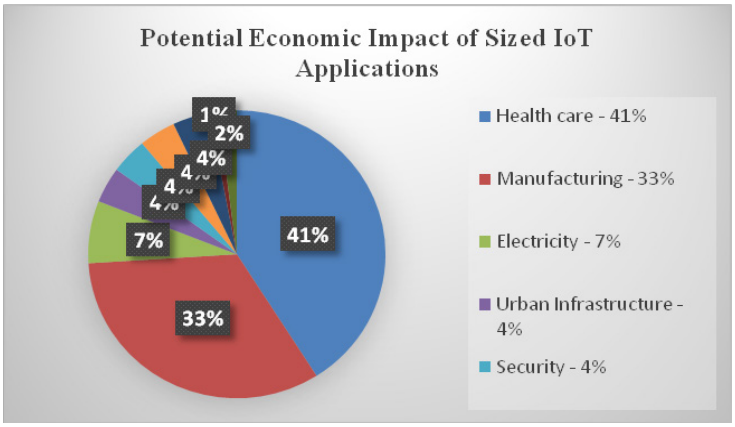


Fig. 2: Expected Market Share of IoT Applications by 2025

ISBN: 978-93-91355-11-1

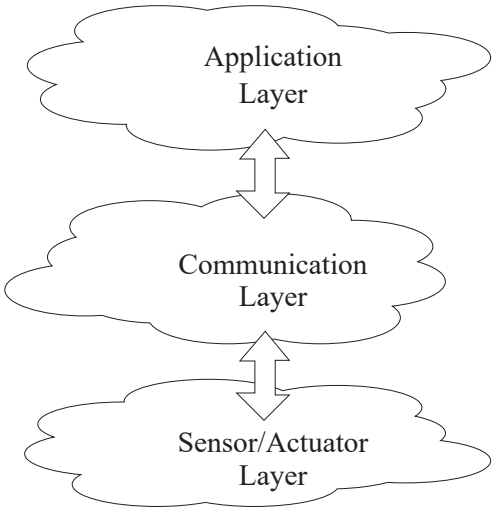
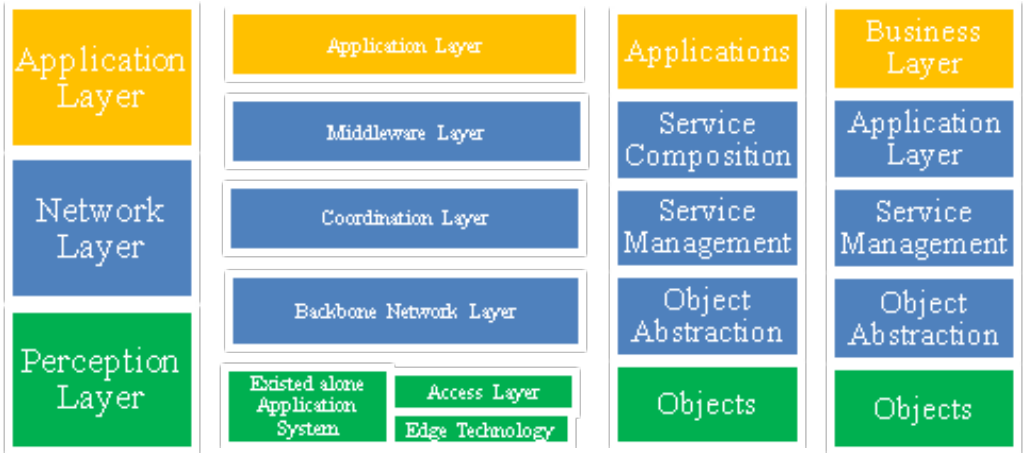


Fig. 3: Three Layer IoT Architecture



(a) (b) (c) (d)

Fig. 4: IoT Architecture (a) Three Layer (b) Middle ware based (c) SOA based (d) Fıve Layer

III. Challenges of the Internet of Things

A. Security

The essential pillar of the internet and major challenge for the IoT. As time elapses the trend of IoT inflates to te.2ns of millions from millions of devices. The chances to exploit safety vulnerabilities is also going to increase as the number of connected devices are increased. The collection of devices may include similar devices.Any single security weakness has a potential impact on the total number of devices that have the same featutes [6],[8],[19].

B. Privacy

The smart objects would need to be secure from opponents apart from the authenticity, trustworthiness and confidentiality aspects. The cloud storage sometime needs a third partywhich also poses a challenge [8],[20-35]. There is need to prepare some new strategies for the privacy choices.

C. Standards

Lack of standards can lead to the senseless activities of IoT devices. The undesirable consequences for the networking resources are results of cheap desıgned and configured devıces. The design products operate in disruptive ways on the internet without standards to guide developers and manufacturers. The technology can be easily available everywhere and can be used by all the applicants when have a standard development process and increase tbe growth also.

D. Trained workforce

Every technology implementation need team of skilled persons those have adequate knowledge of software, hardware network and about the technology. Every organization face a lots of problem during thier phase of changeover from the legancy system to IoT enabed systems.

ISBN: 978-93-91355-11-1

Table 2: Review of Survey on Risk ,Security and Challenges in IoT[34]

S.No.	Survey	Citation	Year	Security & Risk Factor	Challenges
1.	The Internet of Things for Health Care: A Comprehensive Survey	[21]	June, 2015	• Computational Limitations • Memory Limitations • Energy Limitations • Scalability • Mobility • Communications Media • Data Protectio	• IoT Healthcare Platforms • Cost Analysis • Technology Transition • The Low • Power Protocol • Scalability
2.	A Survey on Challenges, Technologies and Applications of IoT.	[35]	March,2016	• Front end sensors and equipment • Networks • Backend of its System	• Scalability • Device Heterogeneity • Energy Optimized Solution • Ubiquitous Data Exchange Through Wireless Technology • Self-Organization Capabilities • Semantic Interoperability and Data Management
3.	Internet of Things (IoT) : Challenges and Future Directions	[36]	March,2016	• As IoT connects more devices together, itprovides more decentralized entry points for malware • Trust and Privacy.	• Standardsand interoperability • Complexity, confusion and integration issues. • Internet connectivity and power requirement.
4.	Smart Home Analysis in India: An IOT Perspective	[37]	June,2016	• Unique identification low security at the server side. • Privacy • Authentication	• Reliability • Co-ordination among connected objects, • Integration of several devices increases the system complexity andconnectivity problem. • Cost and Storage • Self-organisation of network so that there is no data loss due to network failure.
5.	Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective	[38]	Nov, 2016	• Risk is to store the sensitive data either on local server or to use VPN in case using the remote server of vendor. • When Security system based on the CCS (Centralized Controlled System) for processing, application and data storage, then a risk of central point of failure is increase • End point protection, Trust & Safety, Physical Security. • Hacking, DoS , updation, virus, password based attacks and phishing	• Internet connectivity consistency and accessibility of necessary signals bandwidth. • Cost of technology. • Poor supporting organizational setup. • IoT adoption due to nonexistence of welltrained staff. • Lack of awareness of IoT Systems, Services and Applications.
6.	Health Care Systems Using Internet of Things	[39]	December, 2016	• Data security causes concerns in theimplementation of IoT in healthcare.	• Lack of EHR system integration. • Interoperability challenges keep IoT data in different silos. • IoT data alone may not be as meaningful if it is not within the context of a full health record. • Constant changes in hardware and connectivity technology.

V. Applicatons Areas

A. Prediction of Natural Calamities

The natural calamities like earthquake, volcanic eruptions etc. can be predicted through the coordination, interaction and simulation.

B. Detection of Water Shortage

Water shortage is one of the major problem of today's scenario. The IoT network can find out the shortage of water at the possible locations. The sensors not only monitors the water shortage but it can also identifies the release of sewage in water stream which may lead to the accidental hazards.

ISBN: 978-93-91355-11-1

C. Smart Homes

The energy consumption can be managed by IoT via the interaction among the home appliances, finding emergencies and ensuring safety etc.

D. Healthcare

The medical area can be made better by increasing the life of certain monitoring metrics related with health and medicines inventories in the hospital.

E. Smart Farming

With the help of sensors different land requirements can be identified and as per that necessary actions can be taken. It can enhance the productivity of farmers by giving information about the possible land conditions and climate instability.

F. Smart Transport

A network of sensors can effectively monitor the traffic and apply necessary actions like deviating the traffic etc.

G. Smart Cities

The IoT can helps in designing the smart cities e.g. observing the good air quality, emergency routes etc.

H. Smart Security

The area of security can also implement IoT networks for inspection of spaces, maintaining infrastructure and alarming etc.

VI. Conclusion

In conclusion, IoT will serve as a pathbreaker technology but the large amounts of data increases its complexity in detection, communications, controller and in producing awareness but the growth will increase will passage of intervals. The future of IoT will be predicted to be integrated. The paper presented survey of the most important issues and challenges of the IoT and future improvements.

References

[07] Bello, O., and Zeadally, S.:Toward efficient smartification of the Internet of Things (IoT) services. Future Generation Computer Systems. 92, 663-673(2019)

[08] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W.: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal. 4, 1125-1142(2017)

[09] Cui, Y., Ma, Y., Zhao, Z., Li, Y., Liu, W., and Shu, W.: Research on data fusion algorithm and anti-collision algorithm based on internet of things. Future Generation Computer Systems. 85, 107-115(2018)

[10] Sangeetha, A. L., Bharathi, N., Ganesh, A. B., and Radhakrishnan, T.: Particle swarm optimization tuned cascade control system in an Internet of Things(IoT) environment. Measurement. 117, 80-89(2018)

[11] Sha, K., Wei, W., Yang, T. A., Wang, Z., and Shi, W.: On security challenges and open issues in Internet of Things. Future Generation Computer Systems. 83, 326-337(2018)

[12] Singh, S., Jeong, Y.-S., and Park, J. H.:A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications. 75, 200-222(2016)

[13] Talavera, J. M., Tob´on, L. E., G´omez, J. A., Culman, M. A., Aranda, J. M., Parra, D. T., Quiroz, L. A., Hoyos, A., and Garreta, L. E.: Review of IoT applications in agro-industrial and environental fields. Computers and Electronics in Agriculture. 142, 283-297(2017)

[14] Tewari, A. and Gupta, B.:Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems.(2018)

[15] Trappey, A. J., Trappey, C. V., Govindarajan, U. H., Chuang, A. C., and Sun, J. J.: A review of essential standards and patent landscapes for the Internet of Things:A key enabler for Industry 4.0. Advanced Engineering Informatics. 33, 208-229(2017)

[16] Verma, S., Kawamoto, Y., Fadlullah, Z. M., Nishiyama, H., and Kato, N.: A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues. IEEE Communications Surveys Tutorials. 19(3), 1457-1477(2017)

[17] Weyrich, M. and Ebert, C.:Reference Architectures for the Internet of Things. IEEE Software. 33, 112-116(216)

[18] Makkar, A. and Kumar, N.: Cognitive spammer: A Framework for PageRank analysis with Split by Over-sampling and Train by Under-fitting. Future Generation Computer Systems. 90, 381-404(2019)

[19] Saadeh, M., Sleit, A., Sabri, K. E., and Almobaideen, W.: Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. Journal of Network and Computer Applications 121, 1-19(2018)

[20] Asghari, P., Rahmani, A. M., and Javadi, H. H. S.: Service composition approaches in IoT: A systematic review. Journal of Network and Computer Applications. 120, 61-77(2018)

[21] Massana, J., Pous, C., Burgas, L., Melendez, J., and Colomer, J.: Identifying services for short-term load forecasting using data driven models in a Smart Cıty platform. Sustainable Cities and Society 28, 108-117(2017)

[22] Sosa-Reyna, C. M., Tello-Leal, E., and Lara-Alabazares, D.: Methodology for the model-drieven developmentof service oreiented IoT applications. Journal of Systems Architecture. 90, 15-22(2018)

[23] Mehta, R., Sahni, J., and Khanna, K.: Internet of Things: Vision, Applications and Challenges. Procedia Computer Science. 132, 1263-1269(2018)

[24] Salman, O., Elhajj, I., Chehab, A., and Kayssi, A.: IoT survey: An SDN and fog computing perspective. Computer Networks 143, 221-246(2018)

[25] Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F.: Internet of Things security: A survey. Journal of Network and Computer Applications 88, 10-28(2017)

[26] Yang, Y., Wu, L., Yin, G., Li, L., and Zhao, H.: A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal 4(5), 1250-1258(2017)

ISBN: 978-93-91355-11-1

[27] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., and Kwak, K.: The Internet of Things for Healthcare: A comprehensive Survey. IEEE Access. 3, 678-708(2015)

[28] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M.: Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys Tutorials. 17, 2347-2376(2015)

[29] Zhao, J., Gao, Y., Yang, Z., Li, J., Feng, Y., Qin, Z., and Bai, Z.: Truck Traffic Speed Prediction Under Non-Recurrent Congestion: Based on Optimized Deep Learning Algorithms and GPS Data. IEEE Access. 7, 9116-9127(2019)

[30] Nguyen, H., Kieu, L.-M., Wen, T., and Cai, C.: Deep learning methods in transportation domain:a review. IET Intelligent Transport Systems. 12, 998-1004(2018)

[31] Rupi, F. and Schweizer, J.: Evaluating cyclist patterns using GPS data from smartphones. IET Intelligent Transport Systems. 12, 279-285(2018)

[32] Zhu, L., Guo, F., Polak, J. W., and Krishnan, R.: Urban link travel time estimation using traffic states-based data fusion. IET Intelligent Transport Systems. 12, 651-663(2018)

[33] Jing, W., Kang, J., and Liu, M.: Mining taxi trajectories for most suitable stations of sharing bikes to ease traffic congestion. IET Intelligent Transport Systems. 12, 586-593(2018)

[34] Mukheja, P., Kiran K, M., Velaga, N. R., and Sharmila, R. B.: Smartphone-based crowdsourcing for position estimation of public transport vechiles. IET Intelligent Transport Systems 11, 588-595(2017)

[35] Hu, L., Zhong, Y., Hao, W., Moghimi, B., Huang, J., Zhang, X., and Du, R.: Optimal Route Algorithm Considering Traffic Light and Energy Consumption. IEEE Access. 6, 59695-59704(2018)

[36] Fang, Z., Jian-yu, L., Jin-jun, T., Xiao, W., and Fei, G.: Identifying activities and trips with GPS data. IET Intelligent Transport Systems. 12, 884-890(2018)

[37] Luo, Q., Zhu, J., Guan, X., and Jia, H.: Optimal Cordon-Based Congestion PricingConsidering Feasible Cordons and Congestion Transfer. IEEE Access. 7, 93545-93557(2019)

[38] Huang, B., Liu, W., Wang, T., Li, X., Song, H., and Liu, A.: Deployment Optimization of Data Centers in Vehicular Networks. IEEE Access. 7, 20644-20663(2019)

[39] Li, W., Jiang, M., Chen, Y., and Lin, M. C.: Estimating urban traffic states using iterative refinement and Wardrop equilibria. IET Intelligent Transport Systems. 12, 875-883(2018)

[40] Yadav, E. P., Mittal, E. A. and Yadav, H.:IoT: Challenges and Issues in Indian Perspective. 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1-5,IEEE, Bhimtal(2018), doi: 10.1109/IoT-SIU.2018.8519869.

[41] Suruthi, M.,Nivetha D.:A Survey on Challenges, Technologies and Applications of IoT. IJARCCE.5, 693-698(2016)

[42] Pundir, Y., Sharma, N. ,Singh Y.:Internet of Things (IoT) : Challenges and Future Directions.IJARCCE. 5,960-964(2016).

[43] Vyas,C.,Patil,S.:Smart Home Analysis in India:An IOT Perspective.International Journal of Computer Applications.144,29-33(2016) .

[44] Roshan, R.,Ray, A. K.:Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective. IJCA.153,16-19(2016).

[45] Gapchup, A., Wani, A., Gapchup, D., and Jadhav, S.:Health Care Systems Using Internet of Things. IJIRCCE.4,17-20(2016).

ISBN: 978-93-91355-11-1