International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
23 – 27

Internet of Things (IoT): Research, Architectures and Applications

Dr. Aditya Tiwary
Associate Professor
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore
Email ID: raditya2002@gmail.com

Manish Mahato
Final year UG Student
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore

Abhitesh Chidar
Final year UG Student
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore

Mayank Kumar Chandrol
Final year UG Student
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore

Mayank Shrivastava
Final year UG Student
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore

Mohit Tripathi
Final year UG Student
Electrical & Electronics Engineering Department
Institute of Engineering & Science
IPS Academy, Indore

***Abstract*—** Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people, all of which collect and share data about the way they are used and about the environment around them. Experts estimate that the IoT will consist of about 30 billion objects by 2020. This paper presents a study based on IoT and its applications in different field of science and technology. Along with the introduction of the IoT literature review is also provided. The paper also discusses the architecture and elements of the IoT along with its different applications.

Keywords- *Internet of Things (IoT), architecture of IoT, Elements of IoT, Smart grid, Smart city.*

*****

I. INTRODUCTION

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure [1], creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention [2-5]. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Things, in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, cameras streaming live feeds of wild animals in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental, food, pathogen monitoring [6], or field operation devices that assist fire fighters in search and rescue operations [7]. Legal scholars suggest regarding "things" as an "inextricable mixture of hardware, software, data and service [8].

Based on above discussion the future of the IoT will be on many applications. Its application will range from smart grid, smart city, intelligent automobiles, smart electricity meters etc. This paper presents a study on IoT and its application in science and technology. A literature review is provided based on different application of IoT. Architecture and elements of IoT, along with key features is also been discussed.

II. LITERATURE REVIEW

A study based on context-aware computing, learning, and big data in Internet of Things was provided by Sezer et al. [9]. Na et al. [10] has proposed energy-efficient mobile charging for wireless power transfer in Internet of Things networks. Jin et al. [11] proposed an information framework for creating a smart city through Internet of Things. Wu et al. [12] develop a new paradigm, named cognitive Internet of Things (CIoT), to empower the current IoT with a “brain” for high-level intelligence. Xia et al. [13] proposed GPS-free greedy routing with delivery guarantee and low stretch factor on 2-D and 3-D surfaces. Ren et al. [14] proposed a technique for exploiting the data sensitivity of neurometric fidelity for optimizing EEG sensing. Yu et al. [15] developed a method for carbon-aware energy cost minimization for distributed internet data centers in smart microgrids. Abdelwahab et al. [16] discussed enabling smart cloud services through remote sensing: an

internet of everything enabler. Khan et al. [17] discussed a design of a reconfigurable RFID sensing tag as a generic sensing platform toward the future Internet of Things. Zhang et al. [18] provided information about ubiquitous WSN for healthcare. Främling et al. [19] proposed a universal messaging standard for the IoT from a lifecycle management perspective. Sheng et al. [20] proposed leveraging GPS-less sensing scheduling for green mobile crowd sensing. Chen et al. [21] discussed information fusion to defend intentional attack in Internet of Things. Kantarci and Mouftah [22] proposed trustworthy sensing for public safety in cloud-centric Internet of Things. Lin et al. [23] proposes a protocol and a method of spectrum management that can guard against common types of security threats despite the limitations of the local processing. New and innovative IoT based applications and its basics were discussed in literature [26-29]. As the Internet of Things (IoT) is emerging as an attractive paradigm, a typical IoT architecture that U2IoT (Unit IoT and Ubiquitous IoT) model has been presented for the future IoT. Based on the U2IoT model, this paper proposes a cyber-physical-social based security architecture (IPM) to deal with Information, Physical, and Management security perspectives, and presents how the architectural abstractions support U2IoT model. In particular, 1) an information security model is established to describe the mapping relations among U2IoT, security layer, and security requirement, in which social layer and additional intelligence and compatibility properties are infused into IPM; 2) physical security referring to the external context and inherent infrastructure are inspired by artificial immune algorithms; 3) recommended security strategies are suggested for social management control. The proposed IPM combining the cyber world, physical world and human social provides constructive proposal towards the future IoT security and privacy protection [30]. The Internet is evolving rapidly toward the future Internet of Things (IoT) which will potentially connect billions or even trillions of edge devices which could generate huge amount of data at a very high speed and some of the applications may require very low latency. The traditional cloud infrastructure will run into a series of difficulties due to centralized computation, storage, and networking in a small number of datacenters, and due to the relative long distance between the edge devices and the remote datacenters. To tackle this challenge, edge cloud and edge computing seem to be a promising possibility which provides resources closer to the resource-poor edge IoT devices and potentially can nurture a new IoT innovation ecosystem. Such prospect is enabled by a series of emerging technologies, including network function virtualization and software defined networking. In this survey paper, we investigate the key rationale, the state-of-the-art efforts, the key enabling technologies and research topics, and typical IoT applications benefiting from edge cloud. We aim to draw an overall picture of both ongoing research efforts and future possible research directions through comprehensive discussions [31].

III. ARCHITECTURE OF IOT

Architecture of IoT [24] depends on various applications of IoT. Fig. 1 shows general 3 layer / 4 layer architecture for IoT. For e.g. consider two scenarios. Scenario-1: Let's consider smart devices for pollution, wherein sensors sense the amount of carbon monoxide, nitrogen dioxide, sound level etc. and sends these data continuously to the central database. These data will be analysed by using analytical tools and gives information about amount of air pollution in that particular city to the traffic police. This information helps to take the precaution when it exceeds the normal level. Here sensor layer indicates sensors will be continuously sensing the air and sends the data through Wired or wireless communication to the database. This data will be processed and analysed and final consolidated result will be send to the user smart phone through the Air pollution control application. Hence four layers architecture is required.

Scenario-2: Let's consider a sensor is attached near the kitchen or gas cylinder with context to find the gas leakage. In this whenever sensor detects gas leakage it has to alert the surrounding immediately and then has to send the message to the owner. In this case analysing has to be done in the sensor layer itself.

IV. ELEMENTS OF IOT:

Essential components [25] which are required to build IoT are i) hardware components such as sensors, actuators, ii) Middleware components such as database for storage and data analytical tools iii) Visualization through different applications. This section explains important IoT key elements which are used to build IoT as shown in Fig. 2.

4.1 Unique identification for each smart device

IoT consists of huge number of smart devices. Each of this devices requires a unique identification for communication and also helps to control and access remote devices through internet. Ipv4 addressing supports limited number of unique addressing for smart devices.

IPv6 provides large set of unique address. Apart from this unique address, each of these devices also has object id. This object id is used to refer the smart device within the communication network.

4.2 Sensing devices

Each object embedded with sensors continuously sense the data based on the context. Context may be sensing humidity or temperature or sound level, amount of air pollution or motion etc.

4.3 Communication

Sensed data from smart devices are sent to the database through the communication technologies. This communication technology may be Radio Frequency Identification (RFID), Bluetooth, Near Field Communication (NFC), Wi-Fi, ultra-wide bandwidth(UWB), Z-wave, 3G, 4G and Long Term Evolution-Advanced (LTE-A).

4.4 Data storage and analytics

In IoT smart devices produces large amount of data, which has to be stored in the storage device. These stored data has to be analysed to extract the meaningful information. To do this, analytics or analytical tool which incorporates intelligent algorithm has to be developed to extract the useful information from raw data. This analytical tool has to support interoperability with different platforms. In the IoT architecture middleware represents the both storage and

 ISSN: 2454-4248
23 – 27

analytical tools. A centralized infrastructure is required to support both Storage and analytical tools.

4.5 Visualization

Nowadays the world has become smart with smart phones. By using smart phones or laptops user has to download the required application and through which user can interact with centralized database and get the useful information about the actual environment.

V. IOT – KEY FEATURES

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below:

1. **AI –** IoT essentially makes virtually anything "smart", meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favourite cereal run low, and to then place an order with your preferred grocer.
2. **Connectivity –** New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.
3. **Sensors –** IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
4. **Active Engagement –** Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.
5. **Small Devices –** Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

5.1 IoT – Advantages

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer:

1) **Improved Customer Engagement –** Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
2) **Technology Optimization –** The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.
3) **Reduced Waste –** IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
4) **Enhanced Data Collection –** Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

5.2 IoT − Disadvantages

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges.

Here is a list of some its major issues:

1) **Security –** IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
2) **Privacy –** The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
3) **Complexity –** Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.
4) **Flexibility –** Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
5) **Compliance –** IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

5.3 Applications of IoT

IoT finds its application in wide area of science and technology. It finds its application in computing, big data, smart city applications, mobile charging applications, Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security, environmental monitoring, Smart retail, Smart supply chain, etc.

VI. CONCLUSIONS

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in several contexts spanning from the professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of ''anytime, anywhere, anymedia, anything" communications. This paper provided a research review about the Internet of Things (IoT). Different aspects of the IoT are discussed in this paper. Work reported in literature is provided and discussed. Architecture and different elements of IoT is explained. Key Features and its applications are also described.

REFERENCES

[1] "Internet of Things: Science Fiction or Business Fact?" . Harvard Business Review. November 2014.

[2] Vermesan Ovidiu, Friess Peter, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, Aalborg, Denmark: River Publishers, 2013.
[3] Santucci Gerald, "The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects", European Commission Community Research and Development Information Service.
[4] Mattern Friedemann, Floerkemeier Christian "From the Internet of Computers to the Internet of Things", ETH Zurich.
[5] Lindner Tim "The Supply Chain: Changing at the Speed of Technology", Connected World, 2015.
[6] Erlich Yaniv "A vision for ubiquitous sequencing", Genome Research, 25 (10), 1411-1416, 2015.
[7] Wigmore I, "Internet of Things (IoT)", TechTarget, 2014.
[8] Noto La Diega Guido, Walden Ian, "Contracting for the 'Internet of Things': Looking into the Nest", Queen Mary School of Law Legal Studies Research, 2016.
[9] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, “Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey”, IEEE Internet of Things journal, Feb. 2018, Vol. 5, pp. 1-27.
[10] W. Na, J. Park, C. Lee, K. Park, J. Kim, and S. Cho, “Energy-Efficient Mobile Charging for Wireless Power Transfer in Internet of Things Networks”, IEEE Internet of Things journal, Feb. 2018, Vol. 5.
[11] J. Jin, J. Gubbi, S. Marusic, M. Palaniswami , “An Information Framework for Creating a Smart City Through Internet of Things”, IEEE Internet of Things journal, April 2014, Vol. 1, pp. 112-121.
[12] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du, J. Wang, K. Long, “Cognitive Internet of Things: A New Paradigm Beyond Connection”, IEEE Internet of Things journal, April 2014, Vol. 1, pp. 129-143.
[13] S. Xia, H. Wu, and M. Jin , “GPS-Free Greedy Routing With Delivery Guarantee and Low Stretch Factor on 2-D and 3-D Surfaces”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 233-243.
[14] Z. Ren, X. Qi, G. Zhou, H. Wang, “Exploiting the Data Sensitivity of Neurometric Fidelity for Optimizing EEG Sensing”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 243-254.
[15] L. Yu, T. Jiang, Y. Cao, Q. Qi, “Carbon-Aware Energy Cost Minimization for Distributed Internet Data Centers in Smart Microgrids”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 255-275.
[16] S. Abdelwahab, B. Hamdaoui, M. Guizani, A. Rayes, “Enabling Smart Cloud Services Through Remote Sensing: An Internet of Everything Enabler”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 276-288.
[17] M. S. Khan, M. S. Islam, H. Deng, “Design of a Reconfigurable RFID Sensing Tag as a Generic Sensing Platform Toward the Future Internet of Things”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 300-310.
[18] Y. Zhang, L. Sun, H. Song, X. Cao, “Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 311-318.
[19] K. Framling, S. Kubler, A. Buda, “Universal Messaging Standards for the IoT From a Lifecycle Management Perspective”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 319-327.
[20] X. Sheng, J. Tang, X. Xiao, G. Xue, “Leveraging GPS-Less Sensing Scheduling for Green Mobile Crowd Sensing”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 328-336.
[21] P.Y. Chen, S.M. Cheng, K.C. Chen, “Information Fusion to Defend Intentional Attack in Internet of Things”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 337-359
[22] B. Kantarci, H. T. Mouftah , “Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things”, IEEE Internet of Things journal, June 2014, Vol. 1, pp. 360-368.
[23] S.C. Lin, C.Y. Wen, W.A. Sethares, “Two-Tier Device-Based Authentication Protocol Against PUEA Attacks for IoT Applications”, IEEE Transactions on Signal and Information Processing over Networks, Vol. 4(1), March 2018.
[24] Shreedhar A Joshi, Srijay Kolvekar, Y. Rahul Raj, Shashank Singh, “IoT Based Smart Energy Meter”, International Journal of Research in Communication Engineering, Vol. 6, 2016.
[25] Gobhinath S, Gunasundari N, Gowthami P, “Internet of Things (IOT) Based Energy Meter”,International Research Journal of Engineering and Technology (IRJET), Vol. 3(4), 2016.
[26] O. Vermesan, P. Friess, P. Guillemin, “Internet of things strategic research roadmap,” Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.
[27] Pe na-L´opez, Itu Internet Report 2005: The Internet of Things, 2005.
[28] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.H. Kuo, D. P. Agrawal, “Choices for interaction with things on Internet and underlying issues,” Ad Hoc Networks, vol. 28, pp. 68-90, 2015.
[29] O. Said, M. Masud, “Towards internet of things: survey and future vision,” International Journal of Computer Networks, vol. 5, no. 1, pp. 1-17, 2013.
[30] Huansheng Ning, Hong Liu, “Cyber-Physical-Social Based Security Architecture for Future Internet of Things”, Advances in Internet of Things**,** Vol.2, No.1, January 14, 2012.
[31] J. Pan, J. McElhannon, “Future Edge Cloud and Edge Computing for Internet of Things Applications”, IEEE Internet of Things Journal, Vol. 5, Issue 1, Feb. 2018.

ISSN: 2454-4248
23 – 27

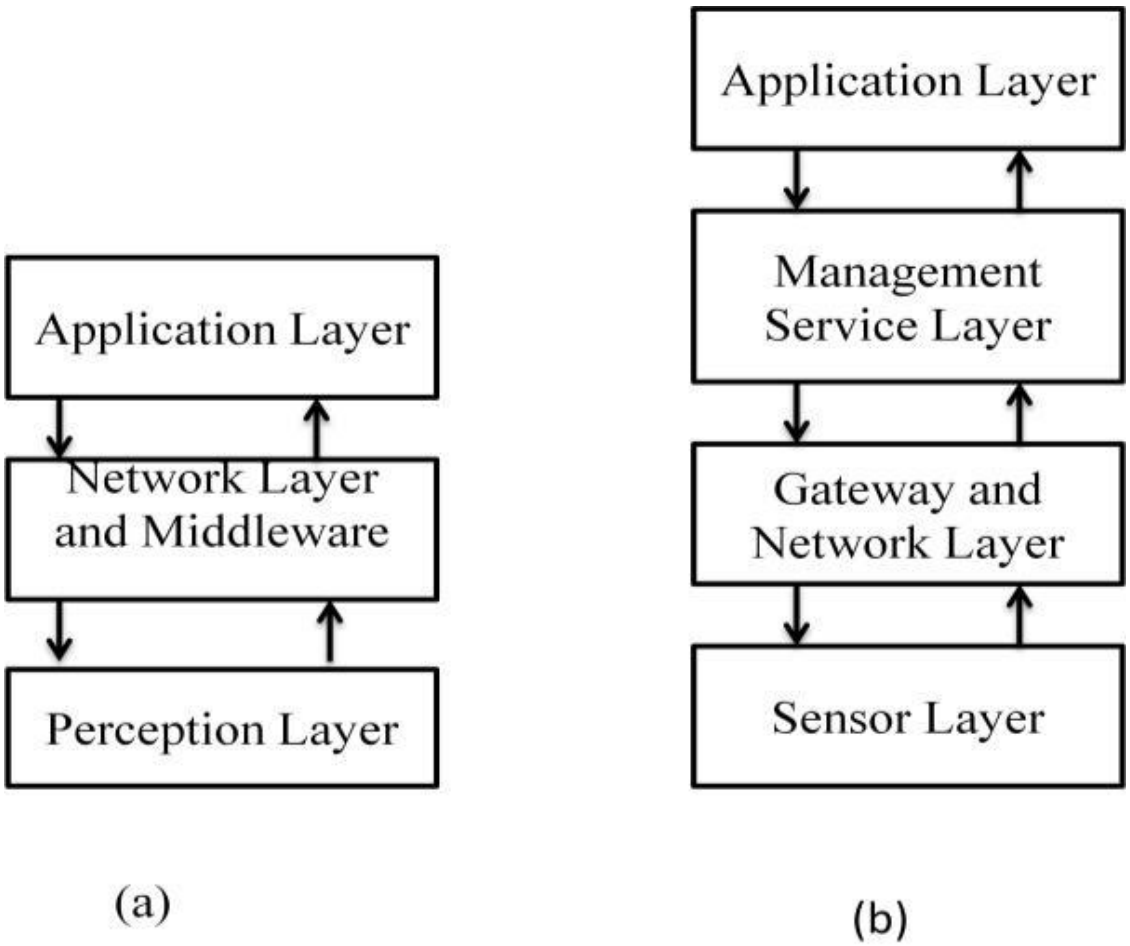

Fig. 1 General 3 Layer/ 4 Layer architecture for IoT

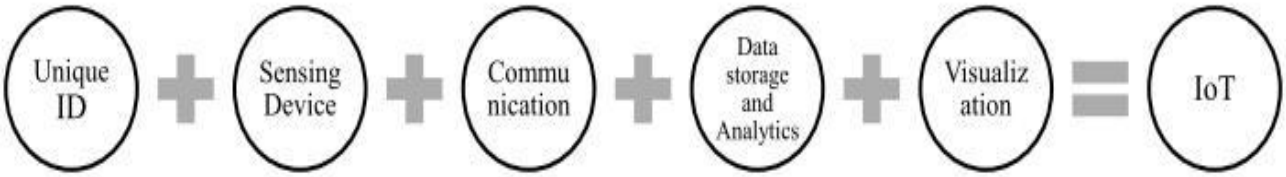

Fig. 2 Essential Key elements of IoT