International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Internet of Things - A Technological Revolution

Vodela Nitya[1], Srinivasa Rao Dhanikonda[2]

[1,2]CSE, GITAM Deemed To Be University

Email: [1]vnitya06@gmail.com, [2]srinivasarao.dhanikonda@gmail.com

Abstract: The term Internet of things coined in the technological era seems to be much more efficient than traditional approaches providing excellent service and ease in life. By introducing IoT, there can be an advancement on a magnanimous scale automating almost everything. IoT is based on real-time data and scenarios that can also be incorporated with the methods of AI and its subcomponents for further improvement. In doing so, the effectiveness of machines along with ease of control increase assisting humans in the everyday schedules of life.

Keywords: AI, Automations, Cloud, Internet of Things, Sensors

1. INTRODUCTION:

Currently, our generation is most abiding to completing tasks with the click of a button which was almost deemed impossible to be invented, however, IoT has proved the theory to be true by doing just that. People can switch lights at home on/off with voice, or hand claps/snaps or even by just being present in the room, which substitutes the need of switches connected to a complex combination of electrical wiring around the house and this example is just one of the many inventions of IoT.

This will be the future of our generation and will most likely be led by the automation industry. IoT or Internet of things is based on data and information collected from any device connected to the internet and containing sensors that help accumulate data easily . To further elucidate this concept, take smartwatches as the best example; this little device worn on hands can provide us with extensive information including but not limited to the surroundings or anything miles away; can attend calls without having to take and hold the phone, moreover it is possible to also use the very basic necessities used in the phone like calculator, calendar and the internet. These devices send information via the internet.

The Internet of things comprises everything learnt in the present and utilizes most of the technological advancements made to help develop the future generations. When understanding in terms of sensors, an example of the self-driving car can best explain it, where the semi-automated car can drive the passenger based on the sensors present which detects the traffic around it as well as various other factors, for example. weather to help regulate the temperature inside the car to maintain proper weather conditions for the person inside or a self driving car, which includes all the mentioned features with an addition of being able to travel without having to actually drive it. Self-driving cars like tesla which can be navigated through an application.

A brief history lesson about the invention of IoT. Since IoT is completely revolving around the concept of communication between 2 or more mediums, furthermore this concept has existed among humans for centuries, this term was first introduced in the year 1985 by Peter T. Lewis during his speech, however, was later revised as the "Internet for Things" by Kevin Ashton in the year 1999. This term got better recognition from the year 2010 and onwards with the ever-growing application of its technology.

2. APPLICATIONS:

In the early 1980s, this concept's first device was developed to know the count of coke bottles present in a vending machine present at Carnegie Mellon University. This went on to be applied in the development of mobiles and sim cards, this helped people connect quicker and furthermore. The latest development is currently the age of 5G Technology that connects innumerable devices.

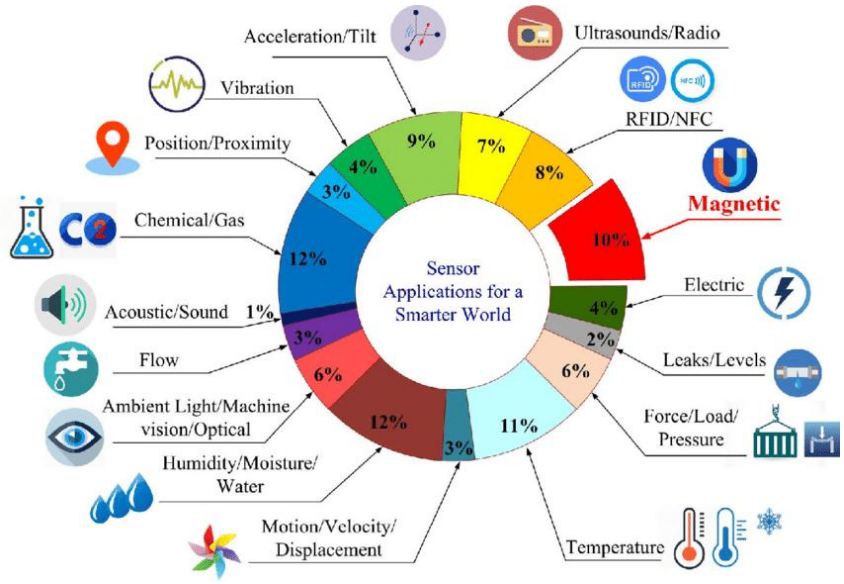

Fig. 1 Displays every application involved in the field of IoT

Most of the evergreen industries have been in constant labor and in constraint with respect to the labour done, which led to the need of automation in order to help reduce workload on humans and help us work smarter compared to the previous centuries.

IoT is hence applicable in every distinct sector, for it mainly works on the internet. The most important sectors currently in this era are the :

1. Healthcare - Chemical, Medical, Nursing, Pharmaceutical
2. Technology - Agriculture, Bio, Computer, Information,
3. Supply & Retail - Businesses : small or organisational
4. Commerce - Economy & Finance
5. Industrial - Building, factories, Mining

These are the ones that are the only deterministic factors for everyday life presently and these would not have been developed and advanced as much as it is currently if it weren't for IoT.

This in-turn helps create a sustainable environment and is advanced enough for this generation with many more inventions to come.

3. WORKING:

The working of IoT can be easily explained as it is applied in the terms of the following main concepts:

- Sensor Devices: i.e devices embedded with sensors for detecting and collecting data
- Internet Connectivity: internet to collect/transfer data
- Gateways: devices connecting the sensor devices with cloud using internet
- Data Processing: input data is processed for outputs
- User Interfaces: user is notified of any missing or upgraded components for their iot device

Fig. 2 An Overview of the working of IoT

When the sensor devices collect data (of any format or size), it is then uploaded to the cloud, however it depends on how much data the cloud can store in a timeframe. This data is transmitted with the use of the internet through gateways and is processed once received.

The next stage, Data Processing, is the involvement of Artificial Intelligence and its subconcepts: Machine Learning, Deep learning, and Data science that are highly involved in working. With the help of AI can the processing task be completed efficiently with accurate results that can be used as data references. Predictions can be implemented too so as to achieve a preventive measure incase of any defaults.

And finally user interfaces hold the highest role in this to help visualise and provide input or feedback which can also create more probabilities to a situation.

4. LITERATURE SURVEY

Researchers have incorporated the field of blockchain with IoT as done by H. Liu et al. [6] who developed a blockchain framework utilizing Hyperledger Fabric along with ABAC named “Fabric-IoT”,which targets the issue of restricted access control in the field of IoT, achieving dynamic access control while overcoming drawbacks in hyperledger fabric. Similarly, a survey done by A. A. Sadawi et al. [1] discusses the effects of blockchain-IoT and highlights which

blockchain-IoT integrated methods help in conquering the challenges faced in that field and proposed a 3 layered architecture comprising of devices, dew and cloudlet that assist in integration of Blockchain-IoT and handle the traffic and security of the integration..

IoT has also seen experiments conducted with 5G networks as done by A. M. Escolar et al. [2] who proposed a 5G Network Slicing framework in IoT using *Automated Scenario Deployment Script* (ASDS) for their experimental deployment and results. A survey conducted by L. Chettri et al. [12] mentioned various applications of IoT in the 5G world comprising of the wireless technologies present like the Augmented Reality, 5G-NR and heterogeneous networks (HetNets), as well as the security and controls involved in low-power wide-area networks (LPWANs) in terms of 5G IoT.

Some authors have reviewed the role of IoT in the healthcare system as referenced by K. M. Besher et al. [11] proposed an encryption-decryption framework that protects the patient data collected via sensors in matrix form, encrypted by generating 2 keys: key 1 with a unique id of the patient and key 2 with ASCII/Binary which is then uploaded to cloud. This is decrypted by the receivers using the inverse of the 2 keys generated to retrieve the original patient data. This helps protect patient data from being misused. H. K. Bharadwaj et al. [5] used Machine Learning with IoT to detect various diseases and serious health complications with algorithms like DT, ANN,KNN, reinforcement learning to analyse and diagnose the data and prevent security attacks on the same. Use of automation helps accurately analyse the data. F. Alshehri et al. [4] surveyed various topics in healthcare involving IoT which are IoMT, cloud, security, medical signals.

J. Wang et al. [10] experimented with security issues faced in IoT by implementing IoT-Praetor based on Device Usage Description(DUD) which detects and understands the behaviors of various devices, sensors, communications evaluating their model with the help of Samsung SmartThings.

5. CONCLUSION & FUTURE WORK

IoT will continue to be serviceable in every aspect of the future generation, become a part of our daily life, and further enhance our future while incorporating the emerging implementation techniques like AI and Big Data. This concept being an emerging industry will be a flourishing sector in terms of effectiveness, employability, security, knowledge gained, and development with only a positive change and increase in its products and services.

6. REFERENCES

[1] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," in IEEE Access, vol. 9, pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[2] A. M. Escolar, J. M. Alcaraz-Calero, P. Salva-Garcia, J. B. Bernabe and Q. Wang, "Adaptive Network Slicing in Multi-Tenant 5G IoT Networks," in IEEE Access, vol. 9, pp. 14048-14069, 2021, doi: 10.1109/ACCESS.2021.3051940.

[3] C. Xie, B. Yu, Z. Zeng, Y. Yang and Q. Liu, "Multilayer Internet-of-Things Middleware Based on Knowledge Graph," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2635-2648, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3019707.

[4] F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," in IEEE Access, vol. 9, pp. 3660-3678, 2021, doi: 10.1109/ACCESS.2020.3047960.
[5] H. K. Bharadwaj et al., "A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications," in IEEE Access, vol. 9, pp. 38859-38890, 2021, doi: 10.1109/ACCESS.2021.3059858.
[6] H. Liu, D. Han and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," in IEEE Access, vol. 8, pp. 18207-18218, 2020, doi: 10.1109/ACCESS.2020.2968492.
[7] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.
[8] J. Hwang, A. Aziz, N. Sung, A. Ahmad, F. Le Gall and J. Song, "AUTOCON-IoT: Automated and Scalable Online Conformance Testing for IoT Applications," in IEEE Access, vol. 8, pp. 43111-43121, 2020, doi: 10.1109/ACCESS.2020.2976718.
[9] J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021, doi: 10.1109/ACCESS.2021.3063671.
[10] J. Wang et al., "IoT-Praetor: Undesired Behaviors Detection for IoT Devices," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 927-940, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3010023.
[11] K. M. Besher, Z. Subah and M. Z. Ali, "IoT Sensor Initiated Healthcare Data Security," in IEEE Sensors Journal, vol. 21, no. 10, pp. 11977-11982, 15 May15, 2021, doi: 10.1109/JSEN.2020.3013634.
[12] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.
[13] M. G. Samaila, J. B. F. Sequeiros, T. Simões, M. M. Freire and P. R. M. Inácio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," in IEEE Access, vol. 8, pp. 16462-16494, 2020, doi: 10.1109/ACCESS.2020.2965925.
[14] M. Savic et al., "Deep Learning Anomaly Detection for Cellular IoT With Applications in Smart Logistics," in IEEE Access, vol. 9, pp. 59406-59419, 2021, doi: 10.1109/ACCESS.2021.3072916.
[15] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.
[16] N. Mazhar, R. Salleh, M. Zeeshan and M. M. Hameed, "Role of Device Identification and Manufacturer Usage Description in IoT Security: A Survey," in IEEE Access, vol. 9, pp. 41757-41786, 2021, doi: 10.1109/ACCESS.2021.3065123.
[17] O. Said, Z. Al-Makhadmeh and A. Tolba, "EMS: An Energy Management Scheme for Green IoT Environments," in IEEE Access, vol. 8, pp. 44983-44998, 2020, doi: 10.1109/ACCESS.2020.2976641.
[18] R. K. Lenka, A. K. Rath and S. Sharma, "Building Reliable Routing Infrastructure for Green IoT Network," in IEEE Access, vol. 7, pp. 129892-129909, 2019, doi: 10.1109/ACCESS.2019.2939883.

[19] S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," in IEEE Access, vol. 8, pp. 188082-188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[20] Y. Li et al., "Toward Location-Enabled IoT (LE-IoT): IoT Positioning Techniques, Error Sources, and Error Mitigation," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4035-4062, 15 March15, 2021, doi: 10.1109/JIOT.2020.3019199.