International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

IoT Challenges and Future Directions

Tarun Kumar R P
PG Scholar, Department of MCA, Dayananda Sagar College Of Engineering, Bangalore.
Dr. Smitha Rajagopal
Assistant Professor, Department of MCA, Dayananda Sagar College Of Engineering, Bangalore.

Abstract:
The development potential for the enterprises in the modern era is huge as they invest in diverse technologies. Internet of Things is a leading technology that has immense growth opportunities. It is predicted that 41.6 billion IoT devices will be operational in 2025. Typically, with the Internet of Things (IoT) expanding at large, there are numerous technical challenges that are encountered. Given the ongoing advancements in the IoT sector, it is quite obvious that IoT may penetrate all the sectors like finance, healthcare, agriculture, smart wearables, to name a few. The IoT has a potential to introduce a major revolution amongst the various sectors. This paper presents an overview on the IoT advancements and discusses the Future applications and investigation Challenges.

Keywords- Internet of Things, IoT Applications , future technologies, IoT Challenges, IoT Future.

Introduction:
The term of Internet of Things (IoT) was first coined in 1999 by Kevin Ashton that refers to huge amount of data being gathered from numerous devices or objects [1]. In reality, all the devices around us are related with the web and accordingly the correspondence to each other with insignificant human mediation. A definitive point is to make a superior world for people, where the articles around us figure out our craving and subsequently act likewise with next to no unequivocal instructions.
The new speedy progression of the Internet of Things (IoT) and its ability to offer different sorts of organizations have made it towards development [2]. With the enormous effective on the public activities and business operations, Internet of Things (IoT) devices are rapidly becoming widespread while IoT organizations are ending up being inevitable [3]. Since there is a continuous usage of IoT devices, they are prone to assaults. Given a plethora of countries dependent on IoT, any cyber-attacks executed on the IoT devices may create a havoc [4]. The cyber-attacks on the IoT devices are increasing constantly. The IoT is being viewed as the next significant paradigm. It is worthwhile to mention that in the context of IOT, if a single node is compromised, then the entire network would be seriously affected leading to a substantial damage [5].

Architecture of IOT:
IoT not just has a similar security issue as sensor organizations, versatile interchanges organizations and the Internet, yet in addition has its claims to fame, protection issues, different validation and access control network design issues, data capacity and the board, etc. Information and security insurance is one of the technical difficulties of IoT [6]. RFID frameworks, WSNs sensors see for the finish of the data innovation, which safeguard the trustworthiness and secrecy of data by the secret phrase encryption innovation in the IoT. Types of layers are. Presentation layer, Transport layer, Application layer. **Presentation layer:** It is the data beginning and the centre layer of IoT. A broad range of the data of the actual world utilized in IoT are seen and gathered in this layer, by the advancements of sensors, remote sensors organization (WSN), labels and peruse scholars, RFID framework, camera, worldwide position framework (GPS), clever terminals, electronic

information interface (EDI), objects, thus like. **Transport layer:** including access organization and centre organization, gives straightforward information transmission capacity. This layer gives a productive, solid, confided in network framework stage to upper layer and enormous scope industry application. **Application layer:** Consolidates data the leader's sub-layer and application organization sub-layer. The data the board sub-layer gives dealing with complex data and uncertain information, for instance, revamping, cleaning, and combining, and gives record organization, market to publicize organization, office the leaders, geomatics, etc. by organization arranged designing, conveyed processing advancements, and so on [7]

Applications:

1. **Health.**

The IoT is utilized in medical services area to work on the nature of human existence by helping fundamental assignments that people should perform through application. IoT has different applications in medical services, which are from remote observing hardware to progress and shrewd sensors to gear coordination. The information assembled by these sensors is made open on the Internet to trained professionals, family members and other very familiar people to additionally foster treatment and responsiveness. With the utilization of sensors and the innovation expressed above we can follow the individual 's internal heat level, heartbeat rate, pulse, and so forth. In case of emergency, the individual and their own PCP will be educated with each one concerning the data assembled by the sensors. IoT in medical benefits conveys new devices revived with the latest advancement in the natural framework that assistants in developing better clinical consideration. This framework will be exceptionally valuable to senior residents and debilitated individuals who live autonomously. IoT helps in reforming medical care and gives pocket-accommodating answers for the patient and medical services proficient.[8][9]

2. **Smart Agriculture.**

The IoT can support and redesign the agriculture region through checking out at soil moistness and by virtue of grape manors, noticing the capacity compartment width. A different sensor can recognize data, perform data taking care of and enlighten the farmer through correspondence structure such as, mobile phone text about the land parcel that need explicit thought. IoT would permit to control and save the amount of nutrients tracked down in rural items, and direct microclimate conditions to take advantage of the creation of vegetables and foods grown from the ground quality. Smart agriculture will help agronomists with having better understanding of the plant improvement models and to have compelling making practices by having the data shoreward conditions and climate alterability. This will according to a general viewpoint extend the agrarian reasonability by avoiding the off-track making conditions.[10][11]

3. **Smart Environment.**

A basic utilization of IoT is perceiving corrupting and normal disasters. Associations connected by the IoT point of view in unbelievable city climate could goes from Monitoring thriving structure, Management of waste, Monitoring air quality, Monitoring disturbance, Traffic blockage, sharp ending, smart lightning, water quality checking, disastrous event seeing, shrewd creating and some more. Remembering of far-off obvious gadgets and IoT movements for normal security and other green applications are one of the best encouraging business region fragments from here on out. An essential IoT application is seeing Air Pollution: By implanting sensors which collects setting data like extent of carbon monoxide, nitrogen dioxide in the air, sound levels, temperature, dampness levels in the climate. Climatic conditions observing: barometrical circumstances checking, for instance, wind speed, temperature, abruptness,

tension, and Earthquake Early Detection, Water Quality: track the presence of waste and stunning planned substances into the streams and sea for diminishing water contamination, can correspondingly stay aware of water being obliged drinking.[12][13]

4. **Smart City.**

Smart City is another noteworthy utilization of IoT delivering interest among all out people. It is a city where data innovation is the vital framework and the reason for offering fundamental types of assistance to inhabitants. IoT will tackle serious issues looked by individuals living in city like contamination, gridlock, and deficiency of energy supplies and so on. There are numerous innovative stages included, including yet not restricted to computerized sensor organizations and server farms. By presenting sensors and the using web applications, occupants can find free open halting spaces across the city. Similarly, the sensors can perceive meter modifying issues, general errors, and any foundation issues in the power framework.[14][15]

5. **Smart homes.**

Smart Home has turned into the progressive stepping stool of outcome in the private spaces, and it is anticipated Smart homes will become as normal as cell phones. A few shrewd home arrangements likewise centre around helping old Hand gloves, Fingerings, Wristwatch/Bands, Eyes-Glasses, Legs-Socks, Foot-Shoes, Helmet, Cloth, and so on. Different electronic devices for example, lights, fans microwaves, fridges, radiators and forced air systems are implanted with sensors and actuators to use the energy adequately, screen and control measure of warming, cooling and level of light, ,room light sense the presence of people and turn on when you enter , when fire or smoke recognized at home, remote smoke and carbon monoxide sensors sound cautions and furthermore alert by telephone or email and adds more solace throughout everyday life, which thus limit the expense and increments energy saving. The IoT can be utilized to control and program the apparatuses in your home from a distance. It tends to be valuable in identifying and keeping away from burglaries.[16][17]

IoT – Platform:

As in IoT, all the IoT gadgets are associated with other IoT gadgets and application to send and get data utilizing conventions.

1. **Amazon Web Services (AWS) IoT platform.**

Amazon Web Service IoT stage offers a bunch of administrations that associate with a few gadgets and keep up with the security too. This stage gathers information from associated gadgets and performs constant activities.[17]

2. **Microsoft Azure IoT platform.**

Microsoft Azure IoT stage major areas of strength for offers component, adaptability and simple mix with frameworks. It utilizes standard conventions that help bi-directional correspondence between associated gadgets and stage. Purplish blue IoT stage has an Azure Stream Analytics that processes a lot of data continuously produced by sensors.[17]

3. **Google Cloud Platform IoT.**

Google Cloud Platform is a worldwide cloud stage that gives an answer for IoT gadgets and applications. It handles a lot of information utilizing Cloud IoT Core by associating different gadgets. It permits to apply BigQuery investigation or to apply Machine learning on this information. [17]

4. **IBM Watson IoT platform.**

The IBM Watson IoT stage empowers the designer to convey the application and building IoT arrangements rapidly.[17]

Challenges:

1. **High-jacking Your IoT Devices.**

Ransomware doesn't hamper your delicate records but it blocks induction to them by means of

encryption. By then, the programmer who penetrated the device will demand an instalment cost for the unscrambling key opening of the records. The cases of IoT devices being damaged with0ransomware are exceptional, but the thought is quickly transforming into an example in obscurity cap hacking world. In light of everything, wearable application advancement, clinical consideration gadgets, sagacious homes, and other sharp contraptions and-conditions might be in peril later on.[19]

2. Sensing and Monitoring.

Whether headways worried about checking and recognizing have gained massive headway, they are reliably developing especially zeroing in on the energy ampleness and basic point of view. Sensors and names are ordinarily expected to be dynamic perseveringly to acquire fluttering information which makes this perspective significant for energy ability, particularly in lifetime development. All the while, new advances in nanotechnology and biotechnology and cutting back have permitted the improvement of actuators and sensors in regards to the Nano scale.[20]

3. Data and data Management.

Planning, dismantling and utilizing the snippets of data made by immense volumes of IoT information in a supportive and significant ways is pursuing for standard foundations. The sheer size of the information gathered will require refined assessments that can channel, investigate and pass on respect from information. As additional contraptions enter the market, more information storerooms are framed, making a jumbled relationship of connection between isolated information sources. The setback of expansive standards and shows will make it broadly harder for relationship to dispose of information storehouses.[21]

4. Complexity, disarray, and combination issues.

With different stages and giant measures of APIs, IoT frameworks blend and testing will be a test no inquiry. The disarray around pushing rules is essentially certain to slow assembling. The speedy progress of APIs will probably consume unforeseen improvement assets that will diminish project packs 'capacities to add concentrate new support. Even more drowsy assembling and frightening improvement asset necessities will probably slip plans and slow an open door to profit, which will require extra supporting for IoT tries and longer runways for new associations. [22]

5. Encryption Capabilities.

Information encryption and unscrambling is a constant cycle. IoT organization's sensors come up short on ability-to-process. The savage power endeavours can be forestalled by firewalls and isolating the gadgets into discrete networks.[23]

6. Privacy and Security.

Privacy and Security Owing to the way that IoT has transformed into a basic part as regards the destiny of the web with its extensive use, it requires a need to address Security and trust limits adequately. Furthermore, the supporting of IoT is laid on the ongoing distant sensor affiliations, IoT as such compositionally gains a for all intents and purposes indistinguishable affirmation and security issues WSN has. Various attacks and inadequacies on IoT frameworks0demonstrate that there are to be certain a necessity for wide running security plans which will safeguard data and plans starting with one completion then onto the next. Many pursues generally exploit deficiencies in unambiguous contraptions as such getting entry into their structures and in this way making secure devices vulnerable. This security opening further spikes comprehensive security outlines that contain assessment that is useful in applied cryptography for data and system security, non-cryptographic security frameworks as well as designs that assist engineers with considering safe structures on devices that are heterogeneous. [24][25]

IoT Future:

1. Consumers.

can get more private item or administration offers, in view of what they really do or where they are. They can travel more productively by keeping away from gridlocks when their associated

vehicle proposes an elective course, considering traffic detailed by different vehicles. They can set aside cash by decreasing energy use or by paying lower vehicle insurance instalments in view of checked safe driving practices. They can be better, more secure, and more autonomous because of wearable gadgets that give criticism on wellbeing or that screen the old in the home.[21]

2. Organizations.

They can safeguard structures by means of far-off security; secure resources like vehicles and apparatus with area trackers and remote locking gadgets; and guarantee that touchy items are reliably put away in right circumstances. They can turn out to be more effective, as on account of utilities utilizing savvy meters to take out waste or misfortune, or on account of hardware merchants giving in the nick of time preventive maintenance. Ranchers can be more valuable with splendid water framework that gives water precisely where and when required. New plans of action considering selling ultimate results as opposed to simply0hardware might support business revenues.[21]

3. States and public specialists.

can likewise profit from the IoT. For instance, wellbeing and long-haul care expenses can be decreased with better remote help for the old in their own homes. Street wellbeing can be worked on considering information from large number of drivers. The proficiency of road lighting can be improved by darkening lights on void streets [2]. As legislatures work to convey quality administrations in progressively complex conditions, gadgets that have previously started to make life simpler and more effective for organizations and purchasers can likewise assist with making more noteworthy public worth.

Conclusion:

The advance of computational articles and things have been furnished with correspondence and normal restrictions of implanted data. This progress persuades toward the impetus improvement of the IoT field. Close to the rising IoT point of view, an in general solid union will present everything and anything by trim virtual linkage of made and addressable contraptions. Henceforward, the result will help clients with making novel answers for be serious areas of strength for basic for a strong head movement to from one side of the world to the next. Reasonably, the instances of IoT space have been broke down in this paper in the point of view of various evaluation regions, for example, plan, information the board, information making due, correspondence, security and affirmation. Essentially, this paper gives plan and clear evaluation of the basic significance of IoT plan point of view. At last, we have dissected the focal IoT stray pieces near by the execution inconveniences and future course of its necessities.[21]

References:

1. Birkel, Hendrik Sebastian, and Evi Hartmann. "Impact of IoT challenges and risks for SCM." *Supply Chain Management: An International Journal* (2019).
2. Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." *Applied Sciences* 10, no. 12 (2020): 4102.
3. Saleem, Jibran, Mohammad Hammoudeh, Umar Raza, Bamidele Adebisi, and Ruth Ande. "IoT standardisation: Challenges, perspectives and solution." In *Proceedings of the 2nd international conference on future networks and distributed systems*, pp. 1-9. 2018.
4. Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International Journal of Critical Infrastructure Protection* 25 (2019): 36-49.
5. Reddy, G. Nikhita, and G. J. Reddy. "A study of cyber security challenges and its emerging trends on latest

technologies." *arXiv preprint arXiv:1402.1842* (2014).
6. Peña-López, Ismael. "ITU Internet report 2005: the internet of things." (2005).
7. Jia, Xiaolin, Quanyuan Feng, Taihua Fan, and Quanshui Lei. "RFID technology and its applications in Internet of Things (IoT)." In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, pp. 1282-1285. IEEE, 2012.
8. Saini, Mohit Kumar, and Rakesh Kumar Saini. "Internet of Things (IoT) Applications and Security Challenges: A Review." *network* 6: 7.
9. Soumyalatha, Shruti G. Hegde. "Study of IoT: understanding IoT architecture, applications, issues and challenges." In *1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications*, no. 478. 2016.
10. Sundareswaran, V. "MS null, "Survey on Smart Agriculture Using IoT,"." *International Journal of Innovative Research in Engineering & Management (IJIREM)* 5, no. 2 (2018): 62-66.
11. Attia, Tarek M. "Challenges and opportunities in the future applications of IoT technology." (2019).
12. Acharjya, D. P., M. Kalaiselvi Geetha, and Sugata Sanyal, eds. "Internet of Things: novel advances and envisioned applications." (2017).
13. Rajguru, Shagufta, Swati Kinhekar, and Sandhya Pati. "Analysis of internet of things in a smart environment." *International Journal of Enhanced Research in Management & Computer Applications* 4, no. 4 (2015): 40-43.
14. Zanella, Andrea, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. "Internet of things for smart cities." *IEEE Internet of Things journal* 1, no. 1 (2014): 22-32.
15. Abomhara, Mohamed, and Geir M. Køien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." *Journal of Cyber Security and Mobility* (2015): 65-88.
16. Whitmore, Andrew, Anurag Agarwal, and Li Da Xu. "The Internet of Things—A survey of topics and trends." *Information systems frontiers* 17, no. 2 (2015): 261-274.
17. Javatpoint" https://www.javatpoint.com/iot-platformJavatpoint".
18. Perera, Charith, Chi Harold Liu, and Srimal Jayawardena. "The emerging internet of things marketplace from an industrial perspective: A survey." *IEEE transactions on emerging topics in computing* 3, no. 4 (2015): 585-598.
19. Ashish Chauhan:"7 Biggest Security Challenges of IoT & Their Solutions".
20. Hussein, AbdelRahman H. "Internet of things (IOT): Research challenges and future applications." *International Journal of Advanced Computer Science and Applications* 10, no. 6 (2019): 77-82.
21. Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660.
22. Pundir, Yogita, Nancy Sharma, and Yaduvir Singh. "Internet of things (IoT): Challenges and future directions." *International Journal of Advanced Research in Computer and Communication Engineering* 5, no. 3 (2016): 960-964.
23. Saini, Mohit Kumar, and Rakesh Kumar Saini. "Internet of Things (IoT) Applications and Security Challenges: A Review." *network* 6: 7.

24. M. Miraz, Mahdi H., Maaruf Ali, and S. Peter. "Excell, and Richard Picking,"." *Internet of Nano-things, Things and Everything: Future Growth Trends,"(to be published) Future Internet* (2018).

25. Daia, Ahmed S. Abu, Rabie A. Ramadan, Magda B. Fayek, and AETiC AETiC. "Sensor networks attacks classifications and mitigation." *Annals of Emerging Technologies in Computing (AETiC), Print ISSN* (2018): 2516-0281