International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 08 | Aug - 2021 ISSN: 2582-3930

Research Challenges in Internet of Things and Future Applications: A Survey

Rajesh Patel , Department of Computer Engineering
Gujarat Power Engineering and Research Institute

Abstract- The Internet of Things (IoT) is a revolutionary technological advancement that will allow users to connect to an endless number of gadgets at all times and from any location. It is a network of physical items such as machinery, automobiles, and appliances that use sensors and Application Programming Interfaces to exchange data via the Internet (APIs). It's critical to understand the numerous potential domains for IoT applications, as well as the research problems that come with them. IoT is projected to infiltrate practically every facet of daily life, from smart cities to health care, smart agriculture, logistics and retail, and even smart living and smart ecosystems. IoT is an important research issue for studies in numerous related domains such as information technology and computer science because it is so broad and influences nearly every aspect of our life. This paper covers a detailed survey of challenges in the internet of things and future applications.

Keywords—Internet of Things; IoT applications; IoT challenges; future technologies; smart cities; smart environment; smart agriculture; smart living

I. INTRODUCTION

The Internet of Things (IoT) is a hot issue with significant technical, social, and economic implications. Consumer items, durable goods, automobiles and trucks, industrial and utility components, sensors, and other ordinary objects are being integrated with Internet connectivity and powerful data analysis capabilities to alter the way we work, live, and play. Furthermore, pervasive network configurations are being designed in which all feasible devices (mainly heterogeneous) link to detect, gather, and analyze data of various types to act on the intelligence derived from deep insights into the data.

The majority of these actions are carried out without the involvement of humans [1]. According to industry analysts, there are presently more than eight billion such devices connected to the network, with the number expected to rise to more than 25 billion by 2020. The core of its architecture is to connect the physical and virtual worlds, as well as to assist businesses in managing device security and connection while gathering data from computers, connecting them to backend systems, developing IoT applications, and protecting interoperability. With all of this in mind, the Internet of Things (IoT) is predicted to continue to grow in terms of the number of devices and functions it can support. This is evidenced by the vagueness in the term "Things," which makes defining the IoT's ever-expanding boundaries difficult [2].

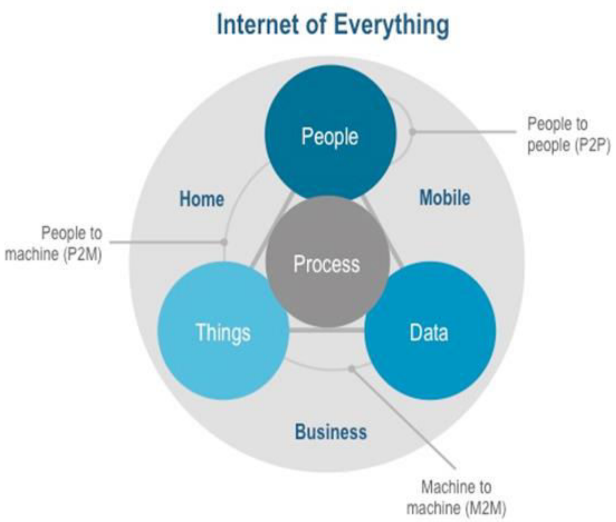

Fig.- 1: Internet of Things (IoT) elements

Internet of things (IoT) provides a communication platform supporting person to person (P2P), Machine to Machine (M2M), and Person to Machine (P2M) interactions. The communication in the IoT applications will normally constitute the connections as seen in Fig. 1

The structure of this paper is going to be as the following: Section I introduced an overview of IoT technology In section II, we explore domains of potential IoT applications In section III, we explore various challenges and opportunities of IoT systems such as security and privacy, M2M communication and communication protocol, Sensor energy, etc. Finally, we make some concluding remarks in section IV.

II. DOMAINS OF POTENTIAL IOT APPLICATION

Manufacturing or Industrial settings are the most common (22%) of the 1,414 public corporate IoT projects found, followed by Transportation/Mobility (15 %) and Energy IoT projects, according to the 2020 review of the top IoT application categories (14%)[13]. The following domains of potential IoT applications are given below.

A. Smart Home

Smart Home comes out as the most popular Internet of Things application across all media. Every month, more than 60,000 people look for the term "smart home." There are 256 firms and startups in the IoT Analytics Smart Home company database. Smart homes have the most companies involved than any other IoT application. The total amount of money invested in smart home businesses now surpasses $2.5 billion. This list contains well-known startups like Nest and AlertMe, as well as large firms like Philips, Haier, and Belkin.

B. Smart City

The term "smart city" refers to a wide range of applications, including traffic control, water distribution, waste management, security, and environmental monitoring. Its appeal is bolstered by the fact that many Smart City solutions claim to ease real-world problems faced by city dwellers today. Smart City IoT technologies help to alleviate traffic congestion, reduce noise and pollution, and make cities safer.

C. Connected Health (Digital Health/Telehealth/Telemedicine)

Many countries' healthcare systems are inefficient, slow, and prone to mistakes. This is easily changeable because the healthcare industry relies on a variety of activities and technologies that may be automated and improved through technology. Additional technology that can facilitate activities such as report sharing to different individuals and places, record keeping, and medicine delivery would go a long way toward altering the healthcare industry [3].

D. Smart Agriculture and Water Management

According to [4], the Internet of Things has the potential to boost and expand the agriculture sector by monitoring soil moisture and, in the case of vines, the trunk diameter. IoT would enable for better control and preservation of vitamin content in agricultural products, as well as regulation of microclimate conditions to maximize vegetable and fruit production and quality. Furthermore, examining meteorological conditions enables forecasting of ice information, drought, wind changes, rain, or snow, allowing temperature and humidity levels to be controlled, preventing fungus and other microbial pollutants. The industrial internet of things (IIoT) is a term that refers to interconnected sensors, instruments, and other devices that are networked with industrial applications on computers, such as manufacturing and energy management. Data gathering, exchange, and analysis are all possible with this connectivity, which could lead to increased production and efficiency, as well as other economic benefits [5]. The IIoT is an evolution of a distributed control system (DCS) that uses cloud computing to enhance and optimize process controls, allowing for a higher degree of automation.

F. Retail and Logistics

There are numerous advantages to implementing IoT in supply chain or retail management. Some examples include monitoring storage conditions across the supply chain, product tracking for traceability purposes, and payment processing in public transportation, theme parks, and gyms, among others. Inside the retail environment, IoT can be used for a variety of applications, including guiding customers through the store based on a pre-selected list, automating payment processes such as automatic check-out with biometrics, detecting potential allergen products, and controlling product rotation on shelves and warehouses to automate restocking procedures [6].

III. RESEARCH CHALLENGES AND IMPEDIMENTS

Despite the growth of numerous IoT applications these days, it is still in its early stages, and as a result, several obstacles and limitations exist, as detailed below.

A. Security and Privacy

Because IoT has become a critical component of the internet's future with its rising usage, it demands the necessity to appropriately address security and trust functions. Researchers are aware of the flaws that many IoT devices now have. Furthermore, because IoT is built on top of existing wireless sensor networks (WSN), it inherits the same privacy and security concerns as WSN does [7, 8]. IoT is one of the most vulnerable technologies, according to cyber security experts, who foresee more focused assaults on existing and developing infrastructures, such as data theft, physical injury, DDoS attacks, and ransomware for smart homes or smart cars. the capacity to operate on IoT devices with limited resources This would allow a variety of experienced users to safely use and install IoT systems, even though practically all IoT devices have insufficient user interfaces. Additional areas such as communication secrecy, trustworthiness, and authenticity of communication parties, message integrity, and supplemental safety criteria should be included in addition to the protection and security components of the IoT.

B. M2M (Machine to Machine) Communication and Communication Protocols

While IoT communication protocols such as Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) already exist, there is currently no standard for an open IoT. Although all objects require connectivity, they do not all need to be internet-ready because they simply need to be able to send and receive data through a specific gateway. Device communication protocols are the driving force behind IoT applications, and they serve as the primary conduit for data flow between sensors and physical objects or the outside world. The transport layer's key goals include ensuring end-to-end reliability as well as providing end-to-end congestion control. Most protocols are unable to provide adequate end-to-end reliability in this regard [9].

C. Sensor Energy

IoT deployment success depends on providing reliable power to the sensors for an extended length of time [10]. This is especially concerning when these sensors are used in remote and far-flung locales such beneath the ground, in the sea, in space, or on other planets. The energy demand must be kept to a minimum, and the supply must be sourced from the environment. Because replacing the batteries in billions of these devices is impractical, the Adoption of the Narrow Band Internet of Things (NB-IoT) idea to construct a Low Power Wide Area Network is one technology that can help with this (LPWAN). The deployment of IoT devices has also benefited from the usage of Bluetooth Low Energy (BLE) transceivers.

D. Architectural Limitations

The adoption and feasibility of the Internet of Things place numerous technological demands on the current Internet infrastructure. When IoT devices were effectively implemented over the current Internet infrastructure, several of these shortcomings were highlighted, such as weak security, interoperability issues, and communication across the many physical interfaces of the IoT devices. It would be significantly easier to reuse technologies from existing protocols rather than create a new one.

E. Interoperability

Because the primary requirement in Internet connectivity mandates that “connected” systems can “speak the same language” in terms of encodings and protocols, interoperability has always been and continues to be a core essential ideal. Currently, several standards are used to support diverse industries' applications. Because of the huge amounts and varieties of data, as well as heterogeneous devices, adopting standard interfaces in such disparate entities is critical, and much more so for applications that support cross-organizational collaboration, as well as a variety of system restrictions. As a result, IoT systems are being developed to manage increasingly greater levels of interoperability [11].

F. Massive Scalability

The number of sensor nodes in use around the world could be in the tens of billions or even higher. Massive scaling is a significant difficulty that has an impact on routing technologies. After IoT is launched, scalability refers to the growing number of devices and networks. As a result, any routing method must be appropriate and scalable for such a large number of sensor nodes [11]. The authors of [12] proposed a novel integration approach for named data networks and pub/subsystems. To meet these issues, concepts from cloud infrastructure and services can be considered.

G. Ethical Concerns

IoT devices are predicted to pervade every aspect of our socio-technical environment, including not only Smart City deployment, but also invasively into our bodies for complete healthcare. This, of course, presents a slew of ethical questions that must be addressed in order to assuage public concern. To safeguard patient confidentiality, eavesdropping on medically sensitive data must be avoided. Also, to protect lives, hacking protection must be assured, which would have particularly severe effects for medical monitoring and equipment maintenance. Employee redundancy and, as a result, possibly enormous job losses are a risk of any automation of manual labour.

H. Big Data

One of the most noticeable elements of IoT is the vast amount of data collected and aggregated by smart objects. Techniques to transform this data into usable information will need to be developed. Data doubles in size every two years, with 44 Zettabytes predicted in the next four years [14]. Various Big Data solutions provide globally connected devices with valuable and real-time data. There are numerous issues with bigdata management and storage, data visualization, and integrity.The device guarantees that no data will be leaked or pirated. Data assembly methods must work in tandem with standard systems and commands on a scale and condition of integrity.

I. Intelligence and Context Awareness in the IoT

“Any information related to the user's interaction with the service, where both the user and the application's environment are of particular interest” [15]. Due to the variety of sources from which context information is collected, context awareness is a complicated process.

Context-aware computer systems have been a significant research challenge for at least 20 years [16], and will become even more so with the Internet of Things, which will include intelligent processors that will monitor our personal health and fitness and control traffic in our cities, affecting personal, business, and community life in m Context-aware computer services are software applications that can operate in a dynamic environment and can run anytime, anywhere, and on any device with little or no user interaction. Context-aware services, on the other hand, employ data from a range of sources, including sensors, repositories, and users.

J. Automatic Discovery of Resources

Because of the enormous variety of IoT items and devices, an uniform standard for resource discovery must be developed. This IoT application-specific protocol, on the other hand, cannot be a simple SIP tweak (session initiation protocol).

Different value-added services can be established to aid in the automatic discovery of resources and to assist the IoT end user. These services can comprise semantics and data identification services, automatic configuration management, device registration/deregistration, service advertising, and device semantic integration, in addition to the standard IoT daily functions. IoT devices must be discoverable and allow themselves to be discovered inside the IoT ecosystem, with full reciprocal sharing of device capability information, for this process to be a complete success.

Prioritization of devices is also required, meaning a ranking of IoT objects along the IoT network chain. This refers to how far and wide an IoT must be detectable in order for the network to notice its presence at first. The discovery procedure can be event-based, one-time only, publisher-subscriber, and indicate if the device is a home or IIoT device. Low-power radio networks can connect IoT devices, but they often suffer from high degrees of attenuation, interference, multi-path effects, and distortion since they use shared electromagnetic spectrum. This frequently results in connection loss and, as a result, several attempts to rejoin during a session

IV. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

To that goal, tremendous progress has been made in IoT technology for a variety of applications that make use of enabling and emerging technologies. IoT application areas are highly diverse, allowing it to serve a variety of users with a variety of needs. Individuals, society or communities, and institutions are three types of users who benefit from technology. Many firms who are involved in IoT in various scenarios still lack a sustainable business model for their IoT applications because IoT is still in its infancy. Till today many challenges and research directions exist in the field of IoT which are explored in this survey paper and given below as a conclusion.

Protocol standardization is essential for the international agreement on the protocol used at the application layer. Need to increase the capabilities of sensors in IoT. A resource allocation method must be agreed upon as IoT Os. There is a requirement for the smooth integration of IoT with the pervasive computing ecosystem. Establishing a reliable network architecture is the job of IoT network Architects. IoT-related components of fog computing are being developed. Human needs for employment, privacy, and accurate information are all ethical requirements. The necessity for an IoT device discovery protocol is outlined in the IoT Discovery Protocol. IoT devices can be found using the Shodan search engine. The identity management mechanism is required for the IoT ID Protocol IoT Power is critical to reduce the amount of energy consumed by IoT devices and to use energy harvesting to power them.

V. REFERENCES

[1] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, “Towards green computing for Internet of Things: Energy oriented path and message scheduling approach,” Sustainable Cities and Society, vol. 38, pp. 195 – 204, 2018.

[2] E. Borgia, D. G. Gomes, B. Lagesse, R. Lea, and D. Puccinelli, “Special issue on Internet of Things: Research Challenges and Solutions" Computer Communications, vol. 89, no. 90, pp. 1–4, 2016.

[3] Mano, Y., Faical B. S., Nakamura L., Gomes, P. G. Libralon, R. Meneguete, G. Filho etc “Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition”. Computer Communications, 89.90, (178-190) 2015, DOI:10.1016/j.comcom.2016.03.010

[4] V. Sundareswaran and M. S. null, "Survey on Smart Agriculture Using IoT," International Journal of Innovative Research in Engineering & Management (IJIREM), vol. 5, no. 2, pp. 62–66, 2018.

[5] Boyes, Hugh; Hallaq, Bil; Cunningham, Joe; Watson, Tim "The industrial internet of things (IIoT): An analysis framework". Computers in Industry. 101: 1–12, October 2018.

[6] P. Tadejko, "Application of Internet of Things in logistics-current challenges," Ekonomia i Zarz{a˛} dzanie, vol. 7, no. 4, pp. 54–64, (2015).

[7] M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Future Internet, vol. 10, no. 8, pp. 68, 2018, DOI: 10.3390/fi10080068

[8] Z. Alansari, N. B. Anuar, A. Kamsin, M. R. Belgaum, J. Alshaer, S. Soomro, and M. H. Miraz, "Internet of Things: Infrastructure, Architecture, Security and Privacy", in 2018 International Conference on Computing, Electronics Communications Engineering (iCCECE), pp. 150–155, Aug 2018, DOI:10.1109/iCCECOME.2018.8658516.

[9] D. B. Ansari, A.-U. Rehman, and R. Ali, "Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP," International Journal of Computer Applications, vol. 179, pp. 9–14, March 2018.

[10] Evans, D. "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything; White Paper 2011; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/Io_IBSG_0411FINAL.pdf (accessed on 27 July 2018).

[11] L. Farhan, A. E. Alissa, S. T. Shukur, M. Hammoudeh, and R. Kharel, "An energy-efficient long hop (LH) first scheduling algorithm for scalable Internet of Things (IoT) networks," in Proc. IEEE 11th International Conference on Sensing Technology, Sydney, Nov 2017.

[12] S. Han and H. Woo, "NDN-based Pub/Subsystem for scalable IoT cloud," in Proc. IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg, Dec 2016, pp. 488- 491.

[13] [Online] https://iot-analytics.com/

[14] L. Farhan, A. E. Alissa, S. T. Shukur, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in Proc. IEEE 11th International Conference on Sensing Technology, Sydney, Nov 2017

[15] Achilleos, A. Yang, K. Georgalas, N. "Context modelling and a context-aware framework for pervasive service creation: A model-driven approach." Pervasive Mob. Comput. 2010, 6, 281–296. [CrossRef]

[16] Hong, J.-Y. Suh, E.-H.; Kim, S.-J. Context-aware systems: A literature review and classification. Expert Syst. Appl. 2009, 36, 8509–8522. [CrossRef]