DOI: https://doi.org/10.46632/daai/2/6/6

Data Analytics and Artificial Intelligence

Vol: 2(6), 2022

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

World of IOT and Its Challenges

Ramji Rajbhar

University of Mumbai, India

*Corresponding Author's mail id: ramji.mit21018@sstcollege.edu.in

Abstract: The Internet of Things (IoT), a new paradigm, has transformed traditional living into a high-tech lifestyle. Smart cities, smart homes, pollution control, energy conservation, smart transportation, and smart industries are among the changes brought about by IoT. Many significant research projects and investigations have been undertaken in order to advance technology through IoT. To fully realise the promise of IoT, numerous obstacles and problems must be overcome. These challenges and problems must be considered from a variety of IoT perspectives, including applications, challenges, enabling technologies, social and environmental implications, and so on. The primary goal of this review article is to provide a thorough discussion from both a technological and a sociological standpoint. The article investigates the Internet of Things' various challenges, critical problems, architecture, and significant application domains. The paper also discusses existing literature and how it contributes to various IoT elements. Furthermore, the significance of big data and its analysis in relation to IoT has been discussed. This page will help readers and researchers understand the Internet of Things and how it applies in real life. Because of the massive number of wireless devices, such as smartphones and the Internet of Things (IoT), and the recent exponential growth in mobile traffic, the wireless network industry has produced and amassed an unprecedented amount of data. According to the International Data Corporation, there will be around 42 billion Internet-connected devices by 2025, with 80 zeta bytes of data created during the same year. There is no question that a new age is dawning as IoT and Artificial Intelligence (AI) grow more prevalent in society, and when 5G technology is implemented, new ideas in all industries will be inspired. We are creating a hyper-connected world in which gadgets are employed for more than simply data transmission and are gradually becoming intelligent and aware of their surroundings as a result of IoT ecosystem innovation. Because of advances in sensing, data processing, cloud, and communication technologies, the systems can interact with the environment and optimise operations by learning via interactions. As a consequence, intelligent settings and self-aware, linked "things" will be developed for applications in health, mobility, the digital society, food, energy, and the environment.

1. INTRODUCTION

The Internet of Things (IoT) is a new paradigm that allows electrical devices and sensors to connect with one another through the internet in order to make our lives simpler. IoT leverages the internet and smart devices to provide innovative solutions to challenges encountered by corporations, governments, and both the public and private sectors throughout the world. IoT is becoming increasingly important in our daily lives. IoT as a whole is a technical innovation that includes a wide range of smart systems, frameworks, intelligent devices, and sensors. It employs quantum and nanotechnology to attain previously inconceivable levels of storage, sensing, and processing speed.

2. ARCHITECTURE & APPLICATION OF IOT

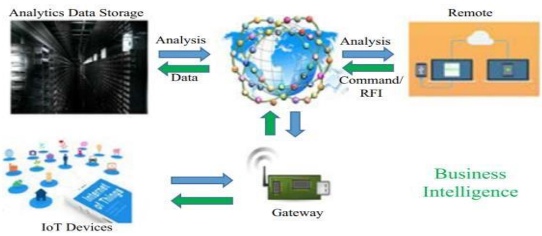

FIGURE 1. Generic Architecture of IoT

To demonstrate the potential effectiveness and applicability of IoT changes, extensive research studies have been conducted and are available in the form of scholarly articles, and press reports, both on the internet and in the form of printed materials. It could be used as a pre-work before creating original, inventive company concepts while taking security, assurance, and interoperability into consideration. Our everyday routines have undergone a significant alteration as a result of the growing use of IoT technologies and gadgets. The idea of smart home systems (SHS) and appliances, which include internet-connected appliances, home automation systems, and reliable energy management systems, is one such IoT advancement. In addition, the Smart Health Sensing system is another significant IoT accomplishment (SHSS). Small intelligent equipment and devices are incorporated into SHSS to support human health. These gadgets can be used both indoors and outside to examine and monitor various health conditions, one's level of fitness, or the number of calories expended at a gym, among other things. Additionally, it is utilised to keep track of acute medical conditions in hospitals and trauma centres. Thus, by enabling it with cutting-edge technology and other innovations, it has completely altered the medical industry's landscape. Additionally, IoT developers and academics are actively working to improve the quality of life for seniors and individuals with disabilities. IoT has dramatically improved in this field and given such people's daily lives a new direction. The majority of people are using these tools and equipment because they were developed at a very low cost and are readily available within a reasonable price range. They can live a regular life as a result of IoT. Transportation is another significant component of our lives. IoT has led to some fresh developments that have improved its effectiveness, comfort, and dependability. At numerous signalised junctions across major cities, intelligent sensors and drone gadgets are now in charge of managing the flow of traffic. Additionally, new cars are coming off the assembly line with sensors pre-installed that can detect impending large traffic jams on a map and propose an alternate route with less congestion. IoT can therefore be very useful in many areas of life and technology. We can conclude that IoT has a lot of potential for improving technology and helping humanity. IoT has additionally demonstrated its significance and promise in a growing region's industrial and economic progress. Additionally, it is regarded as a groundbreaking move in the trade and stock market. However, data and information security is a crucial concern and highly desirable, making it a very difficult problem to solve. The Internet, which is the main source of security risks and cyber-attacks, has provided hackers with a variety of entry points, making data and information less safe. IoT is committed to providing the greatest solutions for handling data and information security challenges, nevertheless. Security is therefore the main IoT worry in business and the economy. IoT developers are working hard to build a secure channel for collaboration between social networks and privacy issues because this is a big topic in the industry.

The Internet of Things (IoT) has a multidisciplinary vision to help many fields, including the environment, industry, public and private sector, healthcare, transportation, etc. Regarding particular areas of interest and issues, different scholars have provided varying explanations of the IoT. IoT's potential and strength are seen in a number of application sectors.

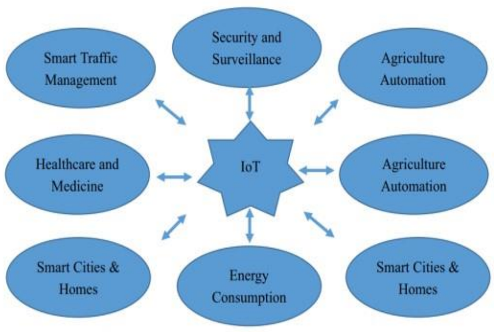

FIGURE 2. Potential Application Domains of IoT

One of the popular IoT use cases that include smart homes is the smart city. The IoT-enabled home appliances, HVAC systems, TV, audio/video streaming devices, and security systems that make up a smart home all communicate with one another to offer the highest levels of comfort, security, and energy efficiency. Through an IoT-based central control system that uses the Internet, all of this communication is conducted. Weber argued that IoT developers need to consider the geographical constraints of the various nations in order to establish global security and privacy challenges. To accommodate the diverse needs for privacy and security around the world, a general framework must be created. Before creating an IoT framework, it is very advised to look into and understand the problems and difficulties with privacy and security. A security flaw in IP-based IoT systems was discovered by researchers. They claimed that the internet serves as the foundation for all device connectivity in an IoT system. Security concerns in IP-based IoT systems are therefore a major issue. Additionally, the capabilities and life cycle of every IoT system object should be taken into account while designing the security architecture. It also incorporates the use of security standards and a trusted third party. It is also desired to have a security architecture that can grow to accommodate both small- and large-scale IoT objects.

FIGURE 3. Potential Application Areas of Smart City

Another challenge in IoT that requires promising solutions to improve security is authentication and access management. A method for handling access control and authentication was proposed by researchers. To stop the loss of sensitive information, it is crucial to authenticate the people interacting. Additionally, they offered an Elliptic Curve Cryptosystembased authentication scheme and tested it against various security risks, such as eavesdropping, man-in-the-middle attacks, key control attacks, and replay attacks. One of the key sectors around the world is Agriculture. Numerous variables, including geographic and biological ones, affect agriculture. According to researchers, the technology being utilised to manage ecosystems is inexperienced and has a low IQ. They said that IoT researchers and developers would find this to be a useful application area. An intelligent monitoring platform framework based on the Internet of Things that has four-layer mechanisms to control the farm ecosystem is required. Together, the framework's layers each of which is in charge of a certain task can produce a better environment with less human interference. Climate change brought on by global warming is a significant issue on a worldwide scale. In order to create an efficient environmental monitoring and control system, researchers developed an integrated information system (IIS) that combines IoT, geo-informatics, cloud computing, a global positioning system (GPS), geographical information system (GIS), and e-science. They claimed that better data collecting, analysis, and decision-making for climate control are provided by the suggested IIS. Another significant issue facing the world now is air pollution. There are numerous technologies and methods for controlling and measuring air quality. Researchers presented the cloud-based air quality and monitoring system called Air Cloud. Utilizing five months' worth of data over the course of two continuous months, they implemented Air Cloud and assessed its performance.

IoT architecture and technologies All of the functionality of IoT systems are defined by the five key layers that make up the IoT architecture. These layers include the business layer, the network layer, the middleware layer, and the application layer. The perception layer, which comprises physical devices like sensors, RFID chips, barcodes, and other physical items connected to an IoT network, is at the base of the IoT architecture. Information is gathered by these devices and sent to the network layer. The information is transmitted from the perception layer to the information processing system using the network layer as a transmission medium. This information transmission may employ any wired or wireless technology, including 3G/4G, Wi-Fi, Bluetooth, and others. The middleware layer is the layer below that. This layer's primary responsibility is to process the data obtained from the network layer and make judgments in light of the outcomes of ubiquitous computing. The application layer uses this processed data after that for worldwide device management. A business layer that controls the complete Internet of Things system, its applications, and services is present on top of the architecture. The business layer further uses this knowledge to develop future goals and objectives by visualising the data and analytics it receives from the application layer. IoT architectures can also be changed in accordance with requirements and application domains. In addition to a layered foundation, an IoT system is made up of a number of functional building blocks that support different IoT functions such as sensing mechanisms, authentication and identification, control, and management.

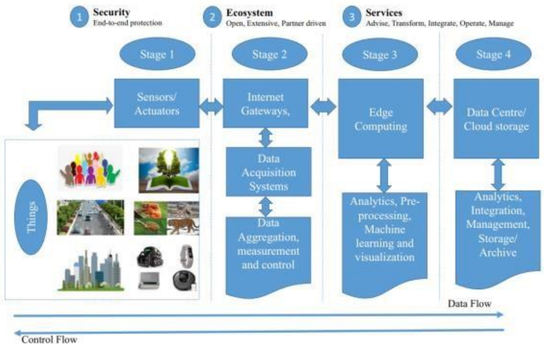

FIGURE 4. Four Stages of IoT to Deal with Massive Amount of Data

Sensors and actuators are critical components of Stage-1 of the design. The real world consists of the environment, people, animals, electrical devices, intelligent cars, and buildings, among other things. These real-world creatures send signals and data, which sensors pick up and translate into information that can be analysed. Additionally, actuators have the power to alter reality, such as regulating a room's temperature, reducing a car's speed, dimming a light, etc. Stage 2 is in charge of working with gateways, data-collecting systems, sensors, and actuators. The enormous amount of data produced in stage 1 is gathered and optimised in this stage in an organised manner that is ready for processing. Stage-3 edge computing technology works with enormous amounts of data and offers a number of features, including visualisation, integrating data from other sources, machine learning technique analysis, etc. Stage 4 includes a number of crucial tasks like in-depth processing and analysis as well as giving feedback to enhance the precision and accuracy of the overall system. At this point, the data centre or cloud server will be used for everything. To manage this massive stream of streaming data, big data frameworks like Hadoop and Spark may be used. Machine learning techniques may be used to create better prediction models, which may aid in the development of a more accurate and dependable IoT system to meet the demands of the present.

3. CHALLENGES IN THE WORLD OF IOT

The primary design considerations for an effective IoT architecture in a heterogeneous context include scalability, modularity, interoperability, and openness. In order to meet the demands of crossdomain interactions, multisystem integration with the possibility for easy and scalable administration features, big data analytics and storage, and userfriendly applications, the IoT architecture must be designed with these goals in mind. Additionally, the architecture must allow for the scalability of functionality as well as the addition of automation and intelligence among the IoT components of the system. Additionally, a new difficulty is the growing volume of huge data being produced by the connectivity between IoT sensors and devices.

4. SCALABILITY

Scalability in IoT systems has raised questions due to the enormous number of devices that need connectivity simultaneously. There are primarily two types of scalability concerns in the IoT: horizontal scalability, which refers to the addition or removal of an IoT node, and vertical scalability, which refers to the addition or removal of computing resources of an IoT node.

5. SECURITY AND PRIVACY

Wireless IoT implementation confronts greater difficulties in these areas than traditional IoT deployment due to the absence of privacy standards and end-toend security solutions. From both a hardware and software perspective, several technologies try to address privacy and security concerns.

6. SELF-ORGANIZATION

Due to the expansion of IoT nodes, there is a constant paradigm change from the Internet of Things to the Internet of Everything, which necessitates new strategies for autonomic administration to make the network proactive rather than reactive. The primary goal of selforganization in the Internet of Things (IoT) systems is to actively react to changing environments in an automatic and coordinated manner. To do this, one or more control loops are used, and they periodically reconfigure the system's behaviour to keep it within predetermined bounds.

7. ENERGY EFFICIENCY

Creating energy-efficient routing protocols *(a)* to minimise the number of hops, improving communication link status, implementing wake-sleep techniques based on network traffic, and regulating network topology is all part of designing energy-efficient IoT networks. *(b)* Implementing load-balancing techniques while also integrating renewable energy devices into the network. *(c)* Utilizing wireless charging technologies to address the core problem of power management, particularly for massive heterogeneous IoT networks

8. IOT AND SENSOR NETWORKS

Road and Transportation: Roadway wireless sensor networks (WSM) enable highly reliable timely signal control, accurate traffic prediction, and road environment monitoring.

Buildings: Future smart buildings (SB) will serve as outstanding instances of cyber-physical systems, which link and integrate the real and virtual worlds. The pinnacle of big data is SBs.

Healthcare Future healthcare systems will undoubtedly depend on a variety of technologies, including communication, sensing, cloud computing, and data analytics. To actualize an end-to-end system from the perspective of communication, both short-range and long-range communication technologies are required.

Education and Training: The education and training sectors have a tremendous opportunity to combine the data gathered from IoT nodes with other data sources, such as user mobility and data analytics, to enable new services and experiences.

9. CHALLENGES IN SENSOR NETWORKS

In the Internet of Things and wireless sensor networks, sensing is a key component. Sensing data is typically delivered through an IoT network for postanalysis and inference to gain insights. The precision of the sensors is essential for the value of the post-processing inference. For the purposes of this agreement, ISO standard 5725:1994 divides accuracy into precision and trueness while highlighting a sensor's integrity. Contrarily, RF sensing uses channel state information for sensing and, because it is inherently EM, uses machine learning to classify sensed data. It also brings additional issues, including linearity, repeatability, resolution, hysteresis, temperature coefficients, stability, and calibration.

10. CONCLUSION AND OUTLOOK

Every day, new technologies and applications are developed, yet there are still issues and holes that need to be filled. We have discussed significant issues, such as scalability, self-organization, security, and energy efficiency that must be taken into account when deploying this emerging technology for the benefit of our society in this editorial article. We have also outlined a few key challenges in IoT and sensing technologies. The development of sensing technologies will also open the door for successful IoT solutions and, as discussed in this article, will spur innovation in a variety of industries, including transportation, healthcare, buildings, supply chains, education, and many other facets of our everyday lives. By standardising architectures, cross-sector application designs, device interoperability, privacy and end-to-end security, highly effective multi-standard communication systems and sensors, as well as cutting-edge device charging mechanisms, the divide between the physical and digital worlds will inevitably be closed and new opportunities for growth will arise. Future IoT applications and human-machine interaction will take on a new dimension thanks to the combination of tactile internet and ultraresponsive, ultra-reliable low-latency communication made possible by 5G systems. This will also accelerate the development of fog computing and mobile edge computing architecture. If we want the digital and physical worlds to coexist, there are many hyper-connected entities in this developing ecosystem, including robots, organisations, algorithms, and humans. These interactions must be effectively controlled through well-defined policies and regulations.

REFERENCES

[1]. Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. 2. Gatsis K, Pappas GJ. Wireless control for the IoT: power spectrum and security challenges.
[2]. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges.
[3]. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things.
[4]. Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures.
[5]. Gaona-Garcia P, Montenegro-Marin CE, Prieto JD, Nieto YV. Analysis of security mechanisms based on clusters IoT environments.

[6]. Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. Sustainability. IoT application areas. https://iotanalytics.com/top-10-iot-project-application-areasq3-2016

[7]. Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities.

[8]. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. A review on internet of things for intelligent energy control in buildings for smart city applications. Internet of Things http://www.ti.com/technologies/internet-ofthings/overview.html.

[9]. Liu T, Yuan R, Chang H. Research on the internet of things in the automotive industry.

[10]. Alavi AH, Jiao P, Buttlar WG, Lajnef N. Internet of things-enabled smart cities: state-of-theart and future trends.

[11]. Weber RH. Internet of things-new security and privacy challenges.

[12]. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP based internet of things.

[13]. M. A., Murad, S., et al. (2017). "A survey on internet of things enabled smart campus applications,"

[14]. Imran, M., et al.(2017). The role of big data analytics in internet of things.

[15]. Kuusik, A., and Le Moullec,Y. (2018). A Survey on the roles of communication technologies in IoTbased personalized healthcare applications.

[16]. Al-Kabi, M. N. (2020). "A survey of internet of things (IoT) in education: opportunities and challenges," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. Studies in Computational Intelligence,*

[17]. Ang, K. L., Seng, J. K. P., and Zungeru, A. M. (2018). Optimizing energy consumption for big data collection in largescale wireless sensor networks with mobile collectors.

