

IoT Technology Stack for Future Generations

Pasupuleti Sailaja, Dr. P. Lalitha Surya Kumari¹
{sailajamail@yahoo.com¹}

Research Scholar, Koneru Lakshmaiah Education Foundation, Hyderabad -500075¹, Professor,
Koneru Lakshmaiah Education Foundation, Hyderabad – 500075

Abstract. As IoT is playing a very important role in different aspects of human lives, the Internet of Things (IoT) will have a deep social, commercial and economical impact on human lives. As increasing in the huge number of connected devices, increasing the data storage and heterogeneous environment, it is necessary that addressing and considering of common problems and challenges in the IoT technology stack. This paper is about the research on IoT technology stack related most common provocations and concerns. In this paper, also provided that many reviews of the various proposed approaches which are dealing with the IoT related challenges and IoT on Cloud related challenges and issues. A systematic review about the attack vectors, possible issues, security challenges in terms of IoT on network is provided. This leads to different challenges or issues that are related to security, standardization, scalability, network, etc. are discussed in this paper. Also provided the proposed methodologies which can benefit for avoiding or reducing the challenges or issues in the technology stack of IoT for future generations.

Keywords: Business Process, Challenges, Cloud, Framework, IoT, Issues, Machine Learning, Model, Network, Security, Server, Service..

1 Introduction

Today, in worldwide IoT Technology is among top 5 technologies according to Gartner's Chart. It means that it's highly used in different sectors with different roles. IoT can be considered as a distributed network and interconnected of embedded system communicating through wired or wireless communication technologies. The associated devices that are smart phones, actuators, sensors, computers, smart buildings, home/work appliances, vehicles and roads infrastructure related items and any another physical devices or an objects which can monitor, actuate or connect. The device can connect to the internet, furthermore with every other through network access of heterogeneous. IoT can be defining as global computing technology network in this each will connect to the internet. Because of it's benefits such as accuracy, speed, etc., the associated objects number will raise every day. In future i.e., going forward, they will be having major concerns about infrastructure, models of business, security and also trade standards, while finishing IT networking and computing systems. It's additionally defined such as networking of the physical things or objects empowered along with limitations of storage, communication and computations capabilities moreover embedded along with the electronics like the sensor and the actuator, network connectivity and software that enabling the objects for collecting data and processing, also exchanging data. This IoT technology supplies a promising opportunities to construct powerful industrial applications and systems (Figure 1). In case of business context, the IoT called as IIoT (Industry Internet

of Thing). The IIoT had become amongst the industrial trade concepts in continuing few years. This IIoT can be define as an additional support to an IoT within the industrial sectors which allowing the industries to enhance their efficiency and trust worthiness in their processes. Moreover, it is allowing the industries to improve their operations and transactions with the help of the sensors, which can raise up optimizing production, work and for avoiding systems failures [11].

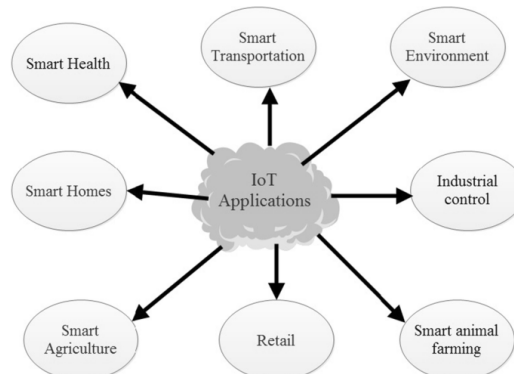


Figure 1: IoT for Industries and Applications

As per IoT records, one of the fastest growth rate is IoT technology in the field of computing technologies. According to the statistics, there're in 2020 over 30 billion connected physical objects around the world. As specified by estimations of the billion global internet connected users and over three times of the global population of the devices associated with each other by the period of 2023 year. And in coming days these numbers will be increasing to reach over 75 billion by the period of 2025 year. The connected IoT objects are spreading in diverse areas with the aim of enhancing the people's regular lives. IoT related things can be referring to objects which are from human regular life, that are ranging from the household items with smartness like smarter adapter, smarter bulb, smarter refrigerator, smarter meter, smarter oven, temperature sensors, AC, smarter smoke detectors and IP cameras and many advanced items. The advanced devices are the RFID (Radio Frequency Identification) devices, accelerometers, heartbeat detectors, sensor for parking and many another sensors in the vehicles etc. The IoT is the implement of existing inter connect facility that to manage each and every which exists in future or exists in world. IoT things having their simulated dispositions and individualities that are functioning using the smart interface in the smart space and that can connect and link within user context and social environment. The high and ultrahigh speed data that can connect currently from the 2020 year. It was expecting that the fifth generations networking i.e., 5GN [10] and must be amuch faster/smarter. And, it will supply grand Quality of Service (QoS) due to thelesser implementation costs, low latency and the higher the efficiency of processing data. Also, these are the networks can either the pointtopoint (P2P) communications links or the point to multipoint (P2M) communications links. P2M can also called as multicasting, which can address the multiple subscriber. These systems of P2M are usually having their various nodes called as 'Things' and these are according to the services with the glassy of security requirements. The nodes are necessary for inter connectivity and uninterrupted network along with cloud platforms for managing the data storage and sharing. Anyway, the IoT (Internet of Things) in real time usages/applications such as wearable gadgets, smart cities, military, medical, driverless cars and many more includes huge data transmission and processing.

However, the integrated circuits (ICs) can be deploy in the IoT related infrastructure as that have the strong constraints such as cost, size, security and power consumption.

On the top of all these, the Cloud computing technology has grandly matured over last few years. This cloud concept is anything that can host on Internet, which is available for the use, for the provision and composition when needed and these are for the sophisticated services from the providers. There are many cloud related key characteristics and that are ubiquitous access, on-demand service provision, elasticity as well as the resource pooling. As the IoT (Internet of Things) vision has evolved and came to the reality, the IoT involving of several different billions of devices (Figure 2) and that interconnected by 2020 in vast amounts with quick versatile or emerging data that is big data and also numerous services. These services aiming to lead the smart, inclusive society, sustainable and economy. The success rate of the IoT services on cloud [13] can be achieved as per expectations according to more business opportunities/requirements with maintaining the reliability, high-performance as per the association of big data, more efficiency and this is for improving the level of providers, users and all other stakeholders and scalability which can be supported the resources, various requirements [12] of users and data may also be involving in this service provision. All these are the points that can make more merging of the IoT paradigms with Cloud technology.

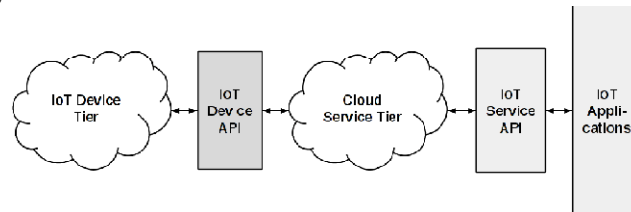


Figure 2: Internet of Things on Cloud

In addition to all above information, the ML (Machine Learning) can also be consider as one of most suitable and useful computational paradigm to provide the embedded intelligence in IoT devices. The Machine Learning can also help smart devices and machines to infer the more useful knowledge from device or human generated data/information. It can be define as ability of smart device to automate or vary the behavior or situation based upon the knowledge that can be consider as essentials part for the IoT solutions. The Machine Learning techniques can be use in the tasks like regressions, classifications and density estimations. The variety of the applications like fraud detection, computer vision, bioinformatics, authentication, malware detection and speech recognitions use machine learning methods and algorithms. In the same way, the machine learning can also be an advantage in the IoT for providing the intelligent services.

2 Related Work

NajlaFattouch, KhouloodBoukadi, Imen Ben Lahmar [1] authors have mentioned that anincredible business managers count that is interesting to integrating the devices of IoT into the Business Processes (BPs) and it known as IoT-aware BP. This type of integration gives an opportunity to business managers for availing from IoT technology into their process from end to end enhancements of their business performances and achievements of their business

specific competitiveness. Hence, many researchers participated for identifying the methods and approaches for integrating IoT technology with BP paradigm. In their paper, authors have presented their review of various proposed methods, which dealing with the integration of an IoT technology with Business Process. Moreover, in their paper, authors have given a rich comparison analysis that based on some group of criteria. Also, authors have identified few challenges and initiatives in IoT-aware Business Process (BP) paradigm. And, they had worked for proposed model that based on IoT-aware BP through BPMN 2.0 extension and through which, authors had aimed to consider few constraints along with other IoT qualities.

Fatima Hussain, Syed Ali Hassan, Rasheed Hussain, Ekram Hossain [2] authors have provided that their extensive efforts to address privacy and security issues which related to IoT networking and this is primarily via traditional cryptographic approach. Anyway, due to unique characteristics of an IoT node extract the solutions, which are existed, and these were insufficient to comprise the whole security within the IoT networking system. In their paper, they were systematically reviewed security attack vectors, requirements and about currently available solutions of security within the IoT networking. Authors have identified the gaps in the solutions of security that invoke DL and ML approaches. At the end, authors discussed details about existing DL and ML solutions that were addressing various problems or issues in security of IoT networking. Authors also discussed about the several future directions of research for the DL and ML based security of IoT. Also authors have given that the machine learning and more about deep learning techniques and DRL methods that can use for enabling IoT device for adapting to the dynamic environments [16]. All the techniques of learning which can be supported operations of self organizing and optimizing overall performances of system by processing and learning the statistical data from an environment i.e., IoT devices and end users. These are the learning methods fundamentally distributing and they don't require the centralizing communications between the controllers and devices. In further, the datasets, which are required for the DL and ML algorithms, are still uncommon, this makes bench- marking efficiency of DL, ML based solutions of security, and this becomes difficult task. In their paper, authors have taken care the ML role and DL role in IoT from privacy and security perspective. Authors had discussed about the privacy and security challenges of IoT, security requirements and attack vectors. They had described the different DL and ML methods of their applications [17] with respective to security in IoT. They have also given the considerations of traditional machine learning approaches. Then they had discussed about solutions of security, which existed and highlighted the challenges, which are open. And, these are for their research directions for future. In their paper, authors have mentioned that the ML methods to the IoT related security and foundation of theory, which related to DRL and DL will necessary to be powerful so that performance of the DRL and DL models can quantify which based on some parameters like complexity of computational, efficiency of learning as well as the strategies for tuning of parameters. Moreover, a new hybrid strategy for learning and the novel data techniques for visualization will be mandatory for efficient and intuitive data interpretation.

Akhilesh Kumar Singh, Vivek Sharma, Manish Raj [3] authors mentioned about the constantly connecting modern world along with devices of computational and actuators for the develop of smart environments. The smart system for an environmental monitoring [18] has systematic sampling which helping in understanding the natural environments such as water, air, land and biota. Actually, an environmental monitoring system is an application of IoT. It is normally depended on the sensors that to help in environment protection through the

monitoring parameters like quality of water, quality of air, etc., And it can also include the area like monitoring wildlife conditions. In their paper, authors have explored an IoT architecture in case of smart environment as well as comparisons between the technologies utilized in the environmental monitoring. It actually, emphasized on different challenges and issues that involved in the smart environment monitoring. The layered framework [14] for smart environment has presented by authors. This paper is an informative to the researchers it suggests effective researches for the domain. In their paper, authors was primarily focused on domain of the smart environments by including its architecture, related challenges and issues. The architecture and security issues knowledge or skill in the smart environment is essential skill for the developers. The comparison between technologies and applications of the smart environment discussed. Their paper also have focused on various challenges and issues, which are necessary to present in the smarter environments. They had performed comparative studies on the smart monitoring with the help of IoT that will help researchers for further improvements or enhancements in their future work about smart environments.

MekalaMS, Viswanathan P [4] authors have given about the rapid growth in industrial infrastructure that creates issues ecologically like climate changes. The prediction accuracy in terms of changes in the weather parameters, field assessments and parameters of soil have become outstanding challenges for IoT in agricultural. They have provided the solution for these problems. As part of this, they proposed (t, n) sensors selections mechanisms and humidity, temperature of soil, water and quality of air measurements that indexing for the node stipulations, which are based upon smarter decisions for making the systems mainly for agricultural fields [19]. This considered temperature parameter, NPK fertilizer regulators models and functions of agronomy. The (t, n) nodes stipulation indexing defined an ideal sensors count for monitoring this field. And the temperature parameter considering the moisture and soil temperatures for assessing rate of the growth. The functions of agronomy based upon the pH level of water and concentrations of SO₂ in the air and this assessing the rate of productions yield in the field. Their framework improved the performances of predictions and detecting the abnormal condition by 75% along with the reductions in unimportant data creation and loss rate of resources. It has increased the agricultural productions yield that was compared to the existing systems.

GayathriNB, Thumbur G, KumarPR, Rahman MZU, Reddy PV [5] have mentioned that the IoT (Internet Of Things) environment contains many number of devices. In fashionable, IoT devices are communicating with every different to change records or connecting to the net via gateway for providing IoT offerings. The most of the IoT devices are participating inside the IoT provider that are lightweight gadgets, wherein the existed cryptographic set of policies can't be applied to provide safety, so a more light-weight safety set of rules have to be implemented. Cryptographic technology to lighten and offer overall performance for IoT environments are currently being studied masses. Especially, it's miles vital for providing efficiency of computations at gateway, a component wherein many of the devices are linked. Moreover, as more gadgets are linking, authentication of data and data integrity ought to be absolutely taken into consideration at the equal time and therefore digitalized signature schemes were proposed. A few of the recent studies about algorithms of signature, the CLS (certificate less signature) primarily depend totally on CL (certificate less public key cryptography) affords overall performance as compared for giving public keys, totally absolutely signatures. Anyway, in the CLS, safety threats, along aside public keys substitute assaults. Also signatures forgery via the nasty KGC (key technology center), also can get up.

In their paper, they have proposed a cutting-edge signature scheme the use of CL in producing and for verifying the signatures messages in IoT environments. Their proposed scheme has combined certificate less arbitrated signatures and gateway aggregate the generated signature messages thru the IoT device institution for reducing the dimensions of the complete signatures. Similarly, it's far implemented for comfortable from the protection threats with the aid of solving the issues due to public keys alternative assaults and nasty KGC and including arbitrate gateway signatures for boosting a non repudiation.

To preserve the integrity of messages transmitted in an increasing number of massive IoT, virtual signatures for messages, service surroundings are required for digital signatures protocol that had studied by authors for long time and many researchers. They have studied for satisfying different security specific requirements even as respecting "light-weight" functionality of IoT environment. Even though studies had performed for applying lightweight signature specific techniques, inclusive of CL to the IoT environments. In this case answers are necessary for the issues of CL dependent schemes. Especially the public keys substitute attacks and nasty KGCs. In this particular, it's far vital to have a look at answers that is satisfying requirements for each protection and performance of computational. Hence, their proposed paper has efficient comfortable CL based scheme.

Their proposed scheme affords the messages integrity that are transmitting in IoT surroundings. And, use of the concepts of arbitrate signatures and an aggregated signatures (AS). The position of AS is for providing performance and this is for arbitrated signatures that are for enhancing the non repudiation by the aggregating arbitrated signatures and it's devices. With this they had designed a relaxed situation in opposition to existing protection threats and with consideration of security gateway, this is intermediate for transmitting records. Their proposed scheme has a design for fulfilling various protection necessities, which includes along with public key substitute assault, nasty KGC assault and leakage of keys. In their present schemes, they had been troubled with leakage of keys and forgeries of the messages and signatures through attacks either with the public keys or nasty KGCs. To resolve this, nonrepudiation become strengthening by applying arbitrated signatures of gateway and it's far feasible for providing efficiency for making use of an AS. The IoT provider may additionally transmit the statistics, consisting of private privateness, depending at the surroundings. Inside the destiny, studies on sensible security technology to provide integrity and confidentiality for the sensitive data need to be carried out.

Dabbakuti JRKK,Ch B [6] authors have mentioned that the IoT (Internet of Things) is continuous growing technology that allowing digital devices for integrating into the network. The usage of IoT technology giving possibilities that are collecting information/data from different GNSS (Global Navigation Satellite System) receivers that are connected to the internet. This is giving unique benefits for obtaining data/information from spatial and temporal distributions. In their article, the iono-spheric monitoring system has implemented with the help of IoT i.e., ThingSpeak. Iono-spheric signals TEC(Total Electronic Content)/delay data from the GNSS stations. KLEF (KoneruLakshmaiah Education Foundation) geographically at 16.44° N, 80.62° E, Port Blair geographically at 11, 43° N, 92,43° E, Bengaluru geographically at 13,02° N, 77,57° E, Lucknow geographically at 26,76° N, 80,88° E and these are used for their analysis in the period of 2015. The iono-spheric signals which are delayed are computed with the help of ThingSpeak and iono-spheric TEC. This is the analysis were performed in MATLAB software directly. Then they compared the

computed and observed TEC values with the International Reference Ionosphere (IRI-16) model values.

Sachin Goswami A, Ketan Patel D, BhargavPadhya P [7] authors have noted that loss of assets and mechanism restricts the implementation of IoT in a full section however in an upcoming time, it is going to be applied in foremost components of society and could significantly change the way of running and living. For this reason it's far important to observe IoT, its programs, structure, boundaries and studies troubles inside the present scenario. Their paper presented the history of IoT, its programs, challenges and essential problems in present context. The contrast of various IoT conversation protocols with their electricity and weaknesses are offered. However, the generation has its own implementation problems and challenges which can be addressed in the paper. They've deliberate future such demanding situations and problems can be addressed and possible answers may be proposed which ultimately makes the IoT structure stable, reliable and secure.

NilupuleeGunathilake A, Rameez Asif, William Buchanan J [8] authors were stated that the main demanding situations diagnosed for the deployed confidentialities, infrastructure and integrities of exchanged facts, authenticity and person private-ness. Hence, nicely securing the powerful algorithms of cryptographic are wished that motive hardware footprints (small) i.e.,LWC (Light Weight Cryptography). In their paper, implementations, demanding situations and futuristic packages of light weight cryptography algorithms for the smart IoT gadgets had mentioned, specially the overall performances of longrange wide vicinity network i.e., LoRaWAN that is an open general that defined communications protocol aboutLPWAN (lowstrength wide place network) generation. LWC is a singular method headed for clever safety packages in low-strength confined statistics-processing devices. Particularly, in IoT programs, provision of excessive-level security is hard (Figure 3) due to their in-constructed low-velocity processors and low memory modules. Consequently, much lighter variations of conventional cryptography or new cryptologic algorithms are researched on to indicate long lasting safety answers. Their paper has covered the necessity of LWC, its modern reputed, well matched technology and protocols, i.e., LoRa WAN, and also demanding situations inside the gift state of affairs by evaluating current theoretical and sensible studies in academia. The overall evaluation shows promising abilities within the path of a hit implementation of LWC and its performance toward 5GN smart cities. Yet, extra theoretical, utility orientated and feasible empirical researches have to be further conducted as a way to reach the final optimization of safety warranty and privacy safety within the IoT international.



Figure 3: IoT Security Challenges

Pooja Yadav, Hemant Yadav, Ankur Mittal [9] authors have furnished the information of their paper that instead of people to people communication, IoT emphasis on gadget to system verbal exchange. Their paper familiarises the fame of IoT growth In India, and additionally consists of protection problems demanding situations. Finally, their paper evaluations the risk component, protection issues and challenges in Indian perspective. sooner or later, the destiny of IoT will become a really worth however massive quantities of data extended its complexity in detection, communications, controller, and in generating consciousness however its increase could be extended daily. Even though IoTs can be predictable that can be incorporated all in one and with ubiquitous. Provider employer required an enclosed group of requirements. Hence, as an sensible systems, progress of IoT can decide with cooperation of the interoperability, skilled, recognition, teamwork, sustainability, privateness, confidentiality, considerations and safety. IoT has turn out to be an anticipated trend of improvement of records enterprise. This will final results in satisfactory of existence. Their paper has their survey about some of most common problems and challenges in IoT w.r.t. Indian perspective. A few feasible improvements that included a facility for dealing with seamless, unified and standardization, customary internet connectivity along with interoperable properties. Power sustainability's, private-ness, and safety are also main points upon which studies may continue by authors. Going forward, improving the challenges, which are effective and ambiguous for the conversation and networking in industrial, business and educational location.

3 Proposed Methodology

IoT Hardware

The IoT can be consider as a distributed network and interconnected of embedded systems that communicating through wired or wireless communication technologies and there are the main three components in IoT Technology.

Network: Any IoT device can communicate to another IoT device (M2M communication) or can talk to servers, which are either located in a local networks or any internet. As it is based upon the network, it will allow every device can benefit of common capabilities for producing and consuming data. Communications are playing an important role in IoT projects. The communication isthe core to whole genre. Hence, there is tradeoff for IoT device. If data rates are higher and the protocols are more complex, then the more powerful processor is necessary. In this scenario, high electrical power of IoT device will be consuming. The protocol TCP/IP is based upon the communications that are Think Web Servers. The HTTP based communications are such as REST server, data stream, UDP protocol also provides the more functionality and flexibility at a reasonable processors price and the power of electricity. A low power Zigbee type, Bluetooth type connections allowing more lower the power of connections according to the corresponding reduction in the functionality and bandwidth. The IoT projects can also be all over world with the requirements for data bandwidth and the communication flexibility. The IoT device contains the full support of TCP/IP and that rated at high. Butit may probably mark down foranother categories like power consumptions.

Sense: Any IoT device can be sensing some other about their environments.

Actuator: Any IoT device can perform something. For example, turn on/off lights, lock doors, turn on/off TV or beep and so on.Currently wide variety of the IoT devices that are in use for miscellaneous requirements. The range of ingenuity function and designs are

expanding at an energetic pace. The combination of devices and their use cases can be present very different analytics challenges and opportunities.

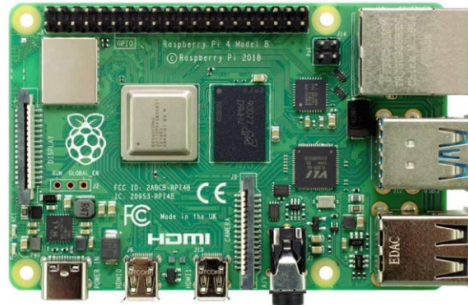


Figure 4: Raspberry Pi

The Raspberry Pi (Figure 4) is the family of a singleboard of computers and this product is from RaspberryPi.org (Raspberry Pi Foundation). This organization had sold more than 9+million of inexpensive and smaller computers. This Raspberry Pi operates numbers of various platform i.e., operating system. The most common operating system is Ubuntu Linux, which has released from Raspbian. Similar to Windows, Ubuntu Linux is an operating system, which can support multitasking. But, Ubuntu Linux is unlike Windows as this is system which can give an option open source. One of the good thing is about the Raspberry Pi is that support of huge number of sensor drivers and devices. This makes this product a best choice for the building IoT related projects. Specifically for the IoT projects, using this as a server. Generally, any low power devices are limiting its usage, Raspberry Pi is not from this category as it is a IoT device. Moreover, this is a great server and great prototyping devices.

There are many various ways of measuring processor power. It includes that the size of processors instructions, processor speed and operating systems, all that are included in the calculations. For many IoT sensors and applications of devices, there is no limit by processor speed as these are all very fast. Here, here is exception to it. In case of using the mechanism of encrypting and decrypting, then these operations mainly expensive in terms of computations. Also these are required a more process power for execute. This tradeoff may also transmits or receives the data very slowly due to requirements of computations for encryptions and decryption methods of the data/information. Hence, higher the processing power that gives the higher ratings will be in the category.

The local storage/media referring to all three main storages that are the EEPROM, RAM and Flash Memory. The Random Access Memory (RAM) is the read and writable memory with high data rate. In general, it is using for stack and data storage while executing of IoT programs. The Electrically Erasable Programmable Read-Only Memory (EEPROM) is using for writing the small amounts of data/information which is related to configurations of the IoT devices and that need to read upon the power supply. The Flash Memory commonly using for programs coding itself. The Flash can read randomly, for example, executable code. Anyway, it can write very slowly in the blocks that are large in size. The Flash is that what code can be written into using the Arduino IDE. The capacity of the local storage that is mainly RAM will add up the cost to the IoT devices. In general, more RAM for prototyping and lesser is the better for deployments as it can reduces the costs.

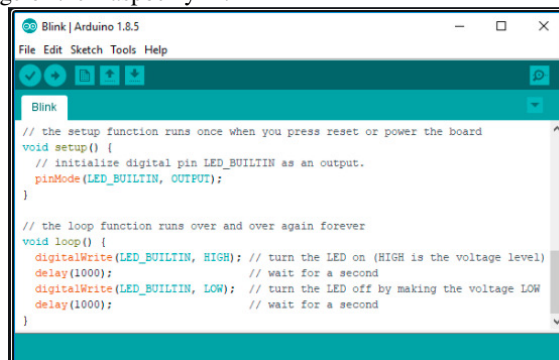
The curse part of every IoT device is the power consumption. In case of not plugging the IoT devices, then that is running off the solar cells or batteries and every single milliwatt unit in the design. The reduction of the power consumption is the complex part. But, some of the points can be considered to reduce the power consumption.

1. By keeping the processor in a sleep mode whenever it is possible.
2. By minimizing the outside communication outside of IoT devices.
3. Trying interrupting driven, but not polling the driven.
4. Scouring the design look for each unnecessary amount of the current.
5. The higher the processing power that gives the higher ratings in the category.

Functionality: This is a kind of catchall category and this is a quite subjective. The example is that, having extra GPIOs (General Purpose Input/Outputs) are available and this is good for the flexibility. Even GPIO is running continuously, it has limitations that are with ESP8266 due to less pins are available. And containing the extra serial interface is benefiting for the debug. Especially a hardware support for the encrypting and decrypting and this can make a device computer with security much easier. The most thing is that the IoT prototyping systems i.e., hardware are supporting the software debugging. The functionality level can be decided by giving the numbers. A number 10 means that a very high functionality and a low number means that a limited functionality.

IoT Software

Precisely, Python is using for Raspberry Pi and C or C++ are for Arduino IDE (Figure 5). Python is a programming language. It is a high-level language and for general purpose. It is providing for emphasizing the code readability and it is especially keeping that out of having loose pointers like curse of all C or C++ programmers. Also, it does the memory managements. This is a programming language for the choice of Raspberry Pi. The Python has huge set of libraries and these are for IoT. Also, the embedded system device of any programming language of the Raspberry Pi.

A screenshot of the Arduino IDE interface. The window title is "Blink | Arduino 1.8.5". The menu bar includes "File", "Edit", "Sketch", "Tools", and "Help". The toolbar contains icons for opening files, saving, running, and other IDE functions. The main text area shows the following C++ code for a Blink sketch:

```
Blink
// the setup function runs once when you press reset or power the board
void setup() {
  // initialise digital pin LED_BUILTIN as an output.
  pinMode(LED_BUILTIN, OUTPUT);
}

// the loop function runs over and over again forever
void loop() {
  digitalWrite(LED_BUILTIN, HIGH); // turn the LED on (HIGH is the voltage level)
  delay(1000); // wait for a second
  digitalWrite(LED_BUILTIN, LOW); // turn the LED off by making the voltage LOW
  delay(1000); // wait for a second
}
```

Figure 5: Arduino IDE

Why C++ is using majorly for IoT devices? There are mainly four reasons of using the C++ for IoT devices.

1. C language programs can be compiled into the native code and these are for the smaller devices. It is providing enough good control on over timing and size. The Python is required interpreter that will be larger code and that can't fit into the smaller IoT device like Arduino. There are possibility of a GB (gigabyte) of RAM with 8GB of SD card storages on a Raspberry Pi. And on an IoT devices, it might only require a2K (2000 bytes) & 32KB of the code storage. This is the ratio of the 500,000 to 1.
2. While working with the C or C++ programs, there is a chance to nearer to the hardware and will benefit for a better controlling of time for the operation/process. This would be an important in few scenarios. The memory garbage collector is one of the issues in Python programming. Sometimes, the program may execute out of the memory and the Python can invoke the garbage collectors to cleanup the memory. This will set this up back for the reuse. That can be causing the programs not to run in a duration as per expectations.
3. The libraries of Arduino C or C++ are almost for all devices and applications that can be imagined for the IoT application. An Arduino library is itself filled with many of the functionalities at huge number and this is making more easier for getting an IoT applications that are running and available.
4. For the small IoT devices, Arduino Integrated Development Environment (Arduino IDE) will be better environment and this is for code writing. Arduino has its own twists and few disadvantages. The main disadvantage is that Arduino does not support a pre-built debugger. Even Arduino not having built-in debugger, it can run on Windows, Linux and Mac. This IDE i.e., Arduino is majorly available. Also many resources are available for learnings and libraries that can be used for designing. Other than Arduino IDE, the alternative includes that the Visual Micro and this also runs on Windows. Visual Micro is built up on Microsoft Visual Studio. Also Eclipse is running based up on Windows, Mac and Linux. The Eclipse will nightmare for setting up as well for updates.

The IoT-aware Business Process (BP) is grouping the both IoT subject and the BP subject. The business process having multiple modeling languages. And, among them UML (Unified Modeling Language) and BPMN (Business Process Modeling and Notation) and Petri net, etc. IoT-aware business process includes that the IoT support. But, according to ISO/IEC 20924:2018 standard, the IoT support must include.

1. IoT device: It is the entity, which can interact with another any physical entity using the actuators and sensors.
2. Actuator: It is the IoT device, which is capable of changing the physical state of the entity.
3. Sensor: It is the IoT device. That is capable of measuring the properties of physical entity like speed, temperature etc. Actually, the sensors sending the captured information/data to an actuators with the help of network like Wi-Fi, etc.
4. IoT user: It is the end user of an IoT device and it represents that may be human so may not be humans.
5. IoT gateway: It is a group of network connectors. This connects one/more networks for transferring information to IoT devices like a router.

IoT Software Architecture mainly the IoT architecture contains three layers. These are the servers, applications and sensor networks. The server's layer of the architecture employees edge computing. It can contain the intermediate nodes, edge nodes and applications. The applications layer of the architecture employees the user layers, edge layers and cloud layers. These are the layers again consisting the functionality and designing elements.

4 IoT Stack Provocations and Concerns

There are multiple security threats that may face while working with IoT models either with or without cloud platform such as device physical attacking, traffic analysis attacks, etc.

1. Regarding to the physical attacking, the attackers can access devices directly. Then they can manipulate in various aspects in IoT devices. Due to attackers have the closer proximity of IoT device or hardware, as per various intentions like limiting lifetime, physical damaging the hardware, endangering communication mechanisms and tampering with source of energy, so on.
2. IoT is combining with different communication technologies like lower protocol stack layers of protocol TCP/IP. It provides the complex networking with heterogeneous. These technologies are included in IoT. But it will not limit to WSN, ZigBee, WiFi, MANET, NFC, RFID and these are the technologies contains their security issues.
3. In case of network layer, the attacking is at routing level, spoofing, traffic analysis, data as well as launching. As routing is mainly functioning at networking layer, it is required that the up to date the information of routing must be updated in the routing tables. In case of attackers, they are capable to modify any information of routing or either spoofin an IoT. Then it will impact to the regular functionalities of applications, also it may be causing the leakage of sensitive data.
4. The process to process delivery is responsible by the transport layer. Here, the transport protocols are enabled the processes for exchanging the data. In this specific subject of IoT, the security of traditional layers problems of transport continues. DoS attack is the most serious at the layers that are choking the networks. Also it will result in a state of rejection about service to application.
5. There are passive attacks and that are traffic analysis attacks. Here, the attackers listen to traffic passively. These are the attacks very hard for mitigating. Because communicating parties are usually having no idea. Mainly, the attackers may looks for the interesting data/information from internet traffic like user personal data/information, credentials, business logics related data and another data/information, which can be any value for the attackers.
6. The most important enablers are for the IoT is the cloud platform. This can leverage for huge amount of data generation after by theIoT subsystems. The security related considerations are the primary importance when cloud is the platform for IoT in terms of cloud tenants, in addition to this from the perspective of the service providers. When the number of IoT devices adding to the IoT network, it includes data producing by all the devices/systems and storing, processing, analyzing by the cloud. In such scenarios, scalable privacy and security are the considerations.

There are standardization challenges and scalability concerns while handling applications of IoT.

1. Standardizing is very important step and major challenges reporting in field of IoT applications. It is backbone of IoT developments. The very important standardizing bodies are like ITU, ETSI, IEEE, IETF etc. These are involving in the framework for the development of IoT. The standardizing activity is a different approach that can provide seamless activity and open standards. There are few issues for integrating with different standards to make it consistent.
2. As per scalability in IoT, it is referring adding new IoT services and devices in existing systems for better performance benefits. It can support a huge number of IoT devices with different constraints. For the applying of the scalability there must be standard architecture and framework. This major issue in the scalability that will appear when adding new objects and devices in IoT.

Cloud platform specific concerns and issues will impact when we deploy and working with IoT on Cloud Platform. These challenges are additional to commonly available concerns with IoT. When we combine IoT with Cloud platform, the combination gives different individual IoT challenges as well as the Cloud challenges. Anyway, due to combination of two technologies i.e., IoT and Cloud causing additional challenges. Actually, the most of IoT data is in form of semi-structure and un-structure. And the data is coming from many distributed sources and a huge amount of the data is coming from the IoT sources. IoT with Cloud is providing the real-time data/information processing benefits as well as the services provisioning techniques like big data. For the Cloud platform, issues are due to providing more resource management dynamically as well as the orchestration techniques. The dynamic concept [15] is offloading from the hosts/clients to cloud.

There are many miscellaneous challenges in IoT technology stack in addition to mentioned above.

1. As the clients are completely immersed in IoT network, there will be a high dependability from user on IoT network especially in the healthcare systems/applications.
2. These days, the personal computers (PC's) are reducing and the new IoT devices may be in a Nano size and will be transparent. It will be tough to maintain quality control, traffic control or audit, because of Nano sizes and huge count of IoT devices.
3. In case of medical applications, localization of IoT cannot be possible. Here, the services can be offered overseas. Hence, it is the challenge for the nations in dealing with the new concepts.
4. There will be difficult situations in terms of differentiating between the virtual devices and physical devices as a human.
5. There will be billions of IoT devices and every device must have unique identification in network regarding maintaining the log. The identification issues will come up with another proof of identity problems.
6. The billions of IoT devices may be always on 24/7 support. This may result in huge amount of information/data i.e., big data [20], which may be much more exposed to the malicious attacks.
7. As human beings are part of the IoT networks along with other sensors and devices, this will result the hybrid network. The interconnected devices are may interfere in the human

actions. In case of continuous implementations/developments of an IoT that may lead to ambiguous behavior and this is causing not fully and efficiently understandable by the end users.

8. As per the considerable count of the network switches, routers, and information, the IoT governance and control will be highly challenging. The data/information exchanges may be less expensive and faster; this leads to difficulty in controlling or monitoring. Additionally, the accountability will be a challenge to tackle.

5 Proposed Methodologies for future IoT Technology Stack

The proposed methodologies are applicable for IoT with or without Cloud platform. These are including hardware specific, software specific, standardization related, etc. benefit for future IoT better implementations.

1. The IoT related concepts must be built on thorough defined standards for IoT with or without Cloud platform. For example, the standards can include the ISO/IEC 20924:2018 as per IoT standards and the working standard Web of Things (WoT) defined by the World Wide Web consortium (W3C), which is intended to enable interoperability across IoT platforms and applications.
2. Must consider IoT qualities like QoS, QoT and QoI regarding the performance improvement of IoT-aware BP.
3. Dynamic and flexible model should be with IoT to overcome the future challenges. Generally, the flexibility is allowing the managers who are closing working with business to avoid access issues.
4. IoT on Cloud platform will be in an attractive mode. This going forward may facilitate the decentralizations of IoT executions. In this context, the business may enhance the executions of their processes and improve their requirements, etc.
5. The propounded models must be initiated by an analysis stage. This will allow the business analyzer for identifying the main requirements, constraints and used tools. Significantly, this leads to propose a model for every IoT build and then the models facilitate the developments of action items. Thereafter, it will be crucial for developing the IoT model i.e., a prototype with the help of available development tools and utilities. Afterward, the developed IoT model should be tested thoroughly as per challenges and issues before finalizing it to production.
6. Machine Learning (ML) and Deep Learning (DL) must be benefited for providing solutions as per challenges or issues discussed in IoT technology stack.

6 Conclusion

IoT can be defined as a global computing technology network in which each will connect to the internet. Because of its benefits such as accuracy, speed, etc., the associated objects number will rise every day. The Cloud computing technology has grandly matured over the last few years. This cloud concept is anything that can host on Internet, which is available for the use, for the provision and composition when needed and these are for the sophisticated services from the providers. The success rate of the IoT services on cloud can be achieved as per

expectations according to more business opportunities/requirements with maintaining the reliability and high performance. In future i.e., going forward, they will be having major concerns about infrastructure, models of business, security and also trade standards, while finishing IT networking and computing systems. IoT related things can be referring to objects which are from human regular life, that are ranging from the house hold items with smartness like smarter adapter, smarter bulb, smarter refrigerator, smarter meter, smarter oven, et. This paper is about the research on IoT technology stack related most common provocations and concerns. This leads to different challenges or issues that are related to security, standardization, scalability, network, etc. are discussed in this paper. There are multiple security threats that may face while working with IoT models either with or without cloud platform such as device physical attacking, traffic analysis attacks, etc. are discussed in this paper. There are standardization challenges and scalability concerns while handling applications of IoT related points mentioned in this paper. Cloud platform specific concerns and issues will impact when we deploy and working with IoT on Cloud Platform. These challenges are additional to commonly available concerns with IoT. There are many miscellaneous challenges in IoT technology stack in addition to these are covered in this paper. The ML (Machine Learning) can also be consider as one of most suitable and useful computational paradigm to provide the embedded intelligence in IoT devices. The Machine Learning can also help smart devices and machines to infer the more useful knowledge from device or human generated data/information. Finally, the given proposed methodologies are applicable for IoT with or without Cloud platform. These are including hardware specific, software specific, standardization related, etc. benefit for future IoT better implementations.

References

- [1] NajlaFattouch,Imen Ben Lahmar,KhouloodBoukadi,IoT-aware Business Process: comprehensive survey,discussion and challenges,DOI 10.1109/WETICE49692.2020.00027,2641-8169/20/\$31.00 ©2020 IEEE.
- [2] Fatima Hussain,RasheedHussain,Syed Ali Hassan,EkramHossain,Machine Learning in IoT Security: Current Solutions and Future Challenges,1553-877X c 2020 IEEE.
- [3] Akhilesh Kumar Singh,ManishRaj,VivekSharma,Architecture, Issues and Challenges in Monitoring based on IoT for Smarter Environment,978-1-7281-4889-2/20/\$31.00 ©2020 IEEE.
- [4] MekalaMS,ViswanathanP,Sensor Stipulation with THAM Index for Smart Agriculture Decision-Making IoTSystem,WIRELESS PERSONAL COMMUNICATIONS,APR 2020 10.1007/s11277-019-06964-0.
- [5] GayathriNB,ThumburG,KumarPR,RahmanMZU,ReddyPV,Lay-EkuakilleA,Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks,IEEE INTERNET OF THINGS JOURNAL,OCT 2019 10.1109/JIOT.2019.2927089.
- [6] DabbakutiJRKK,ChB,Ionospheric monitoring system based on the Internet of Things with ThingSpeak,ASTROPHYSICS AND SPACE SCIENCE,AUG 2019 10.1007/s10509-019-3630-0.
- [7] Sachin GoswamiA,BhargavPadhyaP,Ketan Patel D,Internet of Things: Applications,Challenges and Research Issues,978-1-7281-4365-1/19/\$31.00 ©2019 IEEE.
- [8] NilupuleeGunathilakeA,William Buchanan J,RameezAsif,Next Generation Lightweight Cryptography for Smart IoT Devices,978-1-5386-4980-0/18/\$31.00 ©2019 IEEE.
- [9] Pooja Yadav,AnkurMittal,HemantYadav,IoT: Challenges and Issues in Indian Perspective,978-1-5090-6785-5/18/\$31.00 © 2018 by IEEE.
- [10] ParthibanAnnamalai,JyotsnaBapat,DebabrataDas,Emerging Access Technologies and Open Challenges in 5G IoT: From Physical Layer Perspective,978-1-5386-8134-3/18/\$31.00 ©2018.
- [11] Ahmed AboBakr,MarianneAzerA,IoT Ethics Challenges and Legal Issues, 978-1-5386-1191-3/17/\$31.00 ©2017 IEEE.
- [12] NomusaNomhleDlamini,KevinJohnston,Internet of Things (IoT) in retail businesses, 978-1-5090-2576-3/16/\$31.00 ©2016 IEEE.

- [13] Abdur Rahim Biswas,RaffaeleGiaffreda,IoT and Cloud Convergence: Opportunities and Challenges,978-1-4799-3459-1/14/\$31.00 © 2014 by IEEE.
- [14] KolliC.S.,Krishna Reddy V.V.,VenkataRamanaN,Internet of things: A survey on security threats and study on azure and AWS IoTframeworks,Journal of King Saud University - Computer and Information Sciences.
- [15] Kumar M.P.,SrideviG.,Hussain, M.A.,Secure and reliable VMS for internet of things or cloud based applications,Journal of Advanced Research in Dynamical and Control Systems.
- [16] SagarK.V.D.,DeepikaG.B.,ReddyM.S.,NarayanaS.,RaoK.R.,Developing smart kitchen inventory tracking using internet of things,Journal of Advanced Research in Dynamical and Control Systems.
- [17] ShaikR.,KumarGudapatiN.,KumarBalijepalli N.,Medida H.R.,A survey on applications of internet of things,Management Science Letters.
- [18] Srinivas C.,KumarCh.M.,Toxic gas detection and monitoring utilizing internet of thingsMaterials Today Proceedings.
- [19] Navulur S.,Sastry A.S.C.S.,Giri Prasad M.N.,Agricultural management through wireless sensors and internet of things,International Journal of Civil Engineering and Technology.
- [20] Radhika D.,ArunaKumariD.,The smart triad: Big data analytics, cloud computing and internet of things to shape the smart home, smart city, smart business & smart country International Journal of Engineering and Advanced Technology.