A REVIEW PAPER ON ARCHITECTURE AND WORKING OF INTERNET OF THINGS

ADITHYA M V KASYAP[1]

KANDULA ANKAMMA RAO[2]

[1]*PG-Student, Department of Mechanical Engineering, Mahatma Gandhi Institute of technology, Hyderabad, India*

[2]*Professor, Department of Mechanical Engineering, Mahatma Gandhi Institute of technology, Hyderabad, India.*

***Abstract**: Due to the increase in Automation, Internet of Things (IoT) has gained a huge potential in building a powerful home and industrial automated systems. Deployment of IoT systems has gradually increased in the recent years. In today's world controlling and monitoring have become key aspects for a safe and flexible automated system which is done using IoT with the help of internet access for collecting and exchanging of data. Operating the equipment's without human presence has gained a huge importance especially in the industries since it eliminates the human workers to work in hazardous conditions. The proposed work is associated with the working process in building an IoT system.*

1. INTRODUCTION

Internet of Things can be defined as a system of interconnected devices such as electronic and electrical equipment's, sensors and actuators with internet connectivity so that these devices can interact and communicate over the internet to monitor and control remotely. The basic component used to build IoT system requires a sensor the most commonly used sensors are temperature sensor, pressure sensor, passive infrared sensor and smoke sensor. Sensor starts sensing the corresponding parameters. The data which is collected is conditioned and amplified, and is interfaced to a microcontroller based circuit.

Raspberry pi 3: It is a small single board computer. The Raspberry Pi 3 consists of a quad-core ARM Cortex-A53 processor with on board Wi-Fi, Bluetooth, USB boot capabilities and on chip graphics processing unit with General purpose Input /Output (GPIO) pins

Features of Raspberry pi 3

POWER SUPPLY	5volts
RAM	1GB
NETWORK	10/100Mbps Ethernet and 802.11n wireless LAN
Input/output pins	26
CLOCK FREQUENCY	1.4GHz

IoT Gateway: An IoT gateway is a physical device or a software program that serves as a connection between IoT cloud and sensors, controllers and intelligent devices. The data moving from or to the cloud goes through this gateway. A gateway is used to aggregate the data while it is passing to the cloud since some sensors produce a huge amount of data per second. The data gets summarized due to which the volume of data reduces which have a huge impact on response time. Another benefit of this gateway is that it helps in eliminating data leaks since the data flow is in both directions.

Cloud storage: cloud storage is a model for the data tbe stored in servers so that data can be accessed over internet from any place and at any time. The advantage of cloud storage is that it helps in eliminating the use of physical devices to store large volume of data which helps in reducing the overall cost of an IoT system. The cloud storage providers are responsible for keeping data available and accessible. Application Programming Interface (A.P.I) which consists of set of methods is used to access the cloud storage. This is used as a framework to connect IoT devices over the web so that the sensing data enter to the cloud. The devices are connected to the cloud by using wireless or wired connections.

Wireless connections	Wi-Fi, Bluetooth, Zigbee, light-fidelity (Li-Fi), Long Term Evolution (LTE) Advanced, Low Powered Wide Area Networking (LPWAN)
Wired connections	Ethernet, Power Line Communication

3. WORKING OF AN IoT SYSTEM

In IoT systems, sensors start sensing the corresponding parameters. The data collected by sensors is conditioned and amplified to interface it with Raspberry-Pi system. Simultaneously the sensed values uploaded onto webpage. The authorized person can access the data from any place at any time, monitor the parameters and control the load through IOT successfully.

Sensing phase:

IoT can be considered as a world-wide physical inner connected network, in which things can be connected and controlled remotely. In the sensing phase, the wireless smart systems with tags or sensors are now able to automatically sense and exchange data among different devices. This technology significantly improves the capability of IoT to sense and identify things or environment. The volume of data produced from sensors is large and unstructured. This raw data collected from various sensors must go through some data analysis phases such as pre-processing, segmentation and feature extraction which is done by a IoT gateway using data-mining and machine learning algorithms and models so that the data gets structured and classified. Sensors are interfaced to Raspberry pi 3 since it behaves as an IoT gateway.

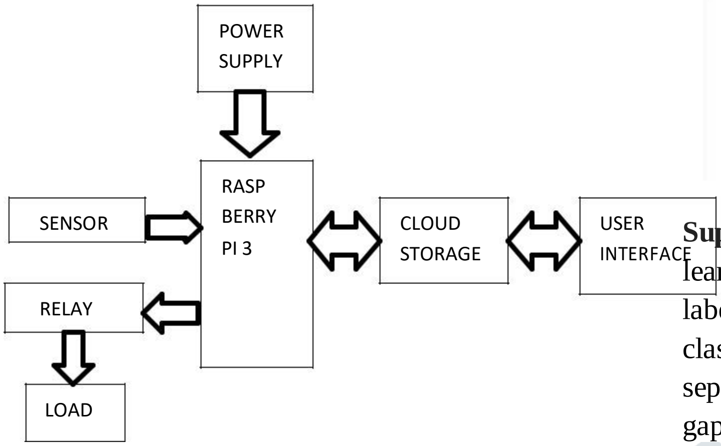
Networking phase:

The role of networking phase is to connect all things together and allow things to share the information with other connected things. To design the networking layer in IoT, designers need to address issues such as network management technologies for heterogonous networks (such as fixed, wireless, mobile, etc.), energy efficiency in networks, Quality of Service requirements, service discovery and retrieval, data and signal processing, security, and privacy. The data received from the sensors send to the cloud by setting up a HTTP client using any programming language which has required libraries to do so.

User phase:

When the data is stored in the cloud the software performs some actions like checking whether the sensed values are under acceptable range if not it sends an alert SMS or a notification to the user. The user can also perform certain actions by sending the commands to the cloud using a user interface which may be a mobile phone or a computer. The user commands from the cloud are received by the raspberry pi which processes them to energize the relay with a small voltage to run heavy loads [1-2]. For the effective implementation of IoT in home automation one of the major parts is communication technology or called as Connectivity. Some connectivity medium is Bluetooth, Wi-Max and Wireless LAN (Wi-Fi), ZigBee, and Global System for mobile communication (GSM). Even though there are many advancements in communication technologies, but some disadvantages which affects the operation. The main connectivity issues can be narrowed down to standards and challenges. The connectivity standards are considered the backbone of IoT as the choice of standards has an untoward impression on execution. The standards usually employed in IoT are Wi-Fi, ZigBee, Z-Wave, Bluetooth LE, Thread, etc., Some challenge factors in IoT communications are Interoperability, Self-

Management, Maintainability, Signalling, Bandwidth and Power Consumption. Depending on connectivity, cloud based IoT concepts is advantageous while considering energy dissipation and a hardware effort [3].

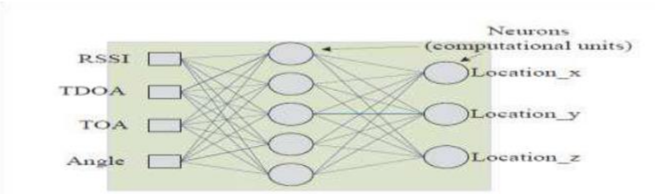


Architecture of IoT system

Data Analysis in IoT

Data analysis is done to aggregate and summarize the data collected from sensors. Machine Learning and deep learning techniques are used for this purpose. Over time, its focus evolved and shifted more to algorithms which are computationally viable and robust. In the last decade, these techniques have been used extensively for a wide range of tasks including classification, regression and density estimation in a variety of application areas such as bioinformatics, speech recognition, spam detection, computer vision, fraud detection and advertising networks. In order to make IoT more efficient and scalable, following three algorithms can be implemented keeping in view the topology and computing ecosystem of the participatory devices in IoT [4].

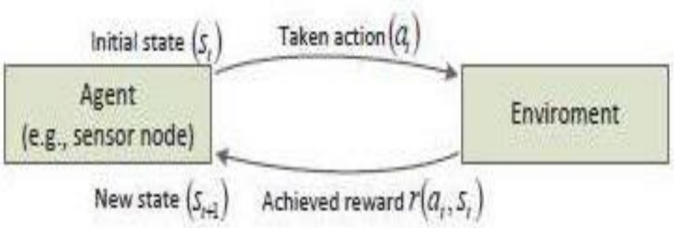
Neural Networks*:* For example, sensor node localization problem (i.e., determining node's geographical position) can be resolved using neural networks. Node localization can be based on propagating angle and distance measurements of the received signals from anchor nodes. Such measurements may include received signal strength indicator (RSSI), time of arrival (TOA), and time difference of arrival (TDOA) . After several training, the neurons can compute the location of the node. This will help us to identify the node location exactly, and machines can detect the node location and target decisions accordingly.



Support Vector Machines (SVM): It is a machine learning algorithm that learns to classify data points using labeled training samples Basically, the problem is to classify those nodes into two parts. These parts are separated by as wide as possible margins (i.e. separation gaps), and new reading will be classified based on which side of the gaps they fall on. An SVM algorithm, which includes optimizing a quadratic function with linear constraints provides an alternative method to the multi-layer neural network with nonconvex and unconstrained optimization problem. This will help us to find nodes in the vast array or pool of IoT devices, and consume data and perform analytics accordingly.

Reinforcement Learning: Reinforcement learning enables an agent (e.g., a sensor node in case of IoT) to learn by keeping trying and gaining experience, just like humans. The agent regularly updates its achieved rewards based on the taken action at a given state. The future total reward (i.e., the Q-value) of performing an action at a given state is computed using following Equation.

$$Q\ (s_t+1,\ a_t+1) = Q\ (s_t,\ a_t) + \gamma\ (r\ (s_t,\ a_t) + Q\ (s_t,\ a_t))$$



Data security requirements:

In the IoT, multiple sensors, tiny computer chips and communications devices will be integrated with physical objects such as appliances to enable communication between them and other computing devices such as cloud servers, computers, laptops and smartphones. These devices will exchange huge amount of data with each other's. Therefore data security is very important concerns for IoT [5].

a) Data Integrity: While exchanging the data if some attackers modifies the contents of data then it can brought huge damage to our system. Thus data integrity while communication is very much important.

b) Data Confidentiality:

Confidentiality must be preserved while communication. Whatever data IoT devices will share should be encrypted using good encryption algorithm so attacker will not be able to interpret the actual data. Therefore IoT devices should be configure in such a manner so they will share data to only authorized device.

c) Data Availability: Principle of availability says that data should be available always to authorized IoT devices and users.

Access level security requirements

a) Authentication: Authentication is used to check weather a communicating device is legitimate or not means if device A has send some data to B then authentication mechanism is used to ensure that it has come from A. It is also used to verify that an authorized user has access to IoT device.

b) Access control: Access control is used to ensure that an authenticated or authorised IoT devices only have access to those things which these devices are authorised for.

c) Availability: Principal of availability states that data or IoT devices should be always available to authorised parties.

d) Non Repudiation: Not- repudiation does not allows a communicating party to refute the claim of not sending the data which it has send.

CONCLUSION

The proposed work describes about the architecture and working of an IoT system. Raspberry pi 3 which is a small single board computer is used as a gateway to structure and classify the large volume of raw data from the sensors by data analysis using machine learning algorithms and then the data is send to the cloud. The user can login by giving a correct username and password in order to control and monitor the system even from remote places.

5. REFERENCES

[1]. Li Da Xu, Wu He, and Shancang Li, "Internet of Things in Industries: A Survey" IEEE transactions on industrial informatics, vol. 10, no. 4, November 2014.

[2]. G.V.V.N.G.Vital, Supriya. Koppula, Rakesh.Potluri, "A IoT System for Industrial Automation" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 6 Issue II, February 2018.

[3]. S.Pradeep, T.Kousalya, K.M.Aarsha Suresh, Jebin Edwin, "IoT AND ITS CONNECTIVITY CHALLENGES IN SMART HOME" International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 12 | Dec -2016.

[4]. From Rashid Ashraf Malik, Asif Iqbal Kawoosa, Ovais Shafi Zargar, "MACHINE LEARNING IN THE INTERNET OF THINGS – STANDARDIZING IOT FOR BETTER LEARNING" International Journal of Advance Research in Science and Engineering Volume No.07 Special Issue No.04 March 2018

[5]. From Laxman Singh Sayana, Bineet Kumar Joshi,"SECURITY ISSUES IN INTERNET OF THINGS " Global Challenges – Role of Sciences & Technology in Imparting their Solutions (GCRSTS 2016).