IOT : Architecture, Applications & Challenges

Ms. Archana Chaugule
Assisstant Professor
Information Technology
Shah and Anchor Kutchhi engg.College
Mumbai ,India.

Abstract— Internet of Things now touching every corner of the globe, IOT simply define as interaction between Physical world with Digital World using Sensors and Actuators. This paper mainly focus on what are the challenges still we are Facing for designing IOT architetures, how to design IOT architecture for different applications because depending on applications ,needs are different.

Keywords— Internet of Things (IOT), Architectures, Challenges.

I. INTRODUCTION

The idea of IoT is to interconnect the physical world with the digital world therefore; sensors measure parameters of the physical world as well as changes of it. Consequently, this information is translated into data by computers , aim of IoT is to act on the physical world through actuators, sensors , e.g., the temperature of a room can be measured and monitored The popular architecture of IoT is illustrated in Fig. 1.It consists of three layers: perception layer, network layer and application layer. Sensors, Actuators, RFID tags and other smart terminals are connected to the IoT from the perception layer. Network layer is responsible for the communication between "things" and human beings. Abundant applications are provided by the application layer [3]

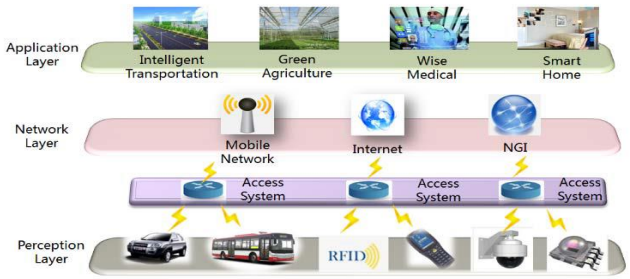

Fig. 1. Three-layer Architecture of IoT.[3].

II. CHALLENGES FOR IOT

Availability

Availability of the IoT must be realized in the hardware and software levels to provide anywhere and anytime services for customers. Availability of software refers to the ability of the IoT applications to provide services for everyone at different places simultaneously. Hardware availability refers to the existence of devices all the time that are compatible with the IoT functionalities and protocols. Protocols such as IPv6, CoAP, etc., should be embedded within the single board resource constrained devices that deliver the IoT functionality. [1]

Reliability

Reliability refers to the proper working of the system based on its specification Reliability aims to increase the success rate of IoT service delivery. It has a close relationship with availability as by reliability, we guarantee the availability of in-formation and services over time. Reliability is even more critical and has more stringent requirements when it comes to the field of emergency response applications. In these systems, the critical part is the communication network which must be resilient to failures in order to realize reliable information distribution. Reliability must be implemented in software and hardware throughout all the IoT layers. In order to have an efficient IoT, the underlying communication must be reliable, because for example by an unreliable perception, data gathering, processing, and transmission can lead to long delays, loss of data, and eventually wrong decisions, which can lead to disastrous scenarios and can consequently make the IoT less dependable proposes a reliability scheme at the transmission level to minimize packet losses in IoT environments. [1]

Mobility

Mobility is another challenge for the IoT implementations because most of the services are expected to be delivered to mobile users. Connecting users with their desired services continuously while on the move is an important premise of the IoT. Service interruption for mobile devices can occur when these devices transfer from one gateway to another. Proposes a resource mobility scheme that supports two modes: caching and tunneling to support service continuity. These methods allow applications to access the IoT data in the case of the temporary unavailability of resources. The enormous number of smart devices in IoT systems also requires some efficient mechanisms for mobility management. Group mobility is managed by a leader based on some similarity metric that is based on the mobility pattern of devices.[1]

Performance

Evaluating the performance of IoT services is a big challenge since it depends on the performance of many components as well as the performance of the underlying technologies. The IoT devices need to be monitored and evaluated to provide the best possible performance at an affordable price for customers. Many metrics can be used to assess the performance of the IoT including the processing speed, communication speed, device form factor and cost.[1]

Management

The connection of billions or trillions of smart devices presents service providers with daunting issues to manage the Fault, Configuration, Accounting, Performance and Security (FCAPS) aspects of these devices. Managing IoT devices and applications can be an effective factor for growing the IoT deployments.[1]

Scalability

The scalability of the IoT refers to the ability to add new devices, services and functions for customers without negatively affecting the quality of existing services. Adding new operations and supporting new devices is not an easy task especially in the presence of diverse hardware platforms and communications protocols. The IoT applications must be designed from the ground up to enable extensible services and operations.[1]

Interoperability

End-to-end interoperability is another challenge for the IoT due to the need to handle a large number of heterogeneous things that belong to different platforms. Interoperability should be considered by both application developers and IoT device manufactures to ensure the delivery of services for all customers regardless of the specifications of the hardware platform that they use.[1]

Security and Privacy

Security presents a significant challenge for the IoT implementations due to the lack of common standard and architecture for the IoT security. In heterogeneous networks, it is not easy to guarantee the security and privacy of users. The core functionality of the IoT is based on the exchange of information between billions or even trillions of Internet connection objects. Privacy issues and profile access operations between IoT devices without interferences are extremely critical. Securing data exchanges is necessary to avoid losing or compromising privacy. [1]

III. IOT APPLICATIONS ARCHITECTUIRES

A. Network function virtualization (NFV) based IOT Architecture

Fig. 2 show NFV base IOT Architecture. This approach enables the IoT gateway to be very simple and not to contain any application logic—providing a kind of translation between Layer 2 protocols towards simple IoT devices, such as sensors and actuators, on its southbound interface (e.g. ZigBee or Bluetooth) and the IP protocol on its northbound interface. IoT applications are running in the data center on a standard hardware shared among different applications. The data center is implemented in a layered approach. The HW layer offers a scalable and elastic hardware platform based on commercial off-the-shelf (COTS) components, the Virtualization layer uses the HW layer to provide virtual machines towards the applications, whereas the management and orchestration layer ensures lifecycle management of IoT applications, as well as the coordination of the resources and different IoT applications. [2]

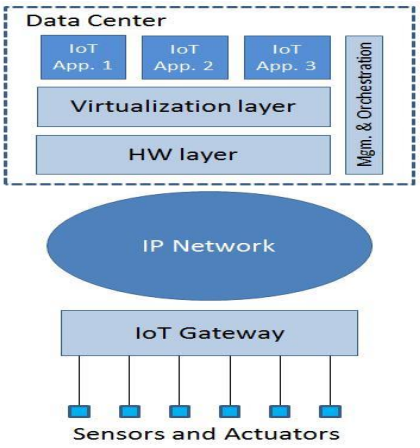

Fig. 2. NVF based IOT Architecture [2]

B. A Novel IoT Access Architecture

As shown in Fig. 3 the system is mainly divided into two main parts: master module and data acquisition module, and the two modules communicate through the universal asynchronous receiver/transmitter (UART) interface. The data acquisition module is responsible for accessing multiple sensors and collecting environmental information. It can support both analog and digital signal inputs through analog-to-digital converter (ADC) and digital-to-analog converter (DAC). A coprocessor is implemented with IP core conducts control and signal disposal of the whole module. According to IEEE1451.2 standard, transducer electronic data sheet (TEDS) is used to describe the type, operation and attributes of sensors, actuators and transducers, which is implemented and stored in block RAM (BRAM) in this design. As the major unit of the whole system, the master module provides other core functions: network communication, local storage, etc. Besides, the master module provides interfaces to access those high-speed devices such as digital camera. An ARM Cortex processor is adopted as the main controller with high performance, reliability and stability.

With this design, the system can access various kinds of sensors, actuators and other high-speed devices in IoT environment. The specifically designed data acquisition module undertakes data acquisition tasks, which enables the master module focus on the complex tasks such as network communication and local storage. [3]

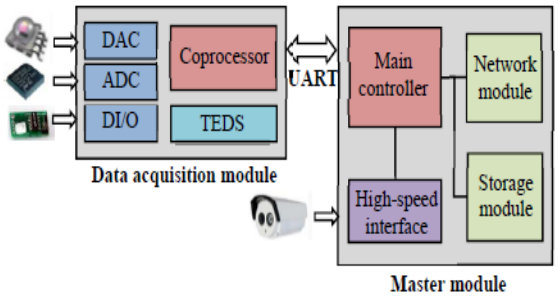

Fig. 3. A Novel IoT Access Architecture [3]

C. IOT Architecture for Caring Home System.

As shown in Figure 4, our system architecture is divided into two main subsystems:

- The smart home engine manages devices locally in hard real-time.
- The cloud analysis engine provides soft real-time analysis.

Our smart home engine is based on *BCS*, a building control system developed by iTechTool over the past 20 years. BCS is designed to manage both sensors and actuators in a home. The central data structure of BCS is the *timewheel*, a time-sorted queue of events. Each sensor reading or actuator command is time stamped; the associated event is placed into the timewheel queue based on its timestamp. The time wheel advances with the real-time clock, processing events in their proper time order.

The cloud analysis engine is based on the Google Cloud *mysql* database. Selected events are translated from the timewheel to the cloud for further analysis. Events do not necessarily appear in the same format in the time wheel and the cloud database, largely for privacy reasons, although storage is an additional consideration. [5]

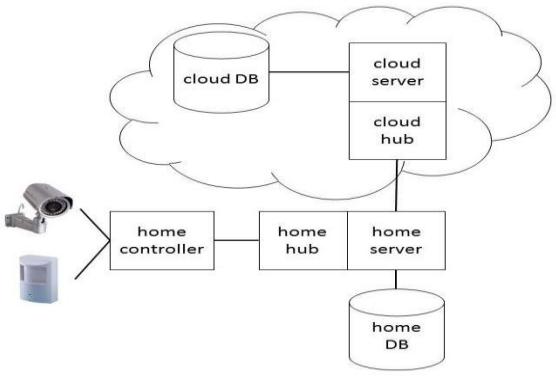

Fig. 4. IOT Architecture for caring home system [5]

D. A generic IoT architecture for a Smart City.

An IoT platform, which could serve as a generic architectural foundation for a 'smart city' development, is depicted in Fig. 5. Its core element is the Integrated Information Centre, operated by an IoT service provider. At the bottom, this centre is linked to a set of services, including electrical energy; water, central heating and gas supply; intelligent transportation services (ITS); city fire protection and security; co-operative medical services; commercial and tourism services; and tax and fees payment services. Supplementary platforms in this architecture pro-viding support for these services include: a cloud computing and data centre, a management centre, an application platform, an evolutional platform of an urban eGovernment, an emergency plan command, a mobile service platform, and an Internet infrastructure. [6]

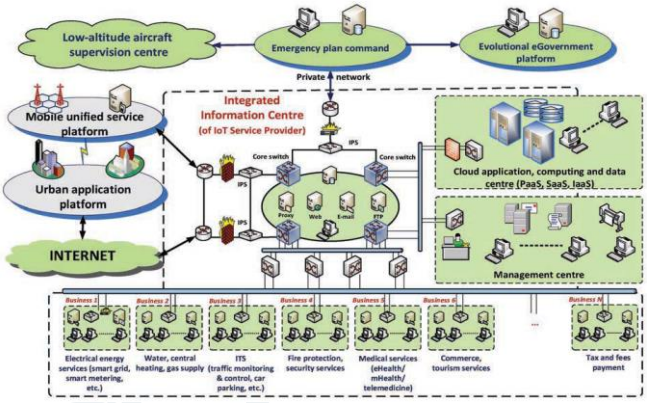

Fig. 5. A generic IoT architecture for a smart city.

E. IoT Football Architecture

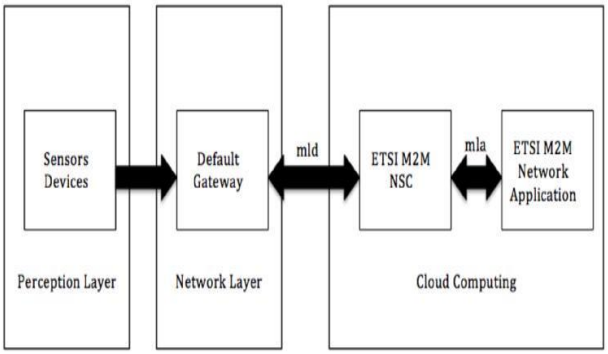

Fig. 6. IoT Football Architecture

As shown in above fig. 6. IoT Football Architecture consists of three main layers, Perception Layer, Network Layer and Application Layer

Perception Layer: There are two networks of sensors in this layer. The body wireless area networks (WBA Ns) are the sensors that have the ability to measure the physiological parameters from the body of the footballer. These types of sensors must not weigh a lot as they are wearable, for example, a T-shirt. In terms of communication with the gateway, each sensor in the body must be able to have its own IPv 6 (6LoWPAN), working with Routing Protocol for Low-Power (RPL).The sensors must operate with a gateway to send and receive packets in the CoAP protocol. In addition, the devices must be able to meet the security capabilities and the QoS requirement. Finally, in-the-body sensors must be able to

be re-configured immediately to meet the requirements if there are any changes in the network topology. The devices around the stadium that measure the temperature and illumination levels do not necessarily have the same capabilities as the body sensors, but they need to be interoperable with the body sensors in terms of dealing with the same cloud service and should provide an accurate result.

Network Layer: ZigBee technology is used for the base station in the system. The base station must be connected with a network domain via a wired connection. The base station also needs to work with 6oLWPAN, which means supporting the IEEE 802.15.4 based network. In addition, the gate way must implement the CoAP protocol to send and receive packets to and from sensor devices. Finally, it must have security capabilities and QoS requirements.

Application Layer: Cloud services must analyze all the data traffic that comes from the devices to give accurate feedback to the coach or supervisor. Predictive analytics in data mining could be used for analyzing and predicting possible injuries or conditions to the footballer. The cloud services must also activate the security capabilities and QoS. The data must be stored in a safe place. Finally, the cloud service must be compatible with different software platforms to provide all services to the coach or the supervision. For example, it should be able to provide the footballer's details including health status, previous illnesses, and fatigue level.[7]

IV. CONCLUSION

In this paper we discuss about basic architecture of IOT which consist of three layers, then we discuss about some common challenges of IOT like management, security etc.. Day by day growth of IOT is increasing rapidly; it's having large impact on our daily life activities so depending upon requirement of application we will design architecture of IOT ,here we discuss some architectures for different applications like IOT football architecture, IOT architecture for smart city etc.

V. REFRENCES

[1] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," ,IEEE communication survey & tutorials vol. 17, No. 4 fourth quarter 2015.

[2] Ignor Miladinovic,Sigrid schefer Wenzel "P1-NFV Enabled IoT Architecture for an Operating RoomEnvironment" ,IEEE 2018.

[3] Shulong Wang ,Yibin Hou , Fang Gao and Xinrong Ji "A Novel IoT Access Architecture for Vehicle Monitoring System", IEEE 2016

[4] Pooja Yadav,Ankur Mittal, Dr. Hemant Yadav "IoT:Challenges and Issues in Indian Perspective ", IEEE 2018.

[5] Christopher Coelho, David Coelho, *Marilyn, Wolf,* " An IoT Smart Home Architecture for Long-Term Care of People with Special Needs" ,IEEE 2015.

[6] Ivan Ganchev, Zhanlin Ji, M´airt´ın O'Droma," A Generic IoT Architecture for Smart Cities", ISSC 2014 / CIICT 2014, Limerick, June 26–27 .

[7] Mohammed Abdulaziz Ikram, Mohammad Dahman Alshehri, Farookh Khadeer Hussain," Architecture of an IoT-based System for FootballSupervision", IEEE,2015.