LOW COST IOT SENSOR SYSTEM INDUSTRIAL AUTOMATION USING SYSTEM ON CHIP (SOC)

N.KARTHIKA[1], J. AKSHAYA[2], G. PALLAVI[3], K.NIROJA[4]

ASSISTANT PROFESSOR[1], UG SCHOLAR [2,3&4]

DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN (UGC-AUTONOMOUS)
MAISAMMAGUDA, HYDERABAD-500100

ABSTRACT: Internet of Things (IoT) is rapidly increasing technology. IoT is the network of physical objects or things embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. In this paper, we are developing a system which will automatically monitor the industrial applications and generate Alerts/Alarms or take intelligent decisions using concept of IoT. IoT has given us a promising way to build powerful industrial systems and applications by using wireless devices, Android, and sensors. A main contribution of this review paper is that it summarizes uses of IoT in industries with Artificial Intelligence to monitor and control the Industry. Index Terms— Artificial Intelligence, IoT, Sensors, embedded electronics.

I. INTRODUCTION

In recent years a wide range of industrial IoT applications have been developed and deployed. Evolution of this starts from RFID technology, which allows microchips to transmit the identification information to a reader through wireless communication. By using RFID readers, people can identify, track, and monitor any objects attached with RFID tags automatically. Another technology is the wireless sensor networks (WSNs), which mainly use interconnected intelligent sensors to sense and monitoring. Its applications include environmental monitoring, industrial monitoring, traffic monitoring. Both RFID and WSN are used to develop IoT[1]. Then upcoming technology is IoT with Artificial Intelligent. In previous year, Industry was monitored manually, but this paper introduces Artificial Intelligent to monitor as well as control the Industry autonomously without human intervention.

II. GOALS AND OBJECTIVES To develop a system which will automatically monitor the industrial applications and generate Alerts/Alarms or take intelligent Decision using concept of IoT. And also design the system to Take Intelligent Decision and Control Devices.

III. EXISTING SYSTEM No ways to detect un-even condition in industry. Manual intervention required for monitoring. CCTV used which only monitor but no Alert generation. Alert and their appropriate actions not present manually. Time consuming approach to detect and generate Alert Manually

IV. NEED OF SYSTEM Industry alert are based on manual intervention. Notification for any circumstances in Industry not provided. Appropriate action for this condition taking.

V. OVERVIEW OF SYSTEM In this modern era of automation and advanced computing using IoT with Artificial Intelligence offer promising solutions towards the automation of Industry. In order to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure. This is implemented as in figure1.

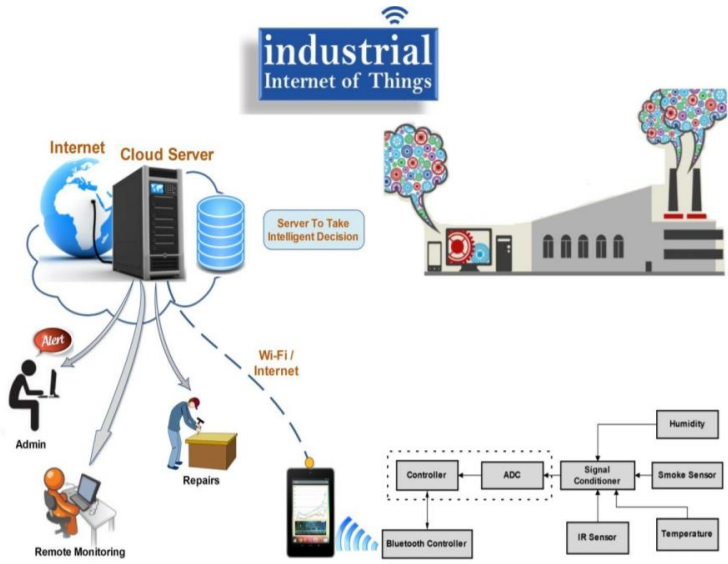

Fig: Block Diagram Of The System

VI.LITERATURE REVIEW:

In "E. A. Lee, "Computing Foundations and Practice for Cyber- Physical Systems:A Preliminary Report," Tech. Rep., 2007. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-72.pdf"

Cyber-Physical Systems (CPS) are integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. There are considerable

challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general-purpose computing. This report examines the potential technical obstacles impeding progress, and in particular raises the question of whether today's computing and networking technologies provide an adequate foundation for CPS. It concludes that it will not be sufficient to improve design processes, raise the level of abstraction, or verify (formally or otherwise) designs that are built on today's abstractions. To realize the full potential of CPS, we will have to rebuild computing and networking abstractions. These abstractions will have to embrace physical dynamics and computation in a unified way. Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. In the physical world, the passage of time is inexorable and concurrency is intrinsic. Neither of these properties is present in today's computing and networking abstractions. This report examines this mismatch of abstractions. Applications of CPS arguably have the potential to dwarf the 20-th century IT revolution. They include high confidence medical devices and systems, assisted living, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, critical infrastructure control (electric power, water resources, and communications systems for example), distributed robotics (telepresence, telemedicine), defense systems, manufacturing, and smart structures. It is easy to envision new capabilities, such as distributed micro power generation coupled into the power grid, where timing precision and security issues loom large. Transportation systems could benefit considerably from better embedded intelligence in automobiles, which could improve safety and efficiency. Networked autonomous vehicles could dramatically enhance the effectiveness of our military and could offer substantially more effective disaster recovery techniques. Networked building control systems (such as HVAC and lighting) could significantly improve energy efficiency and demand variability, reducing our dependence on fossil fuels and our greenhouse gas emissions. In communications, cognitive radio could benefit enormously from distributed consensus about available bandwidth and

from distributed control technologies. Financial networks could be dramatically changed by precision timing. Large scale services systems leveraging RFID and other technologies for tracking of goods and services could acquire the nature of distributed real-time control systems. Distributed real-time games that integrate sensors and actuators could change the (relatively passive) nature of on-line social interactions. Tight integration of physical devices and distributed computing could make "programmable matter" a reality. The positive economic impact of any one of these applications areas would be enormous. Today's computing and networking technologies, however, may have properties that unnecessarily impede progress towards these applications. For example, the lack of temporal semantics and adequate concurrency models in computing, and today's "best effort" networking technologies make predictable and reliable real-time performance difficult, at best. Many of these applications may not be achievable without substantial changes in the core abstractions.

If the US fails to lead the development of these applications, we would almost certainly find our economic and military leadership position compromised. To prevent that from happening, this report will identify the potential disruptive technologies and recommend research investments to ensure that if such technologies are successfully developed, that they are developed in the US.

IN "R. R. RAJKUMAR, I. LEE, L. SHA, AND J. STANKOVIC, "CYBER-PHYSICAL SYSTEMS," IN PROCEEDINGS OF THE 47TH DESIGN AUTOMATION CONFERENCE - DAC'10. NEW YORK, USA: ACM PRESS, 2010, P. 731. [ONLINE].AVAILABLE:HTTP://PORTAL.ACM.ORG/CITATION.CFM?DOID=1837274.1837461"

Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Just as the internet transformed how humans interact with one another, cyber-physical systems will transform how we interact with the physical world around us. Many grand challenges await in the economically vital domains of transportation, health-care, manufacturing, agriculture, energy, defense, aerospace and buildings. The design, construction and verification of cyber-physical systems pose a multitude of technical challenges that must be

addressed by a cross-disciplinary community of researchers and educators.

IN "THE INDUSTRIAL INTERNET OF THINGS (IIOT): AN ANALYSIS FRAMEWORK" Historically, Industrial Automation and Control Systems (IACS) were largely isolated from conventional digital networks such as enterprise ICT environments. Where connectivity was required, a zoned architecture was adopted, with firewalls and/or demilitarized zones used to protect the core control system components. The adoption and deployment of 'Internet of Things' (IoT) technologies is leading to architectural changes to IACS, including greater connectivity to industrial systems. This paper reviews what is meant by Industrial IoT (IIoT) and relationships to concepts such as cyber-physical systems and Industry 4.0. The paper develops a definition of IIoT and analyses related partial IoT taxonomies. It develops an analysis framework for IIoT that can be used to enumerate and characterise IIoT devices when studying system architectures and analysing security threats and vulnerabilities. The concept of Industrial Automation and Control Systems (IACS) is well established. These systems, often referred to as Operational Technology (OT), are employed in diverse industries including manufacturing, transportation and utilities, and are sometimes referred to as cyber-physical systems (CPS). Since the term Internet of Things (IoT) [1] was first used in 1999, it has been applied to connected devices in consumer, domestic, business and industrial settings [2]. Although there is a significant amount of literature attempting to define IoT, its uses, and its typical components, it is rarely made obvious how any of this applies in the industrial setting. Because current definitions of IoT invariably imply a similar approach to the high-level architecture of a system, the ubiquitous use of the term IoT to refer to the use of digital technologies in industry is unhelpful as it hinders the analysis of alternative system architectures, including the location and nature of the data or information processing, and associated performance and security issues. The aims of this paper are to improve on existing definitions of Industrial IoT (IIoT) and to propose a framework for IIoT components as a basis for analysing the use and deployment of IoT technologies in industrial settings. In undertaking this research our aim was to establish a framework that allows us to analyse the nature of IIoT devices and their uses, which is to be used as part of a vulnerability and threat analysis process for these devices. By being able to

characterise the devices in a systematic manner, we anticipate being able to analyse cross-cutting threats and vulnerabilities and identify patterns that may be obscured when focusing on the technology employed or sector specific issues. Whilst researching IIoT we have reviewed a wide range of academic literature and found that when combining the search terms: ("Industrial Machines" OR "Industrial Systems") AND "Internet" OR ("Industrial Internet") AND "Machines"

The following terms were amongst those most regularly found:
Cyber Physical Systems (CPS), Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Industrial Internet. Although not an exhaustive list, it does represent the most commonly used terms in both academic and relevant non-academic literature, for white\ papers and corporate blogs. In the rest of this section we define Industry 4.0 and review the above terms before moving on to develop our definition of IIoT and the taxonomy.

INDUSTRY 4.0

The first three industrial revolutions are characterised as being driven by mechanical production relying on water and steam power, use of mass labour and electrical energy, and the use of electronic, automated production respectively [3]. Whilst the supposed fourth industrial revolution ('Industry 4.0') was first proposed in 2011 in the context of the goal of developing the German economy [4]. This revolution is characterised by its reliance on the use of CPS capable of communication with one another and of making autonomous, de-centralised decisions, with the aim of increasing industrial efficiency, productivity, safety, and transparency. There is a considerable overlap between the concept of Industry 4.0 developed in Germany and the Industrial Internet concept (see 2.6), which originated in the United States. The definition of the latter now encompasses change for both business and individuals: "…the industrial internet is an internet of things, machines, computers and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes, and it is redefining the landscape for business and individuals alike" [5]. A definition of 'Industrie 4.0′ a term which, in its English cognate, the authors treat as synonymous with IIoT, is: "…we define Industrie 4.0 as

follows: Industrie 4.0 is a collective term for technologies and concepts of value chain organisation. Within the modular structured Smart Factories of Industrie 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicate and cooperate with each other and humans in real time. Via the IoS [Internet of Services], both internal and cross- organizational services are offered and utilised by participants of the value chain." [6]

CYBER-PHYSICAL SYSTEMS (CPS)

Whilst there are a number of definitions of CPS [7], [8], [9], [10], [11], this paper uses: "A system comprising a set of interacting physical and digital components, which may be centralised or distributed, that provides a combination of sensing, control, computation and networking functions, to influence outcomes in the real world through physical processes." [12] What sets CPS apart from more conventional information and communications systems (IT or ICT) is the real-time character of their interactions with the physical world. Whilst both CPS and ICT systems process data and/or information, the focus of CPS is on the control of physical processes. CPS use sensors to receive information about, including measurements of, physical parameters, and actuators to engage in control over physical processes. CPS often involve a large degree of autonomy. For example, CPS often have the capacity to determine whether to change the state of an actuator or to draw a human operator's attention to some feature of the environment being sensed.

INDUSTRIAL AUTOMATION & CONTROL SYSTEMS (IACS)

IACS or ICS is a collective term typically used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Descriptions of ICS from authoritative American and European organisations are respectively: "Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Many ICS components were in physically secured areas and the components were not connected to IT networks or systems. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions" [13]; and "Today ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable

modems, and they often use commercial off-the shelf software" and "command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA" [14].

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

SCADA has been described as: A system that allows an operator, in a location central to a widely distributed process, such as an oil or gas field, pipeline system, or hydroelectric generating complex, to make set point changes on distant process controllers, to open or close valves or switches, to monitor alarms, and to gather measurement information [15]; Similar to a Distributed Control System with the exception of sub-control systems being geographically dispersed over large areas and accessed using Remote Terminal Servers [16]. Where a Distributed Control System (DCS) is a supervisory control system typically controls and monitors set points to sub-controllers distributed geographically throughout a factory [17]; and SCADA applications are made up of two elements: the process/system/machinery you want to monitor and control, which can take the form of a power plant, a water system, a network or a system of traffic lights; and a network of intelligent devices that interface with the first system through sensors and control outputs. This network, which is the platform system, provides the capability to measure and control specific elements of the first system [18]. The nature of SCADA has led to conflicting views as to whether it forms part of the IIoT ecosystem. For example, discussion of SCADA system forensic analysis within IIoT [19] contrasts with a view that SCADA is simply the predecessor to IIoT especially as SCADA systems have evolved to connect to the internet but do not have the analytics and level of connectivity that is found in IIoT [20].

INDUSTRIAL INTERNET

The concept of an Industrial Internet was first articulated by General Electric (GE) [21], and described as: "The definition of the Industrial Internet includes two key components: The connection of industrial machine sensors and actuators to local processing and to the Internet; The onward connection to other important industrial networks that can independently generate value. The main difference between the consumer/social Internets and the Industrial Internet is in how and how much value is created. For consumer/social Internets, the majority of value is created from advertisements" [22]. This description clearly separates the Internet and the Industrial Internet, although in both cases the function of the Internet is to

provide the wide area networking. More recently the Industrial Internet has been defined as:

"… a source of both operational efficiency and innovation that is the outcome of a compelling recipe of technology developments [sic]. The resulting sum of those parts gives you the Industrial Internet—the tight integration of the physical and digital worlds. The Industrial Internet enables companies to use sensors, software, machine-to-machine learning and other technologies to gather and analyse data from physical objects or other large data streams—and then use those analyses to manage operations and in some cases to offer new, value-added services" [23].

From this definition, it is apparent that the authors consider a key component of the Industrial Internet to be the ability to analyse data, which is corroborated by a statement later in their report, in which it is stated that "…Big Data analytics is the foundation of the Industrial Internet…". This desire to collect and analyses data is a feature in common with Industry 4.0.

IN "INDUSTRIAL AUTOMATION USING IOT": Internet of things(ioT) is rapidly incresasing technology.IOT is the network of physical objects or things embeded with electronic software, sensors, and network connectivity which enables these objects to collect and exchange data. In this paper, we are developing a system which will automatically monitor the industrial applications and generate Alerts/Alarms or take intelligent decisions using concept of IoT. Safety from leaking of raw gas and fire are the most important requirements of home and industries security system for people. A traditional security system gives the signals in terms of alarm. Automation is one of the incerasing need with in industries as well as for domsatic applications.Automatio reduces the human effords by replacing the human effords by system which are self operated, The Intenet is one way of he growing platfrom for automation,through which new advancedment are made through which on easily monitor as well control the system using internet.As we are making use of Internet the system becomes secured and live data monitoring is also possible using IoT sysytem. Within industries the various hazardous gas are being processed, hence to provide security to those employ working within those industreis, it becomes important issue to work on their security,If leakage of gas takes place then these system alerts by turning ON alram which notifies the employers. This system also helps us take some crucial decision from any point of

the world within internet network.Wifi shield is being used to act as service point between network and connecting network Industrial Automation Using Internet of Things (IOT) In this paper, they are developing a system which will automatically monitor the industrial applications and generate Alerts/Alarms or take intelligent decisions using concept of IoT.[1]. RASPBERRY PI AND IOT BASED INDUSTRIAL AUTOMATION . IOT is achieved by using local networking standards and remotely controlling and monitoring industrial device parameters by using Raspberry Pi and Embedded web server Technology. Raspberry Pi module consists of ARM11 processor and Real Time Operating system whereas embedded web server technology is the combination of embedded device and Internet technology .Using embedded web server along with raspberry pi it is possible to monitor and control industrial devices remotely by using local internet browser.[2] A REVIEW ON INDUSTRIAL AUTOMATION USING IOT.They have developed new technologies that have allowed us to move from the First generation of the Internet into the current transition into the Fourth generation. This generation has been propelled by the concept of the Internet of Things (IoT). [3] IOT BASED AUTOMATED TEMPERATURE AND HUMIDITY MONITORING AND CONTROL In this paper, a raspberry pi running with Linux OS coded with C++ program that retrieves the temperature as well as humidity readings and these values are sensed and sent to the internet. [4] I NDUSTRIAL TEMPERATURE MONITORING AND CONTROL SYSTEM THROUGH ETHERNET LAN This paper presents a PC based temperature monitoring and control system using virtual instrumentation, LabVIEW. Data acquisition is an important role in industry in order to ensure the quality of service. Temperature sensor measures the temperature and produce corresponding analog signal which is further processed by the microcontroller. The simulator acquires data from the microcontroller through Ethernet port. The data will be displayed on the LCD in microcontroller and PC monitor. Automation and control can be done with the help of control circuitry

IN “L. HU, N. XIE, Z. KUANG, AND K. ZHAO, “REVIEW OF CYBER-PHYSICAL SYSTEM ARCHITECTURE,” IN 2012 IEEE 15TH INTERNATIONAL SYMPOSIUM ON OBJECT/COMPONENT/SERVICE-ORIENTED REAL-TIME

DISTRIBUTED COMPUTING WORKSHOPS. IEEE, 2012, PP. 25–30. [ONLINE]. AVAILABLE: HTTP: //IEEEXPLORE.IEEE.ORG/LPDOCS/ EPIC03/WRAPPER.HTM?ARNUMBER=6196100"

With the goal of accomplish the ubiquitous intelligence in social life, Cyber-Physical Systems (CPS) are getting growing attentions of researchers and engineers. However, the complexity of computing and physical dynamics bring a lot of challenges in the development of CPS, such as integration of heterogeneous physical devices, system verification, security assurance, and so on. A general or unified architecture plays an important part in the process of CPS design. In this paper, we review the current and previous works of CPS architecture, and introduce the main challenges and techniques of architecture development : real-time control, security assurance, integration mechanism. Then we propose a general CPS architecture based on Service-Oriented Architecture (SOA), the main advantage of this proposed architecture is the integration flexibility of services and components. At the end, we introduce the typical applications of CPS, and suggest the future research areas. There is no unified concept of Cyber-Physical Systems (CPS). Generally, CPS is defined as the fuse of cyber world and the dynamic physical world. CPS perceive the physical world, process the data by computers, and affect and change the physical world. He JiFeng presented the concepts of "3C":Computation, Communication, and Control. With "information" as the center, fusion the computation and communication and control, to achieve the real-time sensing, dynamic control and information service in large scale systems[1]. CPS have close relationships with embedded systems, sensors,and wireless network, but have their own characteristics, for example, the complexity and dynamics of environment, the big problem space and solution space are closely related with the environment, the requirement for high reliability of the system. In the early stage, CPS had a two-tier structure inherently, the physical part and computing part. The physical part sense the physical environment, collect data, and execute the decision made by the computing part; the computing part analyze and process the data from the physical part, and then make decision. This is a kind of feedback control relation of the two parts. In [2], Hyun Jung La et al. proposed a 3-Tiers architecture of CPS : Environmental Tiers: consists of physical devices and a target environment which includes end-users using the devices and

their associated physical environment. Service Tiers: a typical computing environment with services in SOA and CC (Cloud Computering).

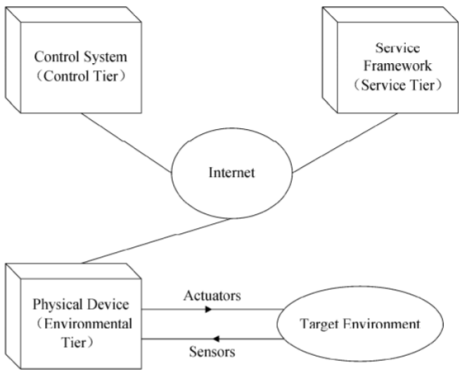

Fig: The three tiers of CPS architecture

Cyber world and physical world are different essentially, but they are connected and affect each other by information. One of the main features of physical world is dynamic, the same entity at different time showed different properties. Therefore, when modeling the physical world entities, the dynamic features should be considered in particular. In the cyber world, changes are represented by state transitions, thus, simulating the physical world may lead to state explosion. This is an important feature to be considered in the modeling and design process of CPS. As the base of CPS research, architecure is very important, but currently, there were no unified framework or general architecture can be used in most applications. In this paper, we review the developments of CPS from the architecture aspects. Based on this, in section 3, a general architecture is proposed based on SOA. This architecture extends the traditional concept of SOA, and introduce it in CPS architecture design. In the 4th section of this article, typical applications of CPS will be introduced. Finally, we discuss the current problems in CPS research, and give future research directions

IMPLEMENTATION:

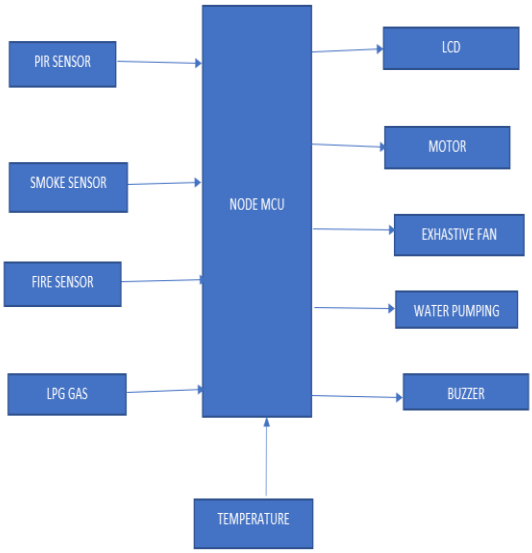

Fig: Block Diagram Of Smart Sensor SoC Architecture For The Industrial Internet Of Things

Sensors (Pir Sensor, Smoke Sensor, Fire Sensor, Lpg) are used to percept the environment and object conditions. Analog signal are provided to android device produced by sensors. Admin set threshold to every sensors placed in Industry. Android check this threshold against

incoming analog signal. When it encounter an uneven condition devices (Buzzer, Alarm, motor, fan) are use to take accurate measures such as Alarm/Alert are generated, it send messages and email to Admin. Then with the help of Artificial Intelligent it takes

APPLICATIONS

Industry and office:-We can implement sensors in wide area over the machines and instruments. Control and Monitor circumstances by using concept of Artificial Intelligence and IoT.

Hospital and Labs: -We can plot sensors on patient's body and Doctor can check current status on his android phone and also take necessary actions and decisions.

Home:-We can implement sensors to household appliances and monitor and control with the help of Artificial Intelligence.

CHALLENGES TO OVERCOME Wi-Fi/Internet Connection is fluctuating which may create problems. SMS/Email Alerts has to send but may have range problem. Decision Making is very difficult as this is question of many life & industry. Wrong tool Selection for Development

CONCLUSION Nowadays we need everything computerized. Earlier we can only monitor the situations with the help of cameras. In industries to reduce manual overhead we have implemented Internet of Things (IoT) in Industry to monitor as well as to inform the responsible person to take appropriate measures, but this will partially fulfill our requirement. As sometimes it will be late in this process and it will harm to property as well as life. For this purpose we are developing a system for Industrial Automation using IoT with the help of Artificial Intelligence to make system automated which will take intelligent decisions.

REFERENCES

[1] Li Da Zu" Internet of Things in Industries: A Survey" IEEE Transactions on Industrial Informatics, vol. 10, no. 4, November 2014

[2] Sadeque Reza Khan Professor Dr. M. S. Bhat "GUI Based Industrial Monitoring and Control System ``IEEE paper, 2014

[3] Ayman Sleman and Reinhard Moeller ``Integration of Wireless Sensor Network Services into other Home and Industrial networks "IEEE paper

[4] Rajeev Piyare and Seong Ro Lee`` Smart Home-Control and Monitoring System Using Smart Phone '' ICCA 2013, ASTL Vol. 24, pp. 83 - 86, 2013 © SERSC 2013

[5] Jinsoo Han, Chang-Sic Choi, Wan-Ki Park, Ilwoo Lee Green home energy management system through comparison of energy usage between the same kinds of home appliances 2011 IEEE 15th International Symposium on Consumer Electronics

[6] S.d.t. Kelly, n.k. Suryadevara and S.C. Mukhopadhyay Towards the Implementation of IoT for Environmental Condition Monitoring in Homes,IEEE Paper 2013

[7] Jinsung Byun, Insung Hong, Byoungjoo Lee, and Sehyun Park, Member Intelligent Household LED Lighting System Considering Energy Efficiency and User Satisfaction,IEEE paper February 2013

[8] Gopinath Shanmuga Sundaram, Bhanuprasad Patibandala, Harish Santhanam Bluetooth Communication using a Touchscreen Interface with the Raspberry Pi 978-1- 4799-0053-4/13/31.00 2013 IEEE