IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IOT FOR INDUSTRIAL APPLICATION: SURVEY

[1]Shamal Sonawane,

[1]Assistant professor,
[1]Electronics Department,
[1]Dr. D. Y. Patil ACS College Pimpri, Pune, India

Abstract: With the rapid development of Internet-of-Things (IoT), wireless sensor networks (WSNs) are giving importance in the continued advancement of information and communication technologies, and have been connected and integrated with the Internet in vast industrial applications. Internet of Things (IoT) has given a good opportunity to construct industrial systems and applications by exploiting of radio-frequency identification (RFID), and wireless communications, sensor devices and mobile. A wide scope of modern IoT applications have been developed and deployed in recent years. To understand the development of IoT in industries, this seminar reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and challenges. Also propose a system which will automatically monitor industrial applications and generate alarms or take intelligent decisions using concept of IoT.

Index Terms - **Radio frequency identification (RFID), Wireless sensor networks (WSNs), Industrial automation, Internet of things (IoT).**

I. Introduction

As a rising innovation, the Internet of Things(IoT) is relied upon to offer promising solutions to change the activity and job of many existing industrial systems such as transportation systems and manufacturing systems. For example, when IoT is used for creating intelligent transportation systems the transportation authority will have the option to follow each vehicle's current location, monitor its movement, and anticipate its future area and conceivable street traffic. The term IoT was initially proposed to refer to uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology [1]. Later on, scientists relate IoT with more technologies for example sensors, actuators, GPS gadgets, and cell phones. Today, a generally acknowledged definition for IoT is a unique worldwide system infrastructure with self concurring capabilities based on standard and interoperable communication protocols where physical and virtual `Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.

So far, IoT has been picking up fascination in industry, for example logistics, manufacturing, retailing, and pharmaceutics. With the rapid improvements in wireless communication, smart phone, and sensor network technologies, number of networked things or smart objects are being involved in IoT. As a result, these IoT-related technologies had an enormous effect on new information and communications technology (ICT) and enterprise systems technologies. In order to provide high-quality services to end users, IoT's technical standards need to be designed to define the specification for information exchange, processing, and communications between things. The success of IoT depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale.

IoT aims to connect different things over the networks. As a key technology in integrating heterogeneous systems or devices, System Oriented Architecture (SOA) can be applied to support IoT. SOA has been effectively utilized in research areas such as cloud computing, Wireless Sensor Networks, vehicular system. Many thoughts have been proposed to make multi-layer SOA architectures for IoT based on the selected technology, business needs, and technical requirements. Fig.1 shows an SOA, where the four layers interact to each other. The architectural design of IoT is concerned with architecture styles, communication and networking, smart devices, Web applications, business models and corresponding process, cooperative data processing, security, etc. From the technology perspective, the design of IoT architecture needs to consider extensibility, scalability, modularity, and interoperability among heterogeneous devices. As things might move or need real-time communication with their environment, an versatile design is needed to help devices dynamically interact with other things. The decentralized and heterogeneous nature of IoT requires that the architecture provides IoT efficient event-driven capability. Thus, SOA is considered a good approach to achieve interoperability between heterogeneous devices in a multitude of way.

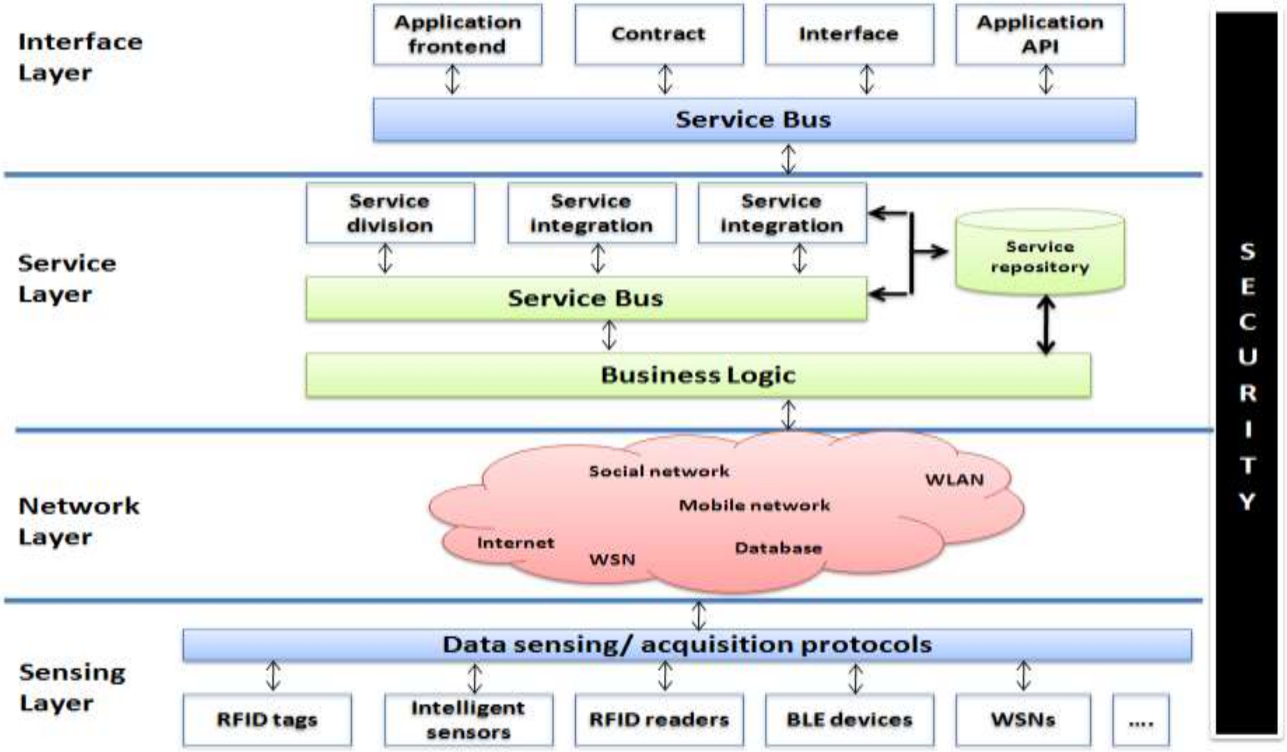

Fig-1 SOA for IoT

II. IoT Challenges in Industrial Automation

Consumer IoT and Industrial IoT have similarity in many faculties, however there are key differences that are reflected in specific real-time and deterministic requirements of industrial IoT applications, we will firstly present general IoT challenges .

Data and service security

Large-scale applications and services based on IoT are increasingly vulnerable to disruption from attack or information theft because having more devices, systems, and technologies connected leads to more decentralized entry points for these security disruptions. As unavailability of service or data can have severe impact on the customer businesses, it is important to provide security mechanisms to increase the level of data protection and security for messages communication between devices as well as from devices (e.g., sensors, actuators, etc.).To the cloud platform to ensure service continuity and required Quality-of-Service (qos).

Trust, data integrity and information privacy

The interconnected devices and the users of the system need to have confidence that the information and services being exchanged can be relied upon. Therefore, trust mechanisms need to be able to deal with humans and machines to ensure trustworthy access to data and proper authorization of service. Moreover, it is essential with assured, proper, and consistent collection, processing, communication, use and disposition of sensitive information and personally identifiable information throughout the whole chain from devices, the edge of the network, and to the cloud. This includes protecting user resources and data from unauthorized access that may compromise their integral and confidentiality. Building a trusted and fault tolerant system in the IoT context requires taking into account how to protect communications, how to ensure integrity and confidentiality of data in the system, and how to manage authentication and access control to resources in systems that consist of thousands of devices.

Scalability

This challenge is reflected in different aspects, including: (i) naming and addressing the scalability of the device address of the existing network must be sustainable; (ii) data communication and networking the connection of new networks and devices should not jeopardize the performance of existing networks, devices, and data transmission despite the high level of interconnection among a large number of devices and system components; and (iii) service provisioning and management due to the massive number of services/service execution options available and the need to handle heterogeneous resources.

Interoperability

Industry is dominated by proprietary interfaces and solutions. The amount of devices and system components from different vendors and different domains poses challenges in terms of multiple platforms, numerous protocols and large numbers of apis. According to, the vast variety of devices, applications, and implementations within the industrial IoT will result in a massively heterogeneous set of data with variation in format and interpretation of data, quality, frequency, and timing of the data. Therefore, interoperability is an important aspect that needs to be considered in IoT solutions so that diverse devices and systems can share information and interact with each other.

III. LITERATURE SURVEY

Li Da Xu et.al [1] describes that IoT incorporates different devices equipped with sensing, identification, processing, communication, and networking capabilities. In particular, sensors and actuators are getting progressively powerful, more affordable and smaller, which makes their utilize universal. Industries have strong interest in deploying IoT devices to develop industrial applications such as automated monitoring, control, management, and maintenance.

Zhengguo shenget et.al [2] introduced the IoT ecosystem and key technologies to support IoT communications, and described the essential management mechanisms for IoT system. Specifically, they have introduced a cross layer design of a lightweight and scalable restful web service based infrastructure to enable efficient and reliable management of wireless sensor networks.

M. Wollschlaeger et.al [3] with the introduction of the Internet of Things (IoT) and cyber-physical system (CPS) concepts in automation is undergoing a tremendous change. This is made possible in part by recent advances in technology that allow interconnection on a wider and more fine-grained scale. The purpose of this article is to review technological trends and the impact.

J.Wan et.al [4] In particular, they analyzed software-defined iot architecture to determine network resource allocation and accelerate information exchange mechanisms through an easily customizable networking protocol. In this paper also discussed the existing problems and possible solutions for software defined iot.

Naresh Ganesh Nayak et.al [5] In a bid to satisfy such requirements, modern manufacturing systems, comprising innumerable cyber-physical systems (CPS), aim to be reconfigurable. CPS implement production processes through an ICT infrastructure networked with sensors and actuators embedded in the shop floor. Reconfigurability, in context of manufacturing systems, must include the entire system of networked components and hence requires a flexible ICT infrastructure. Providing flexible ICT infrastructures, often, comes at the cost of diluted quality of service (qos) guarantees. This, however, is not an option for manufacturing systems, most of which require strict qos guarantees to function correctly.

IV. INDUSTRIAL AUTOMATION USING INTERNET OF THINGS (IOT)

Industrial Internet of Things (IoT) is the best way of connecting industrial machineries and sensors, to each other, over the internet, allowing the authorized user of the industry to use information from these connected devices to process the obtained data in a useful way. IoT-connected applications typically support data acquisition, aggregation, analysis, and visualization. The IoT architecture includes latest technologies such as computers, intelligent devices, wired and wireless communication and cloud computing. Previously Bluetooth and RF (Radio Frequency) technologies were used to control and monitor the industrial applications but were limited to short distance. The operator had to be in the range of the Bluetooth connectivity or in the Radio Frequency area.

Proposed system

Here we are using a microcontroller (Atmega) to make the necessary commands. We are monitoring 3 parameters Voltage, Temperature and oil level check. Respective sensors for the different parameters are used to obtain their values. Voltage sensor, Temperature sensor (LM35) and Oil level check (Monostable multivibrator). Once the values are obtained, it is given to the microcontroller. The microcontroller compares the obtained values with the predefined safe values so that it does not exceeds the safe values. If the obtained value exceeds the safe value, the application (for example a motor) is turned o (in case if voltage exceeds the safe value) or the application (for example a cooling fan) is turned on (if temperature exceeds the safe values). Thus, controlling is done automatically. We are also using a Wi-Fi module (ESP8266) which transmits the data periodically to the cloud from which user can extract the data. The below block diagram (Fig. 2) represents the block diagram for IoT based industrial automation.

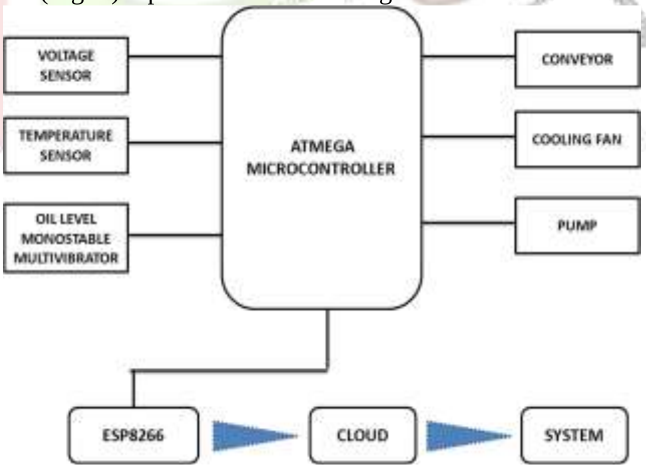

Fig-2 Block diagram of IoT based industrial automation

Advantages

- Long distance controlling and monitoring is possible.
- Faster production and cheaper labour cost.
- Can perform the task beyond the human capability.

Applications

- Home applications: we can monitor and control the home things like fans, TV, fridge etc. by artificial intelligence.
- Industries and offices: monitoring and controlling the machines and instruments using the IoT technique
- Hospitals and labs: doctor can check the current status of the patient's body using his android phone by placing the sensors on patient's body using the artificial intelligence and IoT

V. CONCLUSION

As a complex digital physical framework, IoT incorporates different gadgets outfitted with detecting, identification processing, communication, and networking capabilities. In particular, sensors and actuators are getting increasingly powerful, less expensive and smaller, which makes their use ubiquitous. Industries have solid enthusiasm in deploying IoT devices to develop industrial applications such as automated monitoring, control, management, and maintenance. Due to the rapid advances in technology and industrial infrastructure, IoT is expected to be widely applied to industries. This paper reviews the recent researches on IoT from the industrial perspective.

REFERENCES

[1] L. D. Xu, W. He and S. Li, “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, vol. 10 no. 4, pp. 2233-2243, Nov. 2014.

[2] Z. Sheng, C. Mahapatra, C. Zhu and V. C. M. Leung, “Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT,” IEEE Access, vol. 3, pp. 622-637, 2015.

[3] M. Wollschlaeger, T. Sauter and J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17-27, March 2017.

[4] J. Wan, “Software-Dened Industrial Internet of Things in the Context of Industry 4.0rq” IEEE Sensors Journal, vol. 16, no. 20, pp. 7373-7380, Oct.15, 2016.

[5] Naresh Ganesh Nayak and Christoulakis and K. Thramboulidis, “IoT Based integration of IEC 61131 industrial automation systems: The case of UML4IoT,” IEEE 25th International Symposium on Industrial Electronics (ISIE), Santa Clara, CA, pp. 322-327,2016.