Surveillance in Nuclear Power Plant using Internet of Things

Gopikrishnan S, Priakanth P, Jothiprakash V

Abstract: ***A nuclear power plant is kind of power station that generates the electricity by nuclear reactor. As like thermal power plants, in these nuclear power plants heat energy is used to generate the steam to drive the turbine which is connected to power generator to produce energy. But the heat energy has been produced by the nuclear reactor. On routine process of this type of nuclear power plant operations, the discharge of radioactive effluents from nuclear reactor causes hazardous impacts on its environment and affects the normal life of human beings, animals and plants. Hence it is essential to monitor the nuclear power plant and control the valves and devices to ensure the safety of the environment. Even many safety measures has already implemented at the power plant, the facility of monitoring and controlling from the remote location is better because the operator can be isolated from the environment. This requirement leads to the use of Internet of Things technology in monitoring and controlling the entire plant from remote location through internet. This research proposed a IoT based nuclear power plant monitoring system with security features to enhance the safety of nuclear power plants.***

Keywords: Internet of Things, Monitoring, Controlling, Nuclear Power Plant, Remote Location.

I. INTRODUCTION

In the nuclear power plant, you have a lot of things that need to be monitored. Prevention of entry to prohibited area and damages to the various equipments must be monitored to avoid dangerous situations. The day to day operations of the nuclear power plants produces diminutive amount of radioactive gases and liquids due to its nuclear reaction operation to the atmosphere under controlled and monitored conditions. Because of these radioactive discharges the environment has been polluted with hazardous which affects the normal life of living things in it. Hence it is essential to ensure the safety of the environment from these harmful gases and liquids. As new risks emerge, governments are calling for higher level of security at the plants in order to reinforce the protection of the environment. It will be easy if a provision is made for monitoring the entire plant 24/7 from a remote location. Various wireless technologies like GSM, Zigbee and RFID are already available with certain degree of flexibility. The main disadvantage in these techniques is less security and limited availability.

Revised Manuscript Received on March 08, 2019.

Gopikrishnan S, Department of IT, Karpagam College of Engineering, Coimbatore, India,

Priakanth P, Professor & Head, Department of CT-UG, Kongu Engineering College,

Jothiprakash V, Department of IT, Karpagam College of Engineering, Coimbatore, India,

Internet being a worldwide available high speed network, it can be used to transmit the data securely. So, implementing the concept of Internet of Things for monitoring the plant and controlling safety valves and other equipments may be the effective solution. IoT allows the operator to monitor various parameters and control various actuators from the remote location using a Mobile application or a Web Interface after connecting using the Static IP address, User Name and Password. The secure communication will be established using SSH protocol.

Internet of Things

The Internet of Things (IoT) is the network of smart devices which contains sensors and actuators to collect, communicate and control the environment [1]. This IoT has been applied and used in many innovative applications. The process of IoT consists of three stages. The data collection part about the environment in an IoT network has been done with the help of variety of sensors. Once the data has been collected, the second phase communicates these information to the computing device through internet for efficient and fast data processing. Based on the processed data, the reactive decisions will be made by the computing device and that decision will be communicated to the actuators. Depending upon the decision the actuator will control the environment in the third phase of IoT.

As discussed in [2], a smart environment must use information and communication technologies to make the unpleasant situations into safe and secure. Here the application which is considered should be enhanced with smart technologies like IoT. A nuclear power plant can adapt IoT infrastructure to make it smart environment. The detail discussion about this IoT implementation in nuclear power plant has been discussed in third section.

SSH Protocol

Even an IoT enabled nuclear power plant makes the power plant environment smart and ensures the safety, the security part of the IoT infrastructure must deal with at most care. The high sensitive applications like nuclear power plants, national border security and medical applications require high security in the form of confidentiality, authentication and integrity. On this necessity the secure shell (SSH) protocol has been implemented in IoT communication module. SSH is a transport layer protocol which provides the authentication in the form of remote and biometric server login and it provides confidentiality by adapting any crypto algorithms at data integration phase. Finally it ensures the integrity through internet computing by encrypted MAC headers.

In this proposed model, the SSH protocol has been used as

transport layer protocol to ensure the security features of the nuclear power plant. It implements the SSH algorithm along with sensor and actuators' embedded code and decrypts at the computation engine created at the cloud.

II. LITERATURE SURVEY

Various literatures that explain the implementation of loT technology in various fields, loT architecture, requirements and security improvements have been studied

Liang He et al. [2] provided a brief description for optimization of sensor nodes for reducing the power requirements Deployment of thousands of wireless sensors in an appropriate pattern will simultaneously satisfy the application requirements and reduce the sensor network energy consumption The model in this article makes use of historical data and current data from other sensors to relatively accurately predict a sensors temperature with an average prediction accuracy of 97.0%.

An IoT based new framework for health monitoring has been proposed in [3]. The main objective of this model is to utilize the IoT capabilities to create an interconnected smart devices network for custom made healthcare application in the hospital environment. It proposed a Ubiquitous and Mobile Integrated Clinical Environment platform to provide large scale connectivity with different physiological sensors as well as integration with cloud information systems. Even this model is optimal and secure it can be implemented and successful in PAN and LAN.

Fagen Li and Pan Xiong [4] proposed a secure wireless technology for connecting multiple sensors to the IoT based control unit. This model resolves the security issues between a sensor node and IoT sink node through a signcryption scheme for online and offline heterogeneous networks. It proposed a secure channel between two nodes that supports all the security parameters like authentication, confidentiality and integrity with non-repudiation services. This model is well in security aspects. But the intermediate channel which is implemented in this model makes more delay in data communication to the IoT application layer.

An usual way that how humans can communicate with the internet, the same way the devices are also made to communicate with internet in the model proposed in [5]. This model is very effective in terms of identifying and getting services from the existing network for the IoT application. Even this way of connecting and communicating devices is efficient, the secure network like nuclear power plant should not allow and accept unauthorized node into the network.

Luigi Atrori et al. [6] have proposed a novel framework to improve the security in IoT based social applications. The authors have enhanced their security model in three levels. In the first stage the sensor devices will share the information to the social network of humans. In the second stage, the information can interact with the humans in the social network through application layer. In the third stage the new communication network has been build based on the social interaction. This model ensures the security to involve the new nodes to build a new communication network. But the IoT based nuclear power plant must be implemented in its own authorized, secure network.

Andrea Zanolla et. al [7] have proposed a new IoT framework for smart city applications. Due to different nature of applications implementing a general architecture for IoT is difficult process. But the proposed model in [7] failed to considers the all the types of smart devices, link layer protocols and application layer services. This reduces their scope of framework in applying all smart city applications. More over this model considers only with collection and communication techniques. But the application which is considered in this paper requires control over the power plant.

Zhuming Bi et al [8] proposed a new method for applying the loT in industrial manufacturing. The major object of this method is to apply the IoT features into modem manufacturing unit and investigate its performance compared with manual operation of modem manufacturing. Based on their work, the authors have proved that the emerging IoT infrastructure can support information systems of next generation manufacturing enterprises (Industry 4.0) in an efficient way. It opens extensive way to apply IoT to identify, measure, track and monitor environments with smart objects. This article supports and added strength to our proposed system to apply IoT into nuclear power plant.

The article which is proposed by Shanzhi Chen et al [9] describes the application and challenges in implementing IoT for real time applications. Further it discusses about how machine to machine communications can be done through information sensing devices and communication protocols in IoT networks. This model gives the possible ways to use IoT in machine to machine communication, machine to human and human to machine communication and mobile to machine communication. By understanding the base of this mode, the proposed has been implemented as IoT based surveillance in nuclear power plant monitoring.

III. SYSTEM MODEL

Methodology

As discussed in the previous section, many applications has been implemented and deployed based on Internet of Things. So the theoretical aspects of the proposed model do not required to be elaborated. This section describes in detail about the implementation and deployment of the project. The proposed system uses a Raspberry Pi board as a centralized unit. Internet connection is essential and it can be provided through a LAN cable or Wi Fi adapter. Here we have implemented the proposed model with mobile hotspot. The platform for the client application can be a mobile phone or a web page. Since this application can be monitored by the people who are in control room and also outside superiors, the implementation has been done at both mobile and web application. A user name, Password and an IP address are essential for login into the application. Since this application involves high sensitive information, user authentication is essential. Raspberry Pi module runs the server software. The connection will be established through Secured Shell Protocol (SSH) to ensure the security.

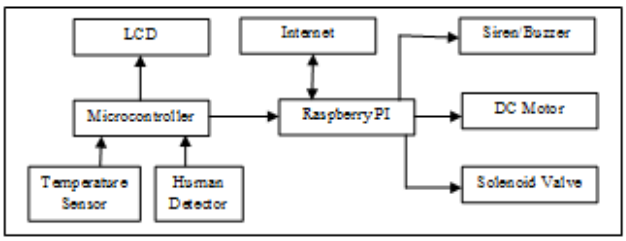

Fig. 1 Block diagram of proposed system

Once connected, the GPIO pins can be monitored and controlled from the remote location through the application. Pi Camera is attached to the Raspberry Pi board, Temperature sensor and Human detector to the system. This helps us to monitor the plant and surroundings from the remote location. Atmega16 Microcontroller is used to run the decoding program So that 8 GPIO pins can be decoded to 2, 3 Output lines. Relays and Motors are used to actuate the switches, safety valves, control valves, etc. The capability of the system can be improved further by connecting more number of sensors and actuators.

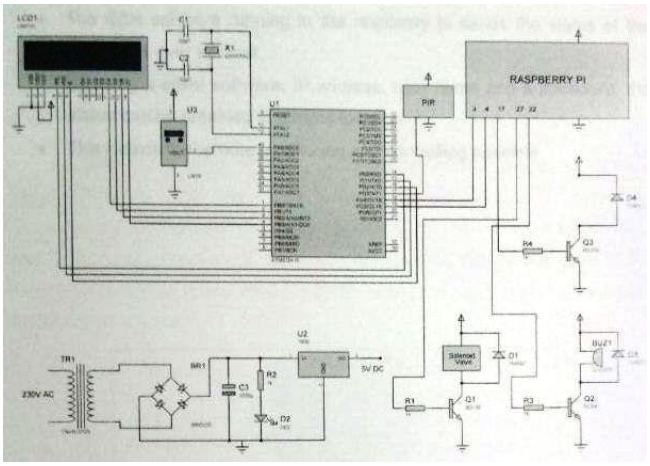

Fig. 2 Circuit diagram of proposed system

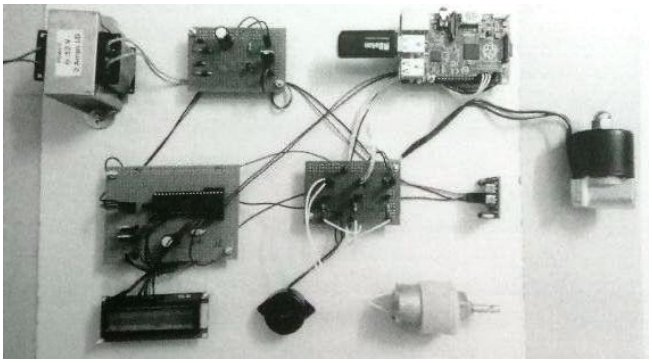

Fig. 3 Hardware Implementation

Modules Involved

There are several modules has been involved in this proposed model as described in the figure 1. These modules consists of 1) Server Applications which includes SSH and WebIOPi for monitoring application. 2) Microcontroller Board with ATMEGA16 with 16MHz Crystal and LCD Interface. 3) Raspberry Pi Board with Micro SD Card 4)Sensors and Actuators modules needs Temperature Sensor - LM35, Human Detector - PIR sensor, Solenoid Valve, DC Gear Motor and Buzzer or Siren. Finally the client application has been implemented as Mobile Phone Implementation and Web Page Implementation. Working Model

As per the circuit diagram represented in Figure 2, the hardware module has been implemented and hardware connections have been shown in figure 3. The system includes a microcontroller board with LCD, Raspberry Pi B+ module, necessary sensors and actuators. The internet connectivity is provided to the raspberry pi through a mobile Wi-Fi hotspot. The LM35 temperature sensor produces 10mV per degree rise in temperature. This sensor is interfaced to the ADC of ATMEGA16 microcontroller. ATMEGA16 is a powerful 40 pin microcontroller from Atmel Corporation. It has 16KB memory and has RISC architecture. And it receives the sensor data from LM35 and sends to Raspberry Pi board.

Table. 1 Hardware Requirements and Budget Analysis

S.No	Hardware Name	Price/ Unit	Image	Total Cost
1	ATMEGA 16 Microcontroller	150		150
2	REES52 LCD	220		220
3	DIY Retails 3.3V and 5V Power Supply Module	150		150
4	Raspberry Pi 3 Model B	2800		2800
5	LM35	60		60
6	PIR Sensor	120		120
7	Solenoid Valve	400		400
8	DC Gear motor	150		150

9	Buzzer	20		20
10	Jumper Wires Set	120		120
11	10 ohm, 100 ohm resisters	5		100
12	Bread Board	80		240
			TOTAL COST	**4530**

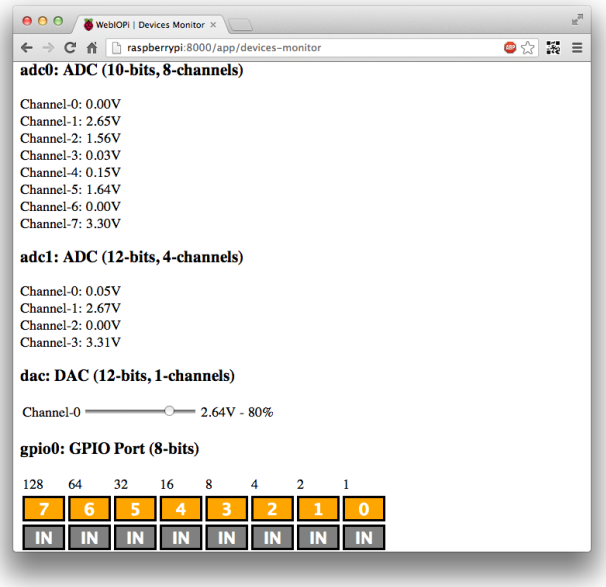

Fig. 4 WebIOPi Client Application

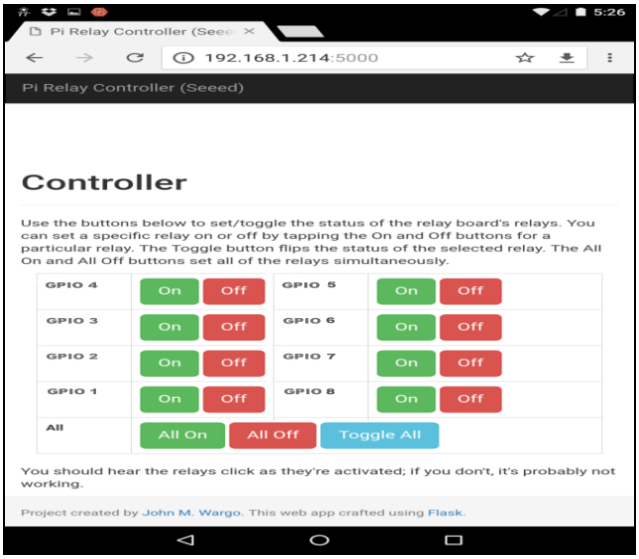

Fig. 5 Raspberry Control (Client SSH Application)

The PIR sensor acts as a human detector to detect the trespassers. It produces digital output when identifies the human interference. The solenoid valve, siren and motor are directly connected to the GPIO of raspberry pi using driver transistors. The sensing action asserts the GPIO pins of raspberry pi. Further 16x2 Matrix LCD iS used to display the system status. The SSH software running in the raspberry pi sends the status of the GPIO pins over internet. By using the client software, IP address, user name and a password. The status can be obtained at remote location and helps to control the environment. This makes the remote monitoring and controlling possible.

Cost Analysis

To deploy this proposed model in a nuclear power plant, the hardware requirements and budget analysis of single node has been listed in table 1. Since this project involves the government approvals for real time implementation, we are assuming that the entire power plant requires at least 100 nodes to monitor the plant. Hence the total cost of this proposed model in real time nuclear power plant required around 4.5 lacks INR.

IV. RESULT AND DISCUSSION

The proposed system has been evaluated with only one node and the monitoring of an environment has been monitored in web and mobile application. Figure 4 represents the Raspberry Control for Client SSH Application. It can control and monitor GPIO 1 to GPIO 8 input output pins. Figure 5 represents the WebIOPi Client Application which shows the implementation and monitoring of the IoT node.

V. CONCLUSION

The Remote Monitoring and Controlling is a developing field. The research in the field Internet of Things makes the remote monitoring and controlling to enter into a new era of development. The number of sensors and actuators can be securely controlled from the remote location using an IP address, User Name and Password. The entire system is safe and easy to operate. Here, the implementation of this technology in nuclear power plant was described. It is also possible to extend the application to wide range and IoT can be integrated with other fields also thus, the IoT is a boon for the field of Technology.

REFERENCES

1. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), pp.1645-1660.
2. Hu, L., Zhang, Z., Wang, F. and Zhao, K., 2013. Optimization of the deployment of temperature nodes based on linear programing in the internet of things. Tsinghua Science and Technology, 18(3), pp.250-258.
3. Jara, A.J., Zamora-Izquierdo, M.A. and Skarmeta, A.F., 2013. Interconnection framework for mHealth and remote monitoring based on the internet of things. IEEE Journal on Selected Areas in Communications, 31(9), pp.47-65.

4. Li, F. and Xiong, P., 2013. Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal, 13(10), pp.3677-3684.
5. Bello, O. and Zeadally, S., 2016. Intelligent device-to-device communication in the internet of things. IEEE Systems Journal, 10(3), pp.1172-1182.
6. Atzori, L., Iera, A. and Morabito, G., 2014. From" smart objects" to" social objects": The next evolutionary step of the internet of things. IEEE Communications Magazine, 52(1), pp.97-105.
7. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M., 2014. Internet of things for smart cities. IEEE Internet of Things journal, 1(1), pp.22-32.
8. Bi, Z., Da Xu, L. and Wang, C., 2014. Internet of things for enterprise systems of modern manufacturing. IEEE Transactions on industrial informatics, 10(2), pp.1537-1546.
9. Chen, S., Xu, H., Liu, D., Hu, B. and Wang, H., 2014. A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal, 1(4), pp.349-359.
10. Kantarci, B. and Mouftah, H.T., 2014. Trustworthy sensing for public safety in cloud-centric internet of things. IEEE Internet of Things Journal, 1(4), pp.360-368.
11. Jin, J., Gubbi, J., Marusic, S. and Palaniswami, M., 2014. An information framework for creating a smart city through internet of things. IEEE Internet of Things Journal, 1(2), pp.112-121.