IMPLEMENTATION OF DATA SECURITY IN IOT BASED SCADA APPLICATIONS

[1]J. PUJA, [2] V.ASWINI
[1]Student, Vignan's Lara Institute of Technology and Science, vadlamudi, A.P, India.
[2]Assistant Professor, Vignan's Lara Institute of Technology and Science, vadlamudi, A.P, India.

Abstract: Generally, SCADA is abbreviated as "supervisory control and data acquisition system". There are various types of systems in industrial control system, but in this paper SCADA (supervisory control and data acquisition) is used. SCADA is used in industry for automation process. Number of accidents happens in the industry are increased in great extent. Due to irregular monitoring and controlling system, accidents are occurred frequently. Such accidents become harmful for human life. To avoid such accidents happened due to system error we have to control the system parameters automatically. So the proposed system gives an advanced solutions to monitor and control the industrial machine parameters. Data acquisition plays important role in industry to ensure the quality of service. Now to provide better security to the server, internet of things IOT and AES instructions are used. This proposed system reduces the maintenance cost and increase the productivity and performance of system.

***Index Terms* - Raspberry pi processor, Raspbian Jessy OS, python language, internet of things (IOT), AES**

I. INTRODUCTION

SCADA is one of the process controls system in industrial automation. Due to rapid technology advancements and security reasons in industry field, the data acquisition and control system has taken important place. SCADA allows the site operator to monitor and control the process which are placed at remote locations. SCADA eliminates the complexity of monitoring and controlling of plants while designing the system. In present days we need accurate parameters while monitoring and controlling the system. SCADA system having computers, controllers, actuators, networks, and interfaces that allows automatic process controlling and also allows data analysis through data acquisition. In the system the sensor waits for a command to provide information of a measured parameter. SACADA system performs the both operation such as data acquisition and supervisory control.

The main advantage of this system is that an engineer or worker not only gets accurate value of industrial parameter but also there is no need of worker to present there. At last sensor is detected by total computation to process the data and it is more than the mechanical devices. The data that is collected from sensor will monitor into the local environments for alarm conditions. In this system readings are read from sensors and then converted to digital by ADC and them sent to Raspberry pi then these values are mapped to the corresponding ranges and compared with thresholds and here the value exceeds the threshold then alarm will be activated and corresponding control measures are taken. After the values are mapped then the data is encrypted using AES encryption algorithm and then data is transmitted to IOT. Basically, to monitor and control the automation process we can use concept of internet of things.

The SCADA system introduced to solve the issues regarding the data monitoring and controlling in the process automation. The SCADA system having real time data accessibility with different types of data communication protocols. Now a days SCADA system provided with rich Graphical User Interface (GUI) which makes easy access and controlling of system. SCADA system requires both hardware and software for successful operation. The main advantages of SCADA software package is the flexibility to design any kind of process by which we can control and monitor the process using smart phone or tablet PC. It does not require any extra development environment. So this paper discuss about the implementation of data security in internet of things based SCADA applications.

II. RELATED WORK

In this we will discuss about the background of SCADA system and as well as how to solve the problems that are occurred due to the SCADA system. According to Mr. Malikamber, Mr. Tamhankar we can build a system which can be used as supervisory control and data acquisition that is SCADA. The term SCADA was first referred in the 1960s at Bonneville Power administration and first published in Power Industry Computer Application. SCADA are computer controlled systems that monitor and control industrial processes that exist in the physical world. The basic SCADA system is made-up of four components Human- Machine Interface (HMI), Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), and Communication Infrastructure.

The SCADA system having wide applications in industrial automation such as signal sensing, control, human machine interface, management and networking. Basically, in SCADA system there are eleven attacker goals and security vulnerabilities. These both inherent the specification and deployment of SCADA system. The both attacker goals and security vulnerabilities will improve the MOBUST standard and suggest best practices to SCADA system. In this paper security protocols are proposed to optimize the SCADA systems.

The SCADA system mainly consists of point-to-point secure channels, authenticated broadcast channels, authenticated emergency channels, and revised authenticated emergency channels. From proposed system it can be observed that it gives an overview about the mechanism of security which secures the SCADA communication which consists of BUMP-IN-WIRE device. The propose system not only provides the security but also eliminates the problems that are obtained from key management by integrating. Now to measure the security level some of the levels are introduced in the system they are secure socket layer/transport layer security (SSL/TLS) and IP security (IPsec) solutions. These are implemented on the test bed to measure the security level. In this system an innovative cloud platform is introduced to reinforce the integrity and security of SOA based SCADA system. As a result, SCADA systems have become very attractive targets for malicious attacks.

III. PROPOSED METHODOLOGY

The main intent of this paper is to monitor and control the industrial machine parameters. This can be done by using internet of things (IOT) and AES instructions. This both provides better security to the server. The below figure (1) shows the block diagram of proposed system. The proposed system consists of ultrasonic sensor, temperature sensor, LDR sensor, AES. Let us discuss each of them in detail.

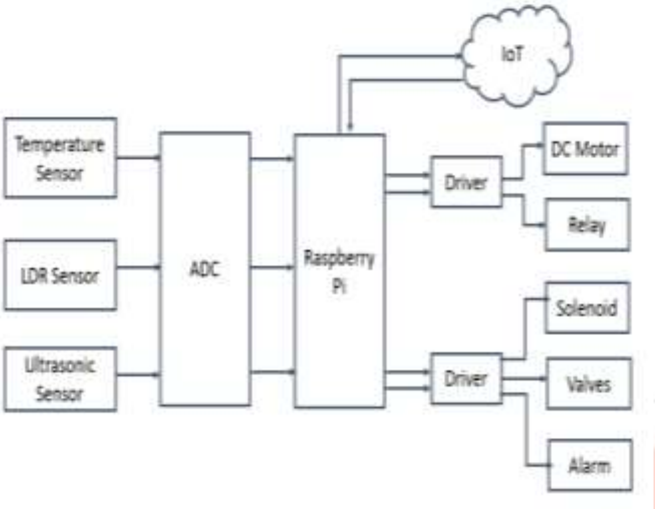


Fig.1 Block Diagram of proposed system

Here Raspberry Pi3 model B is used. It was launched in February 2016. Specifications are:

- 1.2GHz 64-bit quad core ARM cortex a-53 processor
- 1GB RAM, 4 USB ports, 40 GPIO pins
- Integrated 802.11n wireless LAN and Bluetooth (4.1).

a) ULTRASONIC SENSOR

Ultrasonic sensor is a device which measures the distance of an object using sound waves. Ultrasonic sensor work on the principle similar to radar which evaluate attributes of a target by interpreting the echoes from sound waves. Ultrasonic sensor generates high frequency sound waves and evaluate the echo which is received back by the sensor. Now the sensor calculate the time interval between the sending signal and receiving echo to determine the distance of an object. Basically. Ultrasonic sensor has two opening on its front, one of it transmits ultrasonic waves and other will receives them. This technology can be used for measuring wind speed and direction through air and water. They measure the distance without any damage & they can be used easily and they provide better reliability.

b) TEMPERATURE SENSOR:

As there are various types of temperature sensors in this we use LM-35. The below figure (2) shows the temperature sensor. The main intent of this LM-35 is to detect the physical parameters of a device from stored products. LM-35 produces an output voltage which is proportional to Celsius temperature. It is a three pin device out of which the middle pin is used to determine the output voltage. It transmits the data to Raspberry pi.

Fig.2 Temperature sensor

c) LDR SENSOR

LDR is component that consists of variable resistance. It allows to be used in light sensing circuits. LDR is used to control the intensity level of light for protecting photo film and frames. The most common type of LDR has resistance that falls with an increase in light intensity falling upon the device. LDR is made up of semiconductor material. This sensor has high resistance because the electrons in the crystal lattice are locked and unable to move. Hence it can says that it consists of high resistance.

Fig. 3. LDR sensor

When light falls on the semiconductor material then the light photons gets absorbed by the semiconductor lattice. Now some energy is transmitted to the electrons and some energy will be used conduct electricity from crystal lattice. At last the entire data is given to Raspberry pi.

d) AES

AES is a method or process used to change raw information into something that cannot be read. This part of process is known as encryption. This method uses an external piece of information called key, to uniquely change the data. The below figure (4) shows the flow chart of AES system.

The block size of AES is 128 bit and the key size may be 128,192 or 256 bits. Rijindael algorithm proposed a cipher for AES. The block length of cipher is 128 bits. There are mainly three characteristics of Rijindael algorithm, they are given as

1. Resistance against all known attacks,
2. Speed and code compactness on a wide range of platforms,
3. Design simplicity.

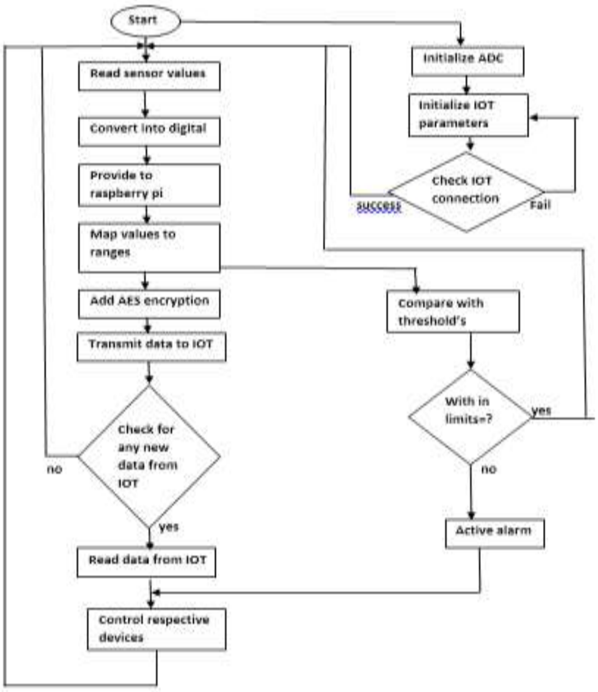


Fig. 4 Flow Chart

A 128 bit block is used as input for both encryption and decryption. This block consists of a square matrix of bytes. The input block is copied to the state array before performing encryption and decryption. Various operations are performed on state of array. By using an array of key schedule words this key is explained. Each word consists of four bytes

System design and operation:

In industries, this system is placed. Initialize ADC, here ADC is a communication channel between the Raspberry pi and sensors. Here the entire system is connected to the internet of things. There are free registering sites on the internet. One of them is “All Things Talk Maker”. First, we need to register on this site. Initialize IOT parameters then check IOT connection, if connection is fail return to IOT parameters & if connection is success then read sensor values. These values convert to digital and provided to raspberry pi. These values have some ranges & compare with thresholds. Enter AES encryption through IOT, if the key is true, the next process will continue otherwise stop the process .If the key is true, new data come from IOT that data collect from IOT. Here the data is within limits then again start the process, if data is not within the limits, go to alarm & control respective devices & again start the process.

Software:

In raspberry pi default language is “python”. OS used in this is Jessie version. It is introduced on Jan 2017. Jessie is the name of the character in cow boy. Connect memory card to the computer to copy the software. Open win 32 disk manager. Copy Jessie image. Remove memory card and insert in raspberry pi. And update the library. Python is most widely used in high level languages for the purpose of general programming and initial discharged in 1991.

Associate degree taken language, Python encompasses a style which emphasizes a code readability and a syntax that permits programmers to specific ideas in fewer lines of code that may well be utilized in languages like C++ or Java. This language is supposed to alter writing clear programs on each a little and huge scale. Python is a dynamic kind of system and it consist of automatic memory management. Python supports various designs like multiple programming paradigms and imperative purposeful programming. Python interpreter’s square measure offered for several operating system. This permits a code to run on large kind of systems.

IV. RESULTS

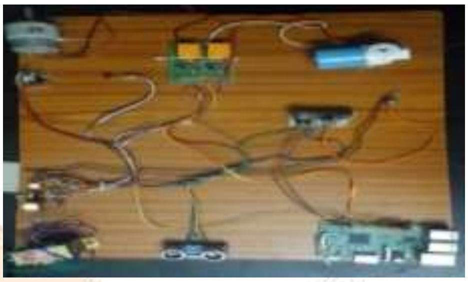
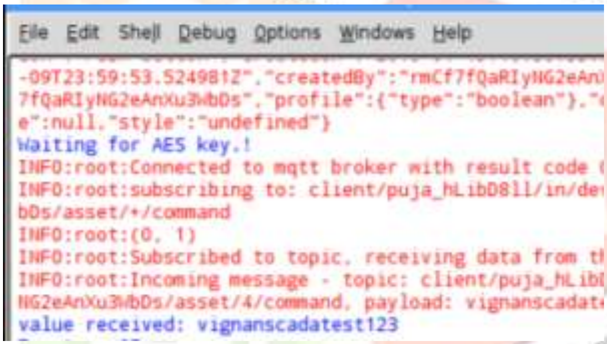


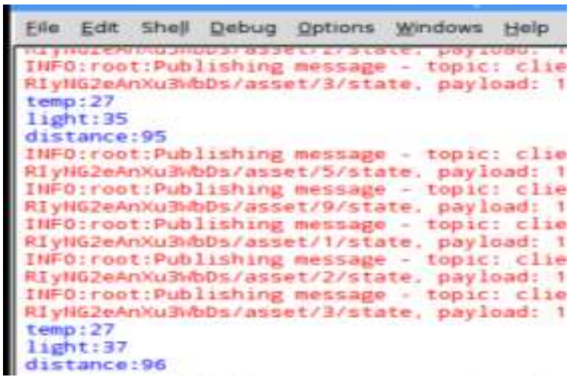
Fig. 5 Proposed System Hardware



```
-09T23:59:53.524981Z","createdBy":"rmCf7fQaRIyNG2eAn
7fQaRIyNG2eAnXu3WbDs","profile":{"type":"boolean"},"
e":null,"style":"undefined"}
Waiting for AES key.!
INFO:root:Connected to mqtt broker with result code 
INFO:root:subscribing to: client/puja_hLibD811/in/de
bDs/asset/+/command
INFO:root:(0, 1)
INFO:root:Subscribed to topic, receiving data from t
INFO:root:Incoming message - topic: client/puja_hLib
NG2eAnXu3WbDs/asset/4/command, payload: vignanscadat
value received: vignanscadatest123
```

Fig. 6 Waiting for AES key

Fig. 7 Output shown in IOT



```
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/3/state, payload: 1
temp:27
light:35
distance:95
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/5/state, payload: 1
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/9/state, payload: 1
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/1/state, payload: 1
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/2/state, payload: 1
INFO:root:Publishing message - topic: clie
RIyNG2eAnXu3WbDs/asset/3/state, payload: 1
temp:27
light:37
distance:96
```

Fig. 8 Parameters Output

We can run the code then first enter the key like vignanscadatest123 through IOT, if the key is true, the next process will continue otherwise stop the process. If the key is true, the data will continue to the 24 hours.

V. CONCLUSION

SCADA system will monitors and controls the industrial environment by using new emerging technology of internet of things. This system gives efficient solution than other systems. In this system, the data collected from the sensors are available to user from remote location at any time. Once monitor the sensors values then it control through IOT. Here AES instruction is used to provide security to the server. To improve cyber security at the interface between IOT technologies and SCADA applications various techniques are used. There are, however, particular challenges that remain to be addressed by further work. At last the proposed system secures the data in a very efficient way.

REFERENCES

[1] (2016). WebSCADA, Web SCADA, Automation Systems, Process Control, Historian, Event Alarm, SCADA Solution, accessed on Feb. 5, 2016. [Online]. Available: http://www.webscada.com/SCADA/SolMedSys.aspx

[2] R. J. Robles and M.-K. Choi, ‘‘Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems,’’ Int. J. Grid Distrib. Comput., vol. 2, no. 2, pp. 27–34, 2009.

[3] Eric J. Byres, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", International Infrastructure Survivability Workshop (IISW 2004), 2004.

[4] Y. Wang, ‘‘SCADA: Securing SCADA infrastructure communications,’’ Int. J. Commun. Netw. Distrib. Syst., vol. 6, no. 1, pp. 59–78, 2012.

[5] B. Zhu, A. Joseph, and S. Sastry, ‘‘A taxonomy of cyber attacks on SCADA systems,’’ Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, 2012

[6] R. Tawde, A. Nivangune, and M. Sankhe, ‘‘Cyber security in smart grid SCADA automation systems,’’ in Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS), Mar. 2015, pp. 1–5.

[7] S. Patel and P. Sanyal, ‘‘Securing SCADA systems,’’ Inf. Manage. Comput. Secur., vol. 16, no. 4, pp. 398–414, 2008

[8] T. Baker, M. Mackay, A. Shaheed, and B. Aldawsari, ‘‘Security-oriented cloud platform for SOA-based SCADA,’’ in Proc. 15th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput., May 2015, pp. 961–970.

[9] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, ‘‘A novel security scheme for the smart grid and SCADA networks,’’ Wireless Pers. Commun., vol. 73, no. 4, pp. 1547–1559, 2013.

[10] S. Patel and P. Sanyal, ‘‘Securing SCADA systems,’’ Inf. Manage. Comput. Secur., vol. 16, no. 4, pp. 398–414, 200