Secure Data Monitoring System with Encrypt Data Transmission over Radio Communication Based on Microcontroller

Kadek Suar Wibawa
Information Technology Department
Faculty of Engneering, Udayana University
Jimbaran, 80361, Indonesia

Nyoman Piarsa
Information Technology Department
Faculty of Engneering, Udayana University
Jimbaran, 80361, Indonesia

ABSTRACT
Data Security is important in communication system. A communication system is reliable as long as it provides high level of security. Some security vulnerabilities may be discovered through the interception of wireless data communication. Intercept and modify data that occur in application system could harm the entire system performance. The Monitoring System is one of application form to implement communication and data exchange over wireless technology. Advanced Encryption Standard (AES) to enscrypt sensitive data could reduce potential data interception. AES-128 Algorithm is sufficiently secure against exhaustive search, using a key sizes of 128 bits. The implementation of the AES-128 on real time monitoring system at this application can protect data form, data source, data transmission until data is archived at database system. Performance Monitoring System is based on embdedded system microcontroller ATMega32 with 7.372800 MHz external crystal resonator that effectively does data encryption with an average time 2.153592 mS.

General Terms
Embedded Systems, Data Security

Keywords
Key word: Embedded system, Microcontroller, Monitoring System, AES 128.

1. INTRODUCTION
Data Security has a vital role in communication system [1]. A communication system is reliable as long as it provides high level of security. The security system includes: privacy, integrity, authentication, and availability [2]. Some security vulnerabilities may be discovered through wireless data communication interception.

The Monitoring System [3] is an application form to implement communication and data exchange over wireless technology. A Monitoring system[4] technology growing fast, driven by the development of Internet of Things (IoT). Data Interception and modification that occurred in application system could harm the entire system performance[5]. Security method needs to be implemented from transmitt the data until it archived in database system.

2. OVERVIEW

2.1. Fishbone Diagram
The monitoring system is divided into two parts: 1. Data Acquisition Unit (DAU) is a sub system field that includes a SHT sensor, Radio Communication, etc. on a microcontroller board embedded system. 2. Data Collecting Unit (DCU) is an end-user application graphic user interface (GUI) that includes radio communication, database management system, etc. built on Personal Computer. Component, system and method is showen in Fig. 1.

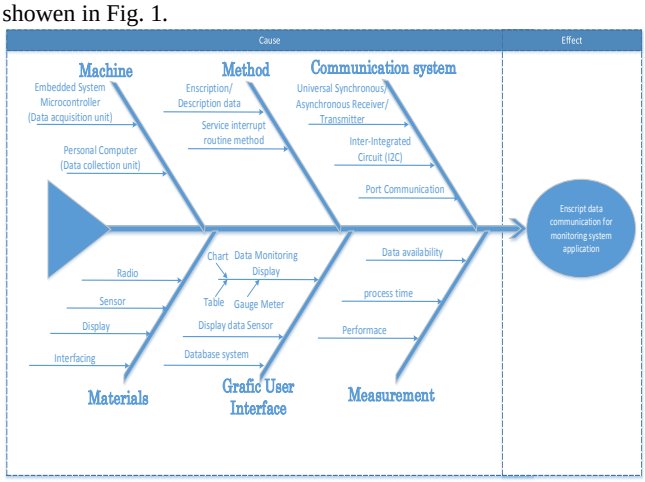


Figure 1: Fishbone Diagram

2.2. Design monitoring system
In this implemented system, SHT11 sensor provides relatively humidity sensor and temperature which is connected to embedded microcontroller using two wire serial interface. Data acquisition results will be encrypted using static private key based on AES-128 encryption[6][7][8], prior to transmitting a packet payload on radio[9]. These data also displayed on dot matrix LCD 4x20 at DAU embedded microcontroller.

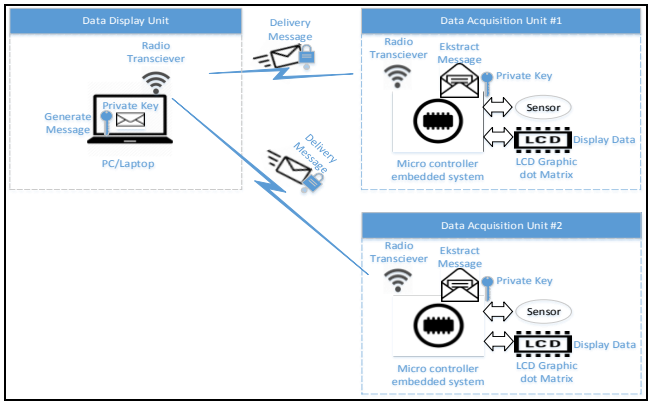


Figure 2: Overview diagram monitoring system

The system was deployed to produce prototype product that allows users to continuously monitor the relatively humidity temperature at a control room through DCU Application. Design of DCU user interface application is shown in Fig. 3.

Figure 3: Design of DAU user interface application

3. HARDWARE ARCHITECTURE DESIGN

The data acquisition unit uses microcontroller ATMega-32 embedded system developed prototyping board with 7.372800 MHz external crystal oscillator that has been used for the hardware implementation and test. The sensor to measure relative and humidity temperature (RHT) used SHT 10 from Sensirion's family. There are only four wires required to connect the sensor with microcontroller board with standard two wire serial interface communication. The SHT 10 have a default measurement resolution of 14bit (temperature) and 12bit (humidity). With this resolution, controller have to wait a maximum of 320 ms for the measurement to complete. Dot matrix LCD 4x20 is used to display data from sensor measuring data acquisition unit.

The component that used for establishing data transmission over radio communication between multiple data acquisition unit and data collection unit is UART (Universal Asynchronous Receiver Transmitter) null modem. The blocks to build up the data acquisition unit embedded microcontroller is shown in Fig. 4.

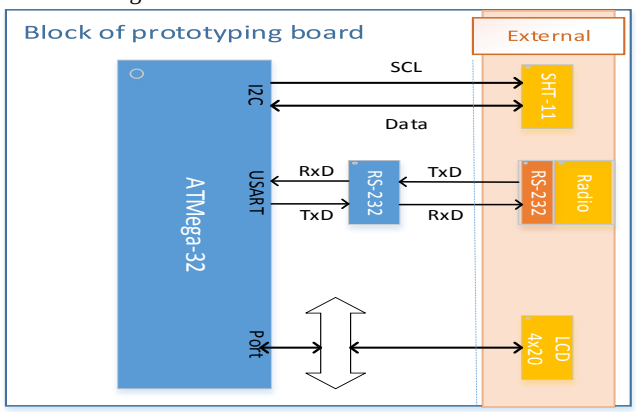


Figure 4: Block Diagram Data Acquisition Unit

4. SOFTWARE DESIGN

4.1. Data Acquisition Unit Software (DAU) Design

Software applications was developed using ANSI C programming language. Structure of applications made a list of process to be executed within a certain slot-time. The Process list include: Counter soft RTC, data read sensor, data Acquisition, data Encryption (), data Transmission and data display.

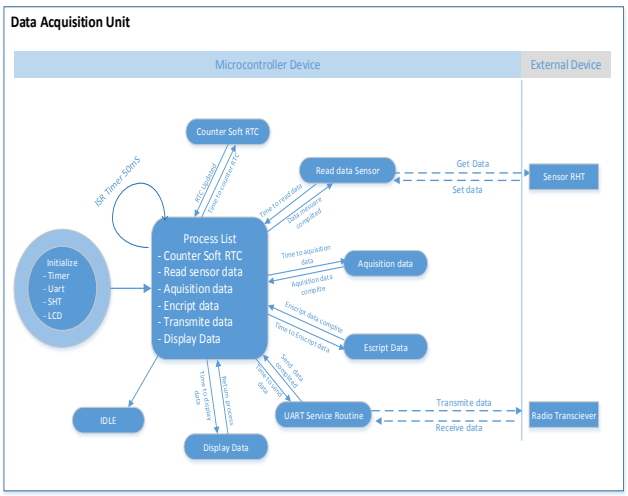


Figure 5: State Diagram DAU

Interrupt Service Routine (ISR) Timer generates triggers every 50 mS. this trigger is used to check when the list should start. There are 20 tasks able to within a second (It able to process 20 task within a second) assuming that completed process is take less than 50mS. If the process runs more than 50 mS, it takes more slot-time to complete this process. Output Compare Register (OCR) timer setting is shown below.

$$OCRn = \left(\frac{Time\_constant \ * f_{oc}}{N}\right) - 1$$
$$OCRn = \left(\frac{0.05\ S * 7372800\ Hz}{1024}\right) - 1$$
$$OCRn = 359\ .$$

The data frame format is shown in Fig. 7. Data frame format is used to simplify the expansion of the system on data link layer. Redundant checksum is added at the end of the frame covering from *jumlah* to nByteData as error checking during the data transmission. Data encryption, only on payload data.

Figure 6: Format data frame protocol

Description :

Start bit	: Start of data
Jumlah	: Number of data
Sumber	: ID from data source (8 bit)
Tujuan	: ID from data destination (8 bit)
nByte data	: Data *payload* (n byte data)
Checksum	: error checking (8 bit)
Stop bit	: End of data

4.2. Data Collection Unit (DCU)Software Design

DCU software applications was developed using Java SE programming language with the NetBeans Platform. Graphic user interface was designed for easy use that utilizing the library's: jfreechart-1.0.19 , libsteel, rxtx-2.1-7r2 nd mysql-connector-java-5.1.39.

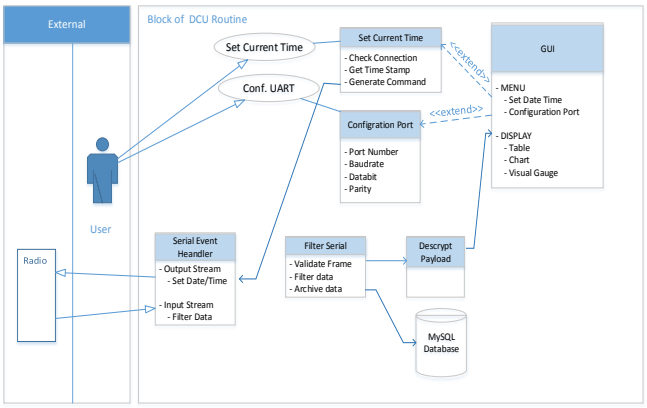


Figure 7: Use Case Diagram DCU

Users can configure the serial port or setting current time DAU through setup menu-bar. Use case diagram software module DCU is shown in Fig. 8.

5. IMPLEMENTATION

In according to its functions, sub-unit of the DAU are grouped into four major categories: (1) Unit data communications (radio communication), (2) Sensing the temperature and relative humidity (Sensor), (3) Information Display (LCD) and (4) processing center unit (Microcontroller). The implementation of DAU hardware is shown in Fig. 9.

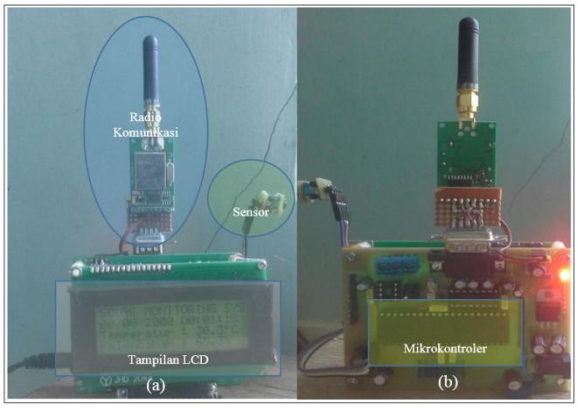


Figure 8: Data Acquisition Unit (DAU)

The DAU is an integrated module embedded system on board with a microcontroller as the center of processing unit. External modules such as LCD is connected to main board using data port, radio communication using UART RS232, and SHT sensors connect to main board using two wire serial interface. Technical DAU as shown in table 1.

Table 1. Technical DAU Specification

No	Unit	Specification
1	Main board	➢ Microcontroller ATMega 32A - Memory flash: 32KB, SRAM 2KB, EE-Promp 1024Byte ➢ Peripheral Board - Serial RS-232 - Serial two wire interface - Port data ➢ Oscillator Clock 7.7328MHz ➢ Voltage in DC 5 Volt
2	Radio communication	➢ frequency 433MHZ ➢ Baudrate 19200 ➢ Half duplex (TXD-RXD)
3	Sensor	➢ SHT 10
4	LCD	➢ Dot Matrix 4x20 ➢ Char dot 5x8

According to the design that has been done, the information on the DCU is presented in three different forms of information: information in the form of tables, graphs and visual information display.

Figure 9: Data Collection Unit (DCU)

DCU software runs on Java platform Virtual Machine which runs on most of operating systems and hardware types and a common platform for software to be written. To archive the data, DAU used MySQL Open Source Database application. MySQL is fast and tends to use less system resources. MySQL runs on over a dozen operating system platforms. It is relatively easy to install, configure and use. The implementation of DCU software is shown in Fig. 10.

6. RESULT AND TESTING

Plaintext is the data acquisition result from temperature and relative humidity sensor. Plaintext is encrypted using 128-bit secret key. Fig. 10 showed the test results plaintext encryption in hex format.

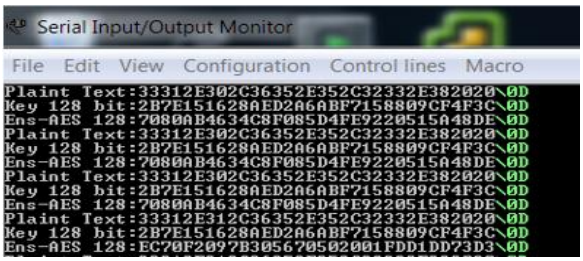


Figure 10: Encryption DAU Test Result

Fig. 11 is shown The Encryption DAU test results. The test results were compared using AES 128 online calculator and the results are in accordance. It can be stated that DAU devices are capable of performing the encryption result correctly.

The DAU received byte stream format frame protocol over serial port communication. The byte stream data must be processed to separate the payload (the actual data) with the components of other identities. Payload is the data encrypted. The data must be decrypted using the same private key before display at graphic user interface DCU application.

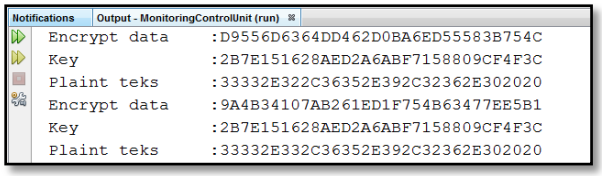


Figure 11: Decryption DCU Test Result

Fig. 12 is shown The Encryption DCU test results. The test results were compared using AES 128 online calculator and shows the results are in accordance. It can be stated that DCU devices was capable of performing the encryption result correctly.

Fig. 13 showed format data frame layer on the serial port communication. Data byte stream received had a shape in accordance with the design of format frame protocol which have been discussed previously.

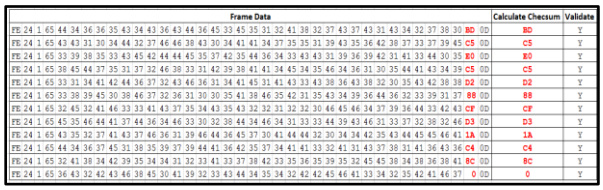


Figure 12: Validate Redundant Check

When the DAU received byte stream data over the port communication, serial event handlers will check the packet format received by compared value of the redundant. If the redundant value included on the frame is different from the calculation results of the sum check, certainly there has been a change of bits of data when it was transmitted. In this case, the data frame received has encountered an error. Thus the system will not process the data. If the redundant values is equal to calculation results value, it can be stated that the data is still in the intact condition and the process can be performed (displayed and archived data).

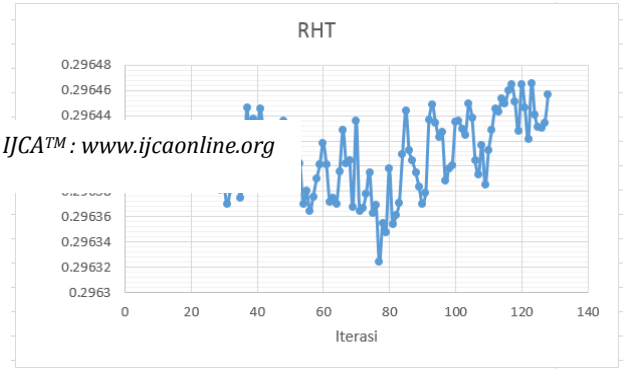
Performance testing was done to ensure the system can work properly in accordance with the system design and each sub-system characteristics function. The test was done by counting the processing time required to complete the task. The measurement method used a 16 bit timer interrupt service.

RHT sensor measurement requires a range between 324 056 296. mS up to 296.465522 with the average value of the execution time is 296.407387 mS. Detailed test results is shown in table 2.

Table 2. RHT Test Result

	Cycle	Time (Second)
Average	2185352	0.296407387
Minimum	2184738	0.296324056
Maximum	2185781	0.296465522

The performance of RHT measurement sensor method showed that the variation of measured value vary from 296. 324056 mS to 296.465522, but the value is still in safe operating area, referencing to datasheet sensor for measuring sensitivity of 14 bits is 320 mS. The graph of test results is shown in Figure 14.



IJCA™ : www.ijcaonline.org

Figure 13: Graphic performance RHT Test Result

7. CONCLUSION

The aim of this proposed design is to perform a real-time data communication humidity and temperature monitoring system exhibiting a significant level of data security and providing reliable data on database archive system. The system works effectively and could be implemented with little cost.

8. REFERENCES

[1] Saleh Saraireh 2013, 'A Secure Data Communication System Using Cryptography and Steganography', International Journal of Computer Networks & Communications, vol. 5, no. 3, hh. 125-137

[2] Simson Garfinkel 1995, PGP: Pretty Good Privacy, O'Reilly & Associates, Inc.

[3] Beth A. Schroeder 1995, 'On-Line Monitoring: a Tutorial', State University of New York, Binghamton

[4] Balachandran T, Saleh M. Sbenaty and Jeffrey Walck 2013, 'Remote Humidity and Temperature Real-Time Monitoring System for the Study of the After-Ripening Process in Seeds', American Society for Engineering Education.

[5] Budi Rahardjo 2002, 'Keamanan Sistem Informasi Berbasis Internet', PT. Insan Indonesia - Bandung & PT INDOCISC, Jakarta7

[6] Rifki Sadikin 2012, 'Kriptografi untuk keamanan jaringan', Andi, yogyakarta.

[7] Rinaldi Munir 2006, 'Kriptografi', Informatika, Bandung.

[8] Ali E. Taki El_Deen and Ahmed Mohamed Fanni 2013, 'Implementation of AES Algorithm in MicroController Using PIC18F452', IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 5, Issue 5, hh. 35-38

[9] Zhiyuan GAO, Yingju JIA, Hongwei ZHANG & Xiaohui LI 2012, 'A Design of Temperature and Humidity Remote Monitoring System based on Wireless Sensor Network Technology', International Conference on Control Engineering and Communication Technology, pp. 892 – 895