*Article*

# Secure Wireless Sensor Network using Cryptography for Smart Farming Systems

**Abdul Wahid[1*], Ilham Juliady[2], Satria Gunawan Zain[3], Jumadi Mabe Parenreng[4]**

[1,2,3,4]Computer Engineering, Makassar State University, Makassar, South Sulawesi, Indonesia

* Corresponding author: wahid@unm.ac.id

**Abstract:**

Internet of Things (IoT) technology has become part of human life. Agriculture, in many parts, is one of the IoT implementation segments, including the cultivation of mold oysters. The Internet of Things (IoT) is applied to collect data from combined sensors in the Wireless Sensor Network (WSN). This will make it easy for farmers to monitor and control the garden remotely. Regardless of the application system control distance far based WSN that will make it easy for a farmer, the system has gap security, and one of them that is hacking and tapping of communication IoT data is dangerous on effort if condition room mold oyster the known by someone hacker who can is rival effort. It is a needed method for secure communication when the data transfer process is over-guaranteed. The technique used is application Base64 -based data encryption/decryption on WSN node devices and controlling and monitoring mobile devices. Based on the results, trials carried out after implementing Secure WSN with scenario tapping using the Wireshark tool show no data can be read. Analysis results show that this model could be applied as Secure WSN for Smart Farming System.

**Keywords:** Data Security, Base64 Encryption, IoT, WSN, Smart Farming, Aquaculture Mold Oysters, Wireshark



**Citation:**A.Wahid,I.Juliady,S.G.Zain,J.M.Parenreng,“ Secure Wireless Sensor Network using Cryptography for Smart Farming Systems”. *Iota*, **2022**, ISSN 2774-4353, Vol.02, 04. https://doi.org/10.31763/iota.v2i4.554

Academic Editor : P.D.P.Adi

Received : Oct, 05 2022

Accepted : Oct, 17 2022

Published : Nov, 20 2022



## 1. INTRODUCTION

Application increasing technology in a significant manner has changed life to become more modern and practical, like using more valuable and accessible tools. [1] One of them that is the process of monitoring land plantations in the middle area of the current urban this many in demand (urban farming), which is usually only conducted manually and requires a long time, too, resulting in less monitoring accuracy. The development of urban farming the more fast one of them utilizes technology to make it easy activity in nurse kumbung to cultivate mold oysters [2]. of course, technology monitoring applies a draft of The Internet of Things (IoT) that will contact devices complicated as sensor nodes and Microcontrollers, which will send information to monitoring software through the internet [3]. However, vulnerable internet networks to secure network. See the moment IoT of cases of hacking and data leaks occur, and then the system must do an approach for data [4]. So every system must have enhanced data transfer security with applied technique encryption, so it is not susceptible to test data [5]. Data security using Base64 encryption can become a solution so no anyone can read data during the transfer process and server [6]. So that with

apply Server Base64 Encryption Technique and data transfer will be guaranteed safe from reading and data leakage because When Esp 8266 captures data from DHT22 Sensor then occur an Encryption process on Esp 8266 and When the data transferred so will change be random data or no data could read [7]. So by applying Base64 Encryption on Smart Farming Cultivation Mold oysters, the data will be guaranteed safe from data reading and leakage.

## 2. THEORY

### *2.1 Data*

Data is facts and figures that can form and become a piece of information. Data is a bunch of descriptions from something obtained through observation or search of specific sources. Obtained data could Become a fact or information [8]. Data sent through track public (internet or Wi-Fi) can be leaked because intercepted by parties that are not authorized for this[9]. Him that need there is an effort to ensure the confidentiality of this data.

### *2.2 Sensor Node or Microcontroller ESP8 266*

In the WSN system, the microcontroller used as the sensor node is microcontroller ESP8266. These sensor nodes will collect outcome data reading environments from various WSN network sensors. ESP 8266 is a Low-cost chip Wi-Fi with TCP/IP managed capabilities and MCU (microcontroller unit) manufactured by Shanghai-based Chinese manufacturer Espressif Systems. This ESP 8266 module uses Wi-Fi to communicate data between the client and server [10]. The tool Becomes the brain of a working Internet of Things (IoT) system. Processing data sent to the database as well monitoring applications [10].

### *2.3. Sink Node or Raspberry Pi*

The sink Node is a functioning node for collecting sensing data from the Sensor Node, then passing it on to a device or system, like the database server for storage or the monitoring website. Besides for collect data from sensor nodes, the sink also works as a spreader package from the device or other systems to WSN, for example, for necessary programming or configuration reset the sensor node remotely[12]. On the WSN implementation for smart farming cultivation mold oysters, In this case, the Raspberry Pi is used as a sink node. Raspberry pi is an SBC (Single-board computer) for card ATMs. Raspberry pi is already Complete with all computer functions and uses ARM's SOC ( System-on-a-chip ) packaged and integrated on top PCBs [13]. Raspberries pi has a system operation alone that is Raspbian, and it also can use system operation-based Linux like Debian, kali Linux, etc. System operation of the open source could then be used without limits and can apply network security [14].

### *2.4 Cryptography*

Now, so many data and information security systems use Cryptographic Techniques. Cryptography originated from Greek, Crypto, and graphics. Crypto and graphics means (writing). Moreover, to reach data confidentiality, System cryptography utilizes the technique of converting clear messages (plaintext) to messages that have been encoded (ciphertext) with a specific algorithm. The conversion process this called encryption. Instead, translated ciphertext Becomes plaintext called with decryption. Encryption and decryption processes use one or several vital cryptographies [15].

### *2.5 Base64 encryption*

Base64 encoding for obfuscation or dataBase64 randomization is an algorithm for Encoding and Decoding data in ASCII format, which is based on numbers base 64 or could meaning as one of the methods used for To do encoding ( encoding ) of binary data [7]. Base64 is a gathering scheme binary-to-text encoding that represents binary data in ASCII string format with translates it to denote radix-x64 (64 characters unique) [16]. Term Base64 originated from encoding delivery specified MIME content. Each base64 digit replaces 6 data bits [13]. Base64 encoding feature can be used as a technique for encryption description of monitoring data and control data on the cultivation of WSN Smart Farming system mold oysters. Sensitive data sent through network public goods, whether via the internet or wireless, will be encoded using Base64.

## 3. METHOD

### *3.1 Architecture Base64 encryption*

This study uses Research and Development (R&D) type. R&D is a step-by-step process for developing something product new or a perfect product that has there. Study this will focus more on the system security network that is encryption using base64, which works to increase security data communication data transfer NodeMcu ESP 8266 with Raspberry pi to avoid hacking hacker attack system data reading as well manipulating data. The global system architecture is shown in the following figure, the components that make up and build a Secure Smart Farming system in this study. The component icon used in this system encryption architectural drawing illustrates a data security system that will be implemented later.

The illustration in Figure 1 viz Effort to increase data security so not everyone can read data and not could be manipulated by attack hackers. Principle work from System security uses This Base64 encryption when the ESP 8266 captures data from the DHT22 sensor; then the encryption process occurs then sent to the raspberry pi, MQTT Server, and when web monitoring calls for display, the decode on a raspberry pi server will work.

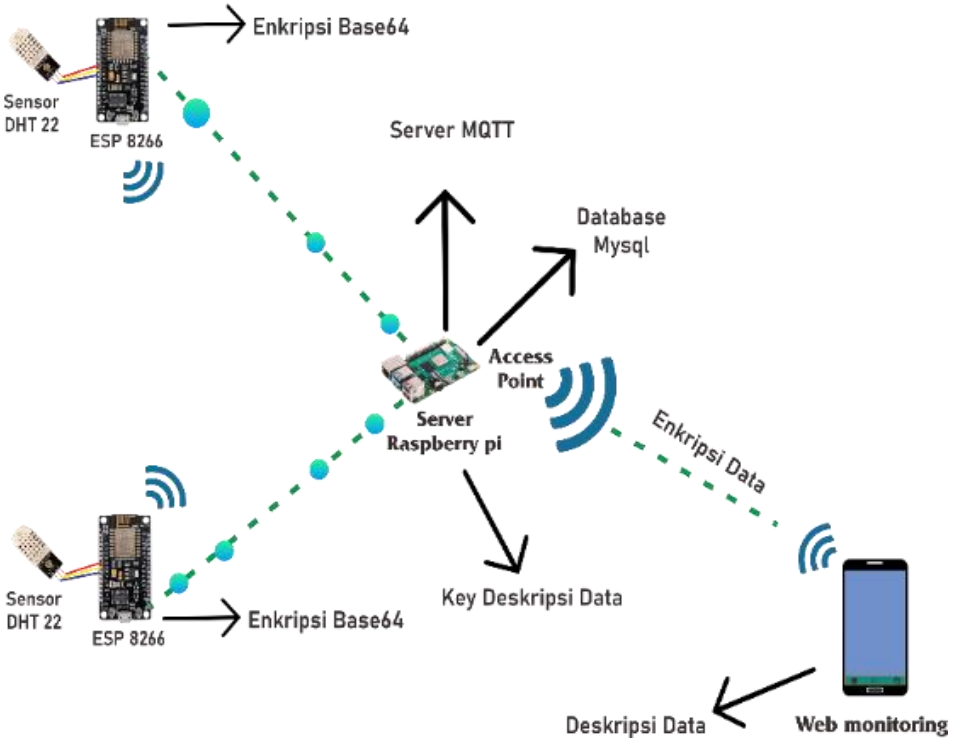


***Fig.1*** Encryption/Decryption Architecture

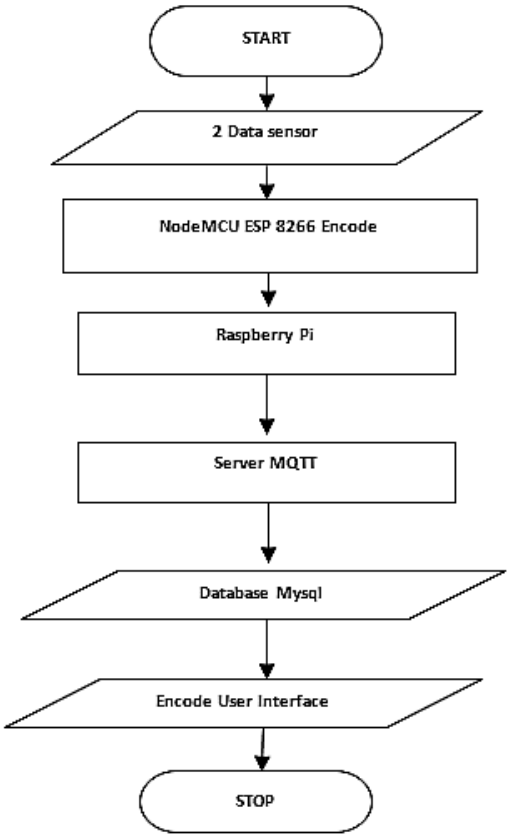


***Fig.2*** Flowchart of the Encryption / Decryption process

Figure 2 shows the flowchart of the encode-decode process. Here, the encoding process is carried out on the sensor node (ESP 8266) and the end user side, monitoring mobile web applications. This show that encryption process decryption happens on the end user's side, i.e., end first in the form of sensor nodes as center sensor data collector and innovative farming device control center. And tip only one again is user side or the farmer will monitor and control their intelligent farming system from a distance.

*3.2 Arduino ESP 8266 data encoding program*

To do Coding on the Arduino IDE uses the C programming language and utilizes the Arduino IDE library, namely Base64, with a destination for securing the sensor data that will be sent to raspberry pi servers. When the ESP 8266 transfers data to the raspberry pi server, the encryption process where is the original data in form numbers and will be converted be a data string that is not recognized or data that has been encrypted after the process occur so The ESP 8266 microcontroller will transfer data to the raspberry pi server.

*3.3 Base64 decode configuration*

Furthermore, configuration on the Raspberry Pi server uses Python programming language. The base64 decode is a key or key from Base64 encryption sent from ESP 8266, then with Thing, such as When the sensor data has been received on the last raspberry pi server. And that will be continued to MySQL databases, and then the base64 key will work for open key encryption to be original data. When processing the encryption key, work with the method convert Returns the encryption string data be data char or in form numbers. So with Thing, those data will have come on stage, i.e., original sensor data, temperature, and humidity.

*3.4 Base64 decode Result*

Figure 3 is a website for controlling and monitoring the temperature and humidity cultivation of mold oysters. Displayed data is the original data that was initially encrypted, and when web monitoring calls for displaying, Encode will work and then display the original data. Moreover, this website can also remotely control all connected gardens in the cultivation of innovative farming network mold oysters. Guess you can instruct the fan or watering medium for work following needs based on the data sent by sensors from each garden. This website control and monitoring could open from a desktop device or mobile device because it utilizes the responsive feature of a user web application.

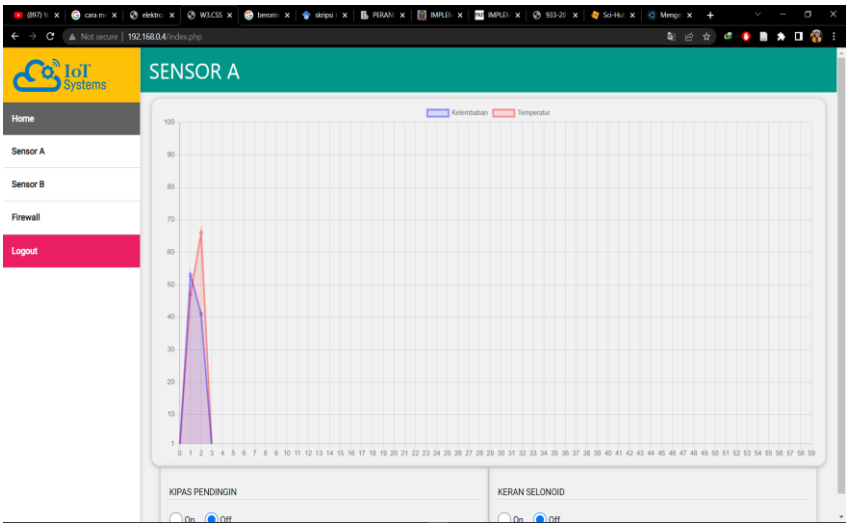


***Fig.3*** Website Monitoring

*3.5 MQTT Server Raspberry pi/Sink Node*

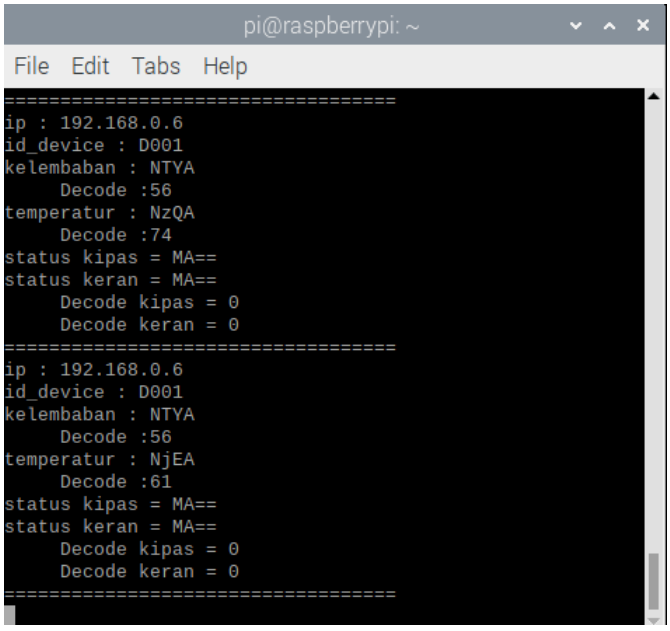


***Fig.4*** Raspberry pi MQTT Server

In Figure 4, the sink node, the raspberry pi MQTT Server, displays the encrypted and original data. The server also works in data transfer displayed on the monitoring website. To do an MQTT server configuration on raspberry pi using the Python programming language. Configure this server to keep all data sent from The ESP 8266 microcontroller stored on the raspberry pi server. So thereby, raspberry pi will utilize the main server or last sink node to continue to MySQL databases for display on the website control and monitor smart farming.

This website uses a secure protocol for data security between an end user and the web server.

*3.6 Trial Scenario*

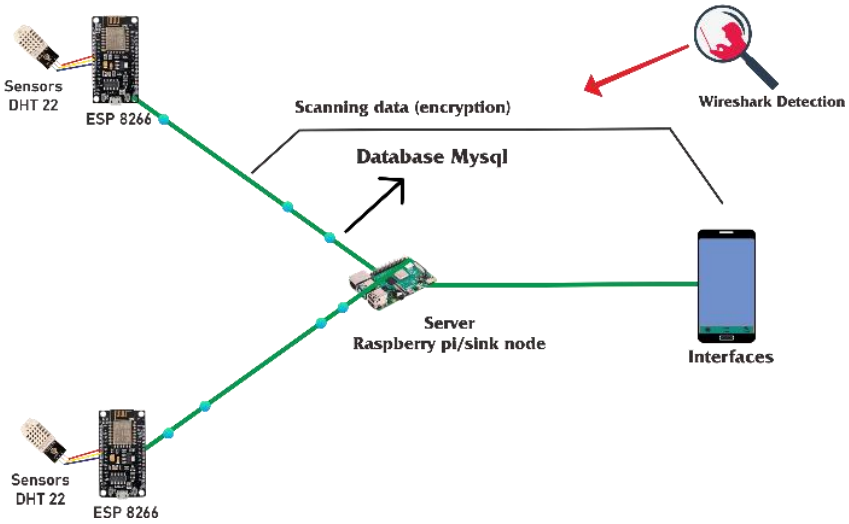


***Fig.5*** illustration attack

A trial scenario was conducted to see the level of success after applying data encryption using Base64 Encryption on Smart Farming Cultivation Mold Oysters Simulation attack with the use of kali Linux tools Wireshark for stream scanning network and viewing the transferred data.

## 4. RESULT AND DISCUSSION

Research results from this form enhancement security on the system Internet of Things (IoT) and Wireless Sensor Network (WSN), which is implemented in Smart Farming Cultivation mold oyster based on Wireless Sensor Network (WSN). Development on the side security this smart farm aims to increase security on a system and specifically system Deep Internet of Things (IoT). The effort to increase security for every data transfer communication as well control. Because of the concept of base Internet of Things (IoT), the system could be safe from an attack that takes advantage of the internet network in data transfer.

*4.1 Testing Monitoring Encrypted Data Scenario*

A company rival Smart Farming Cultivation mold A curious oyster with Smart Farming Cultivation company mold oyster B because of rapid sales with quality mold very good oysters, so the B company wants to To do hack and try to see server content in the company smart farming cultivation mold oyster B. Then hacker execution of the cultivation smart farming company server mold oyster the with To do data reading using tools kali Linux Wireshark for see how temperature and humidity so that mushrooms in the company the quality.

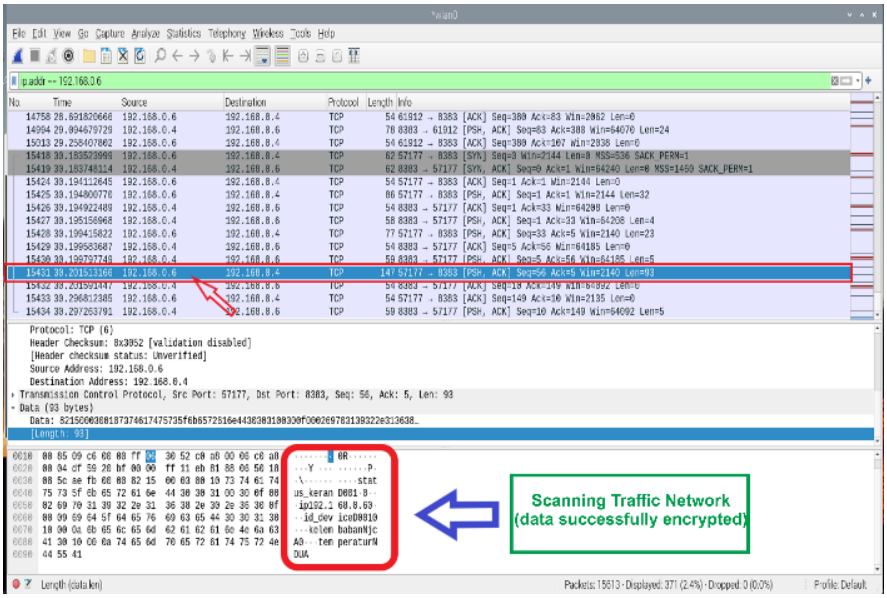


***Fig.6*** Capture sensor encryption data A Traffic Wireshark

Figure 6 testing detection Genre network use kali Linux tools Wireshark, where the devices could detect and view temporary data in the process of transferring to the server. So with testing, this is the data sent from IP Addresses 192.168.0.6 data that was successfully detected in form encryption or could not read.

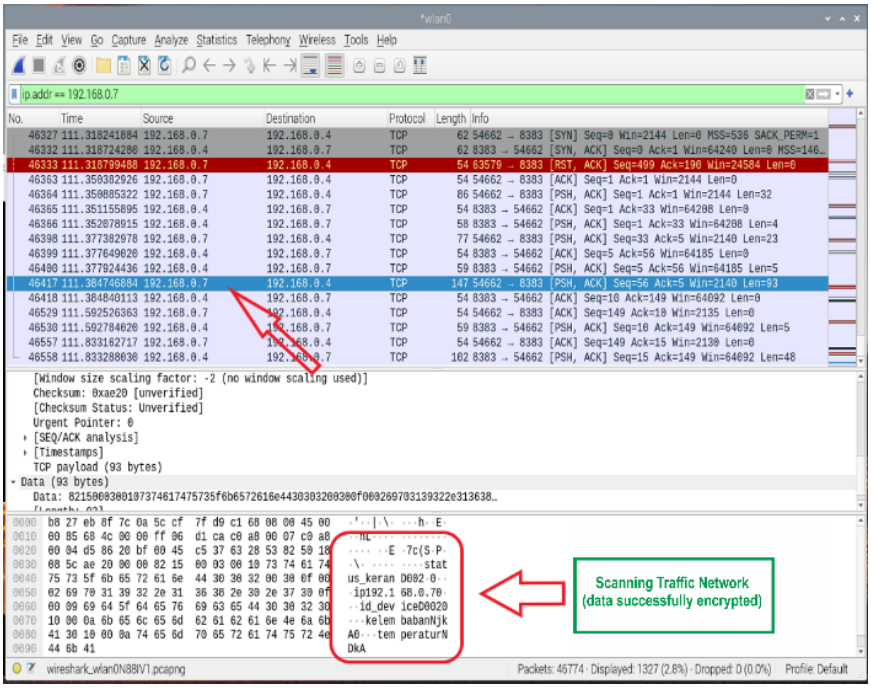


***Fig.7*** Capture B Traffic Wireshark sensor encryption data

Figure 7 is testing detection Genre network from sensor data A with Ip Address 192.168.0.7 using Kali Linux tools Wireshark where the devices could detect and view temporary data in the process of transferring to the server. So with testing, This is the data that was successfully detected in the form of encryption or not could be read.

*4.2 Testing Control Message Base64 Encryption Scenario*

In one particular case study, Smart Farming company's rivals, Oyster mushroom cultivation A, are curious about Smart Farming Oyster mushroom cultivation company B because of fast sales with very good quality oyster prints. Therefore, company B wants to hack and try to view server content on smart farming company oyster mushroom cultivation B. Then The hacker executes the smart farming of the oyster mushroom server mushroom cultivation company by reading the data to see how and what controls are carried out on the oyster mushroom so that the product is of high quality.

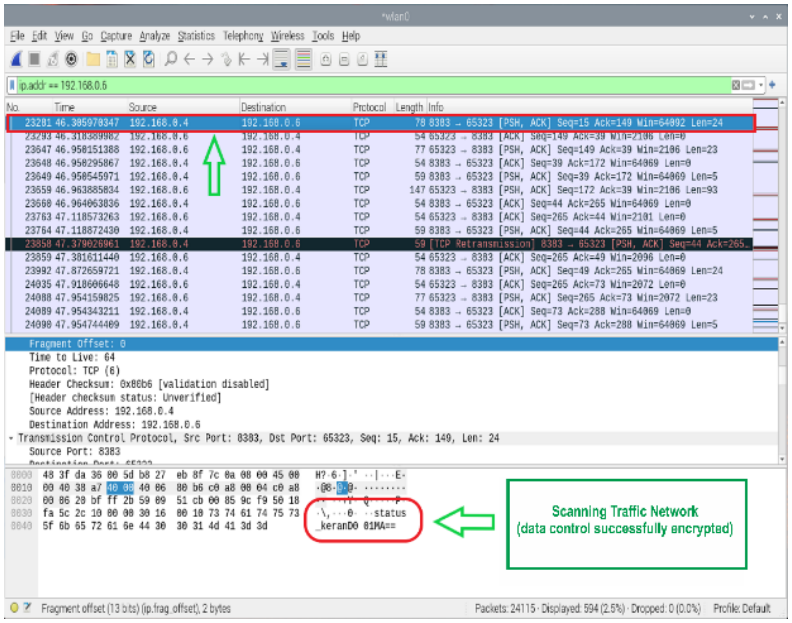


***Fig.8*** Capture controls tap encrypted Sense A Traffic Wireshark

Figure 8 testing detection Genre network using Kali Linux tools Wireshark, where the tools could detect and view temporary data in the process of transferring to the server. So with testing, this message control sent faucet from IP Addresses 192.168.0.7 data that was successfully detected in form encryption. Or no one could read.

Moreover, Figure 9 tests the detection Genre network using Kali Linux tools Wireshark, where the tools could detect and view temporary data in transferring to the server. So with testing, this message control sent fan from IP Addresses 192.168.0.6 data that was successfully seen in form encryption or no could read.

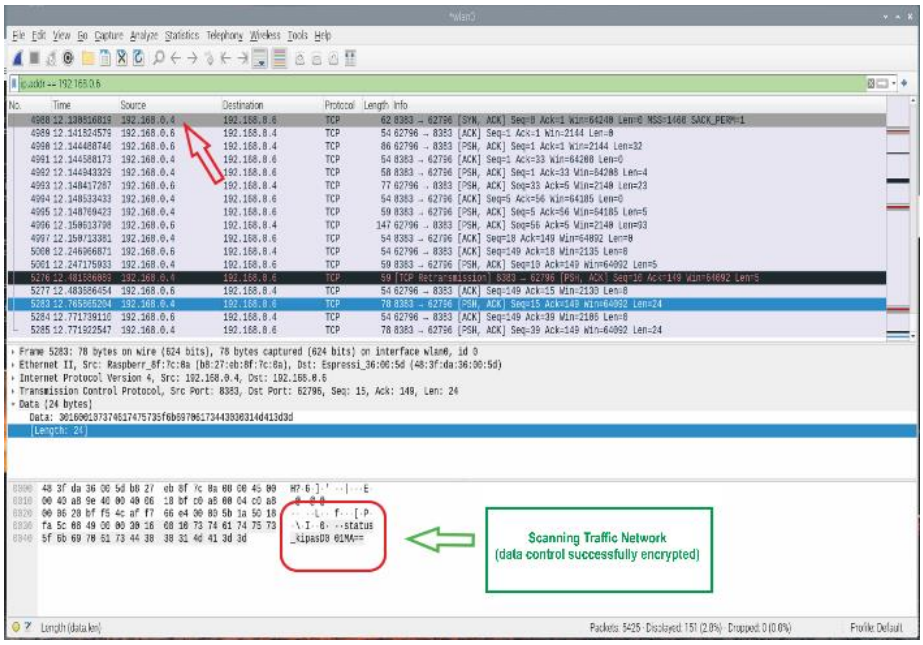


***Fig.9*** Capture controls fan encrypted Sensors A Traffic Wireshark

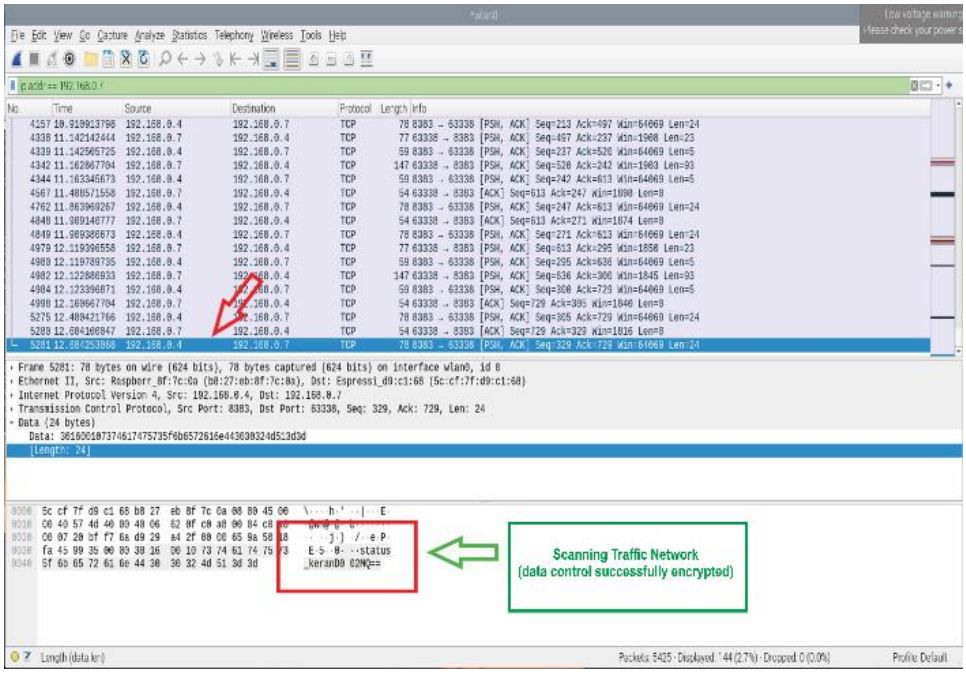


***Fig.10.*** Full Capture tap encrypted Sensor B Traffic Wireshark

Figure 10 testing detection Genre network using Kali Linux tools Wireshark, where the tools could detect and view temporary data in the process of transferring to the server. So with testing, message control sent a faucet from sensor B with IP Addresses 192.168.0.7 data that was successfully detected in form encryption or no could read.

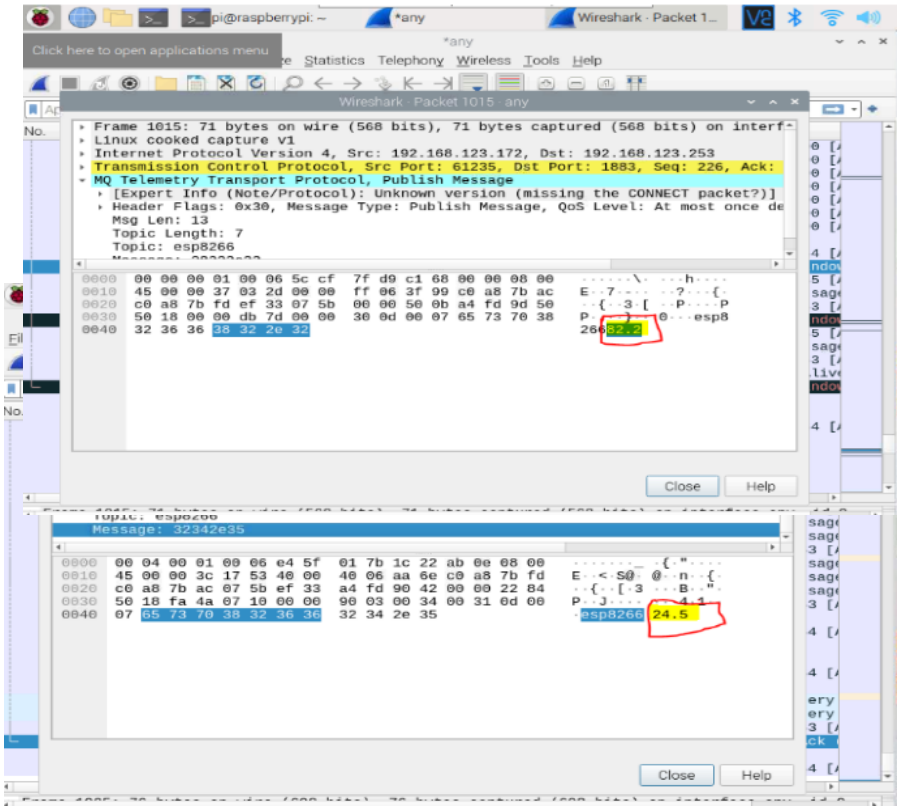


***Fig.11*** Capture without BASE64 encryption sensors A Traffic Wireshark

Figure 11 is testing without Base64 encryption using capture network traffic to see the Genre network When Esp 8266 sends data to a raspberry pi server. It could be seen that the data is in the process of transfer without the use of Base64 encryption is then very easy To do data reading using Wireshark.

*4.3 Test Results Base64 encryption*

*4.3.1 Sensor node A*

The trials we did here were to see the data sent by the sensor node to the monitoring application. Will see whether the data flowing on the network between sensor nodes to the application server can be read or not. Table 1 shows the results reading of one of the sensor nodes (sensor node A). Tested five times on sensor node A and will see results from the temperature sensor and humidity sensor readings on this node.

***Table 1.*** Test Results Data on sensor node A encryption

| No | ID_Device | Temperature | Humidity |
|---|---|---|---|
| 1 | D001 | NZMA | NjYA |
| 2 | D001 | NZuA | NTUA |
| 3 | D001 | NzQA | NjmA |
| 4 | D001 | NjCA | NTKA |
| 5 | D001 | NzQA | NDYA |

*4.3.2 Sensor node B*

Table 2 shows the results of other sensor node readings again (sensor node B). Here also carried out five tests on sensor node B and got seen results from the temperature sensor and humidity sensor readings on this node.

***Table 2.*** Test Results Data on sensor node B encryption

| No | ID_Device | Temperature | humidity |
|---|---|---|---|
| 1 | D002 | NzuA | NTUA |
| 2 | D002 | NTUA | NJAA |
| 3 | D002 | NTMA | NJEA |
| 4 | D002 | NDMA | NTGA |
| 5 | D002 | NTUA | NTCA |

*4.3.3 Encryption Results of message control for sensor node A*

Furthermore, we need to test the control data sent by farmer users to ask the sensor node to do to existing devices in the garden, like faucets and fans. Table 3 and Table 4 show reading test results commands the user gives.

***Table 3.*** Test Results encryption of message control for sensor node A

| No | ID_Device | Tap | Fan |
|---|---|---|---|
| 1 | D001 | MQ== | MA== |
| 2 | D001 | MA== | MA== |
| 3 | D001 | MQ== | MA== |
| 4 | D001 | MQ== | MA== |
| 5 | D001 | MA== | MA== |

*4.3.4. Encryption Results of message Control for Sensor node B*

***Table 4.*** Test Results encryption message

| No | ID_Device | Tap | Fan |
|---|---|---|---|
| 1 | 002 | MA == | MQ== |
| 2 | 002 | MA == | MA == |
| 3 | 002 | MQ== | MQ== |
| 4 | 002 | MA == | MA == |
| 5 | 002 | MQ== | MA= |

## 4. DISCUSSION

Method Encryption is implemented to keep the data so it doesn't because no one can read data When in the sending process. Mechanism work done This Base64 encryption; When the ESP 8266 has to receive data from the DHT22 sensor, then the information initially in form number will automatically convert form strings and letters random, which is not could read. When that data is sent to the inside raspberry pi server, circumstances have been encrypted, or no one can read it. the data has until to the MQTT server and the Mysql database will

occur an opener or key from the so-called encryption description, with the goal so When User Interfaces To do calling for displayed then the data is sent in form encryption just now will convert into description data or readable data. Testing encryption has been conducted using Kali Linux tools Wireshark scanning data stream sent and visible clear the data sent from ESP 8266 encrypted or inside data form random which is not can be read

If compared with the system, Smart Farming without Base 64 encryption is straightforward to read using the kali Linux tool Wireshark so that somebody could View original data and conditions circumstances kumbung mold cultivation mold oysters.

Based on the results study Secure Wireless Sensor Network on cultivation mold oysters that have been tested method Base64 encryption can be concluded that could secure data with method to do Encryption or letter random which is not could read When in the transfer process and the server.

## 5. CONCLUSIONS

On research, this has succeeded apply Base64 encryption on the system Smart Farming Cultivation mold oyster with method data work to be sent from ESP 8266 will do the encryption process then forwarded to the raspberry pi server and when it comes to raspberry pi server MySQL database then (User Interfaces) UI does calling for displayed on the monitoring page then in a manner automatic encryption key that has been programmed on ServerMQTT will work so that the data is displayed data that can be read or in original data form. For the next research, we need to guarantee data integrity, for example, implementing digital signatures on WSN or IoT systems in general and intelligent farming systems in particular.

## AUTHOR CONTRIBUTIONS

Conceptualization; Abdul Wahid [AW], Ilham Juliady [IJ], Satria Gunawan Zain [SGZ], Jumadi Mabe ParenrengJ [J.M.P], methodology; [AW],[IJ],[SGZ],[JMP]; validation; [AW],[IJ],[SGZ],[JMP], formal analysis; [AW],[IJ],[SGZ],[JMP], investigation; [AW],[IJ],[SGZ],[JMP], data curation; [AW],[IJ],[SGZ],[JMP], writing—original draft preparation;[AW],[IJ],[SGZ],[JMP]; writing—review and editing; [AW],[IJ],[SGZ],[JMP], visualization; [AW],[IJ],[SGZ],[JMP], supervision [AW],[IJ],[SGZ],[JMP], project administration; [AW],[IJ],[SGZ],[JMP], funding acquisition; [AW],[IJ],[SGZ],[JMP], have read and agreed to the published version of the manuscript.

**ACKNOWLEDGMENTS**

Thanks to all the team at Computer Engineering, Makassar State University, Makassar, South Sulawesi, Indonesia, who have worked hard in completing this article so that this article can be published in this journal.

**CONFLICTS OF INTEREST**

The authors declare no conflict of interest.

## REFERENCES

1. A. M. L. Afit Dan Y. B. Yusuf, "Analisis Sistem Pengelolaan, Pemeliharaan Dan Keamanan Jaringan Internet Pada It Telkom Purwokerto," Evolusi, Vol. 6, No. 2, 2018, Doi: 10.31294/Evolusi.V6i2.4427.
2. R. Rosmiah, I. S. Aminah, H. Hawalid, Dan D. Dasir, "Budidaya Jamur Tiram Putih (Pluoretus Ostreatus) Sebagai Upaya Perbaikan Gizi Dan Meningkatkan Pendapatan Keluarga," Altifani, Vol. 1, No. 1, Des 2020, Doi: 10.32502/Altifani.V1i1.3008.
3. Y. Wibowo, F. E. Prasetyadana, Dan B. Suryadharma, "Implementasi Monitoring Suhu Dan Kelembaban Pada Budidaya Jamur Tiram Dengan Iot," Jtep-L, Vol. 10, No. 3, Hlm. 380, Sep 2021, Doi: 10.23960/Jtep-L.V10i3.380-391.
4. A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android," Sst, Vol. 4, No. 3, Hlm. 110, Jun 2018, Doi: 10.36722/Sst.V4i3.280.
5. D. Y. Rizaldi Dan I. F. Kurniawan, "Implementasi Multichain Sebagai Alternatif Solusi Keamanan Dan Privasi Data Pada Komunikasi Perangkat Pintar Rumah," Jinacs, Vol. 1, No. 02, Hlm. 115–121, Jan 2020, Doi: 10.26740/Jinacs.V1n02.P115-121.
6. R. Dhall Dan V. K. Solanki, "An IoT Based Predictive Connected Car Maintenance Approach," Ijimai, Vol. 4, No. 3, Hlm. 16, 2017, Doi: 10.9781/Ijimai.2017.433.
7. M. R. L. Rakha, Dr. Ir. R. Munandi. M. T. Rendy, Dan A. I. I. Arif, "Analisis Algoritma Advanced Encryption Standard (Aes) Untuk Sistem Pemantauan Konsumsi Daya Listrik Analysis Of Aes Algorithm For Electrical Power Consumption Monitoring System," 2020.
8. Parta Ibeng, "Pengertian Data Adalah - Fungsi, Jenis Dan Contohnya Lengkap," 2022. Https://Pendidikan.Co.Id/Pengertian-Data/ (Diakses 13 April 2022).
9. Abdul Wahid, Retantyo Wardoyo, Dan Jumadi, "An Implementation Of Audio Security Using Des Algorithm," 2021.
10. A. H. Saptadi, "Perbandingan Akurasi Pengukuran Suhu Dan Kelembaban Antara Sensor Dht11 Dan Dht22," Vol. 6, No. 2, Hlm. 8, 2014.
11. Prastyo, "Arsitektur Dan Fitur Esp32 (Module Esp32) Iot - Edukasi Elektronika | Electronics Engineering Solution And Education," 2020. Https://Www.Edukasielektronika.Com/2019/07/Arsitektur-Dan-Fitur-Esp32-Module-Esp32.Html (Diakses 28 Maret 2022).
12. Abdul Wahid, Muhammad Eka Firdaus, Dan Jumadi Mabe Parenreng, "Implementation Of Wireshark And Ip Tables Firewall Collaboration To Improve Traffic Security On Network Systems," 2021.
13. R. Novrianda Dasmen, "Implementasi Raspberry Pi 3 Sebagai Wireless Access Point Pada Stiper Sriwigama Palembang," Jpit, Vol. 3, No. 3, Hlm. 387–393, 2018, Doi: 10.30591/Jpit.V3i3.943.

14. R. Novrianda Dasmen Dan . R., "Implementasi Raspberry Pi 3 Pada Sistem Pengontrol Lampu Berbasis Raspbian Jessie," Jepin, Vol. 5, No. 1, Hlm. 46, 2019, Doi: 10.26418/Jp.V5i1.29720.
15. D. B. Nurcahyo Dan S. Amini, "Implementasi Kriptografi Dengan Algoritma Base64 Dan Advance Encryption Standard Untuk Mengamankan Data Email Berbasis Web," Vol. 1, No. 3, Hlm. 8, 2018.
16. T. Apri Triansyah, "Authentifikasi Login User Pada Perangkat Lunak Menggunakan Arduino Dan Enkripsi Aes 256," 2017.