International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Internet Data Security System using AES256 Encoding Technique

Pamarthi Kanakaraja, Vemuri Sahithi, Katari Ramyavani, Donepudi Richa

Abstract: ***Now a days 60% of communication are done only through internet based in this circumstance data security is very important while we are communicating through any internet based networks like cloud, servers etc. With the help of some few sensors like temperature, alcohol or gas sensor data encrypted. In AES256 standard, the sensors convert the plain text into cipher text (which is not understandable) and it is uploaded to the cloud on the transmitter side. On the receiver side we can decode the data only with the help of AES256 key and hash code which are used on the transmitter side. In between this process any person is trying to hack the data he cannot get the original data because the data is in the form of cipher text format.***

Key Words*: *AES256, Cloud, Secret Key, Encryption, Decryption.

I. INTRODUCTION

Now a days the internet plays a very major role in our daily life. In the present society the information is being received and misused by the people in that situation a lot of security threats arises [1]. 2 types of encryption in use, they are symmetric type and asymmetric type [4]

i) Symmetric key: encryption using secret keys. In this technique, the sender and the receiver use the same key to reveal the hidden text or image. Each sender and receiver has to encrypt the original message and decrypt message cipher text format.

ii) Asymmetric key: encryption uses both public and private keys. Asymmetric cryptography, also known as public_ key cryptography. In this technique we use completely two different keys one to lock or encrypt the plain text, and one to unlock or decrypt the cipher text. The keys are simply larger but are not identical. Depending upon the present condition of worldwide industrial Internet growth, this paper examines the fresh demands of industrial Internet expansion on network, read the collection and integration of industrial huge data, and examines the data handling and security difficulties facing industrial Internet in the upcoming future [2].

Manuscript published on November 30, 2019.
* Correspondence Author
P.Kanakaraja*, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram,.
V.Sahithi, Department of Electronics and Communication Engineering , Koneru Lakshmaiah Education Foundation, Vaddeswaram
K.Ramyavani, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram
D.Richa, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram

Cloud computing is developed for various facilities like networking, security, storage. From anywhere in the world one can access various applications and software with the help of the 3rd party as cloud [4]

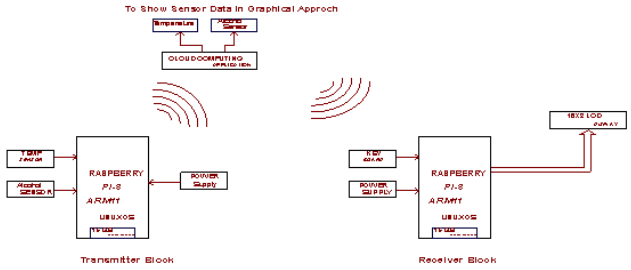
In cloud computing privacy and security is more important because here a large amount of data is transferred due to which the hackers are increasing day by day.Cloud Computing is an most demanded profitmaking computing transfer of database, storage, applications, compute power and a small number of IT resources through a cloud services raised area via internet with pay as you use course of action provided by the service provider [3].The Cloud Computing idea implies that anything that can be facilitated on the web, i.e., resources, administrations, information is accessible for use, when required, for the organization and arrangement of increasingly complex administrations. It portray server farms accessible to numerous clients over the Internet. Enormous mists, dominating today, regularly have capacities appropriated over various areas from focal servers. Distributed computing imparts qualities to Client–server model Grid processing, Fog figuring ,Mainframe PC ,Utility registering, Peer-to-peer, Green figuring ,Agility(as distributed computing may build clients adaptability with re-provisioning, including, or growing innovative framework resources),Cost decreases(purportedly brings hindrances down to section, as foundation is ordinarily given by an outsider and need not be acquired for one-time or rare concentrated registering assignments) Maintenance, Multitenancy, Productivity, Reliability, Security. The Cloud Computing isn't just sharing the assets yet additionally augmenting the assets. It is additionally area free and access the cloud administrations from any area and with any gadgets through web association. The virtualization of p hysical gadgets is another significant attributes, virtualization enable clients to share the gadgets. Multitenancy highlight of distributed computing empowers sharing of assets to various clients over spatial and time appropriation. What's more, Cloud offer elasticity and adaptable of assets and application, the administration and assets are effectively open and accessible**.** Services established on cloud computing technology and permit operators to store big files or use software on a server path over the internet. One in five characters put in storage files on internet servers [5].In the similar way the internet provide us benefits as well as it also raises a lots of security threats.

II. LITERATURE SURVEY

In 2019, J. Lin et al. [2] initially there are a lot of tasks in operation of Industry Internet, for sample: IT security problems. The Industrial Internet want big-scale network set-up to offer care, and data-driven system constructions run possible answers. The major problem is create the organization slower than before and stealing of private data.
In 2019, X. Jing et al. [1] Network spasms are the main dangers for safe keeping over the web have involved special care. The honesty and interconnection of the network and the security exposures of protocols and software main to several and multilevel network spasms. In 219, Y. Hui et al. [3] The present model accepts not the same keys for the 3 stages of data privacy (i.e. no confidentiality, incomplete confidentiality and solid confidentiality) depending on the data sensitivity stages. This model confirms the end-to-end security by shielding the data from source device to cloud.

III. PROPOSED METHODOLOGY

In this project along with the AES secret key additionally hash code (i.e., hash code is nothing but password) is also used to secure the data. There is no limit for the hash code so it is difficult for the person (hackers) to hack the original data. Whatever the hash code and the AES key used at the transmitter side to encrypt the data same key and the hash code should be used at the receiver side to decrypt the data then only the cipher text is converted into plain text. Here 256 bit encryption is used which contains 2^256 combinations which is very complex to hack the original data.



In this above block diagram, taken two raspberry pi. One is transmitter side and another receiver side. Given the power supply to raspberry and taken two sensors one is DHT11 which means to measure temperature and humidity and another one is MQ2 (alcohol) which means to measure smoke leakage sensor. Connecting the sensors and the raspberry pi to the power supply. Sensors are used to read the input data. For that data we have to give password and AES secret key (advance encryption system) to the raw data. After applying both AES secret key and password the data will be encrypted. The encrypted data is sent to the cloud. After cloud computing, the data will be decrypted. The decrypted data is send to the receiver block. Again applying same key and password to the decrypted data. Finally, the encrypted data text is converted into the decrypted text. The decrypted data text is displayed in the 16*2 LCD liquid crystal display.

IV. METHODOLOGY

In this paper different types of devices are used i.e., which are explained below

A. Raspberry Pi

Raspberry pi is nothing but a small size computer it is in the size of a credit card and it is a best-selling computer in the world ranked at 3rd place. We can connect this minicomputer to display or TV, and a keyboard. Majorly it is used to learn for coding and to build a great electronic projects. In our project we used RASPBERRY PI 3 MODEL B+, having special features like speed is 1400MHz , RAM is 1GB , having 4 USB ports , Ethernet is 1000Base-T , soC is BCM2837B0 . As Raspberry Pi 3 model B+ is more capable than the earlier models so are going to use in this project [6]. In March 2018 this raspberry pi 3 b+ model was launched. Raspberry pi 3 b+ model works more effectively than a modern computer. We have to buy SD card separately because raspberry pi does not have this SD card feature, here we used 16 GB Samsung micro SD card. Micro Secure digital is a kind of removable flash memory card and it is used for storing information or data Raspberry pi OS can be switched very easily and it is low cost compared to normal computer. The (SOC) System on Chip is a Raspberry Pi Computer, a plan where a single board transmits all the needed circuits, such as the (CPU) Central Processing Unit, the (GPU) Graphics Processing Unit, and a number of input, output and processing circuits [7]

Figure1: Structure of Raspberry Pi 3 b+

B. DHT11

In this project dht11 is used to take the temperature and humidity values as the input. Operating Voltage is 3.5V to 5.5V and Operating current is 0.3mA (measuring) 60uA (standby) .output of DHT11 is serial data and temperature varies from 0°C to 50°C. Humidity Range is20% to 90%. Resolution is Temperature and Humidity both are 16-bit. Accuracy is ±1°C and ±1%.

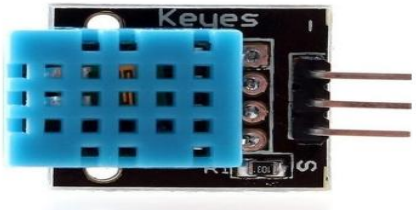


Figure2: Structure of DHT1

C. MQ2

MQ2 is the smoke sensor used in this project.MQ2 is an electronic sensor used for sensing the concentration of gases in the air like carbon-di-oxide and some other gases.
MQ2 be a metal chemical compound semiconductor type of gas detector. Concentration of gases within the gas are measured employing a potential divider network gift within the detector. It will discover within the concentrations of 10000ppm.

Figure3: Structure of MQ2 gas sensor

D. ADC

In our project internet data security system we use ADC (analog to digital converter) separately. Because raspberry does not has that analog to digital converter feature. ADC is a circuit that converts an unbroken voltage value of (analog) signal to binary value (digital) signal that is ones and zeros that can be understood by a digital device.

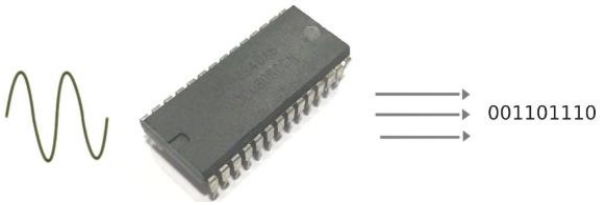


Figure4: Structure of ADC

E. Encryption

Encryption is the procedure of changing normal text to cipher-text (had to understand) by applying mathematical changes. These changes are also named as encryption algorithms and need an encryption key. In computing, unencrypted information is named as plain text, and the encrypted information is named as cipher text. The principles which are used to encrypt and decrypt communications are known as encryption algorithms or ciphers. In encryption initially the characters are in plain text cover the real information with the support of calculating ASCII code values of unique characters, in order to stop being cracked easily.

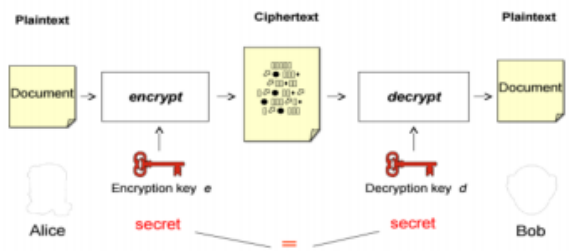


Figure5: Symmetric key Encryption

Figure6: Asymmetric Key Encryption

F.AES 256

AES256 is a symmetrical encryption algorithm that has become universal. .Because of the length of the key is (256 bits) and the number of hashes is (14), it takes a viciously long time for a malicious software hacker to perform a dictionary attack. Conclusion of a stream or stored data won't likely happen in your lifetime, or in the next 100 lifetimes. AES has major advantage which means to implement in either hardware or software. Advanced Encryption Standards is a symmetrical encryption function. It takes input as 256 data bit block and do the action of conversion stages to get cipher text as output.

G. AES working

Advanced Encryption symmetrical cipher works on identical secret key is used for both encryption and decryption, and both the transmitter and receiver require a copy of that key. But, asymmetrical key uses unique key for each on the two processes and it good for external file transfers.
Cipher text format is nothing but an encrypted text format .plain text means the data before the encryption. Cipher text is divided in two types one is substitution cipher means it replaces the characters and another one is transposition cipher means characters should rearrange their position. By applying the AES secret key and hash code (password) to the sending data. When it comes to encryption the plain text is converted into cipher text which is in cyber text format so hacker does not know the language of the data text. When it comes to decryption the cipher text is converted to original plain text.

H. 256 Bit Encryption

Advanced encryption system is also identified as block cipher. The information to be in plain text (encryption) is divided into section called blocks. AES uses 256 block size. Size of each block is measured in bits. AES 256 uses 14 rounds of encryption. It has the more rounds, the more complicated the encryption, so AES 256 is the most secure AES implementation. AES 256-bit encryption is refers to the length of the encryption key used to encrypt a data. A hacker will require $2^{\wedge 256}$ unique combinations to break a 256-bit encrypted message .By using 256 bit encryption hacker impossible to hack any system data. It is one of the most and best encryption methods for security after 128- and 192-bit encryption, and is used in most modern encryption algorithms

I. Circuit Diagram

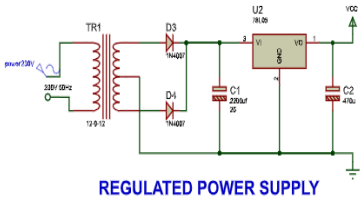


Figure7: Regulated power supply

This is the regulated power supply of the system.

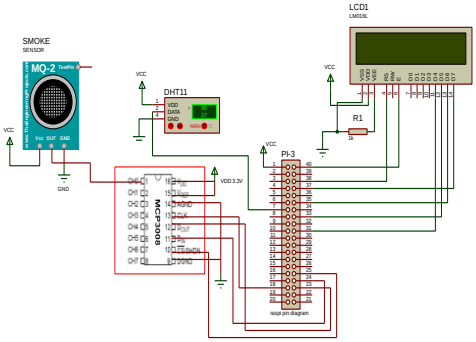


Figure8: 8.circuit diagram of "Internet Data Security System using AES 256"

In this circuit diagram we use ADC, Raspberry pi, DHT11, MQ2 and Power supply. All are connected as shown in a above figure

V.FLOW CHART

A. Transmitter Side

On transmission side, we have to perform encryption first we have initialize 16*2 LCD display and AES256 algorithm. Further we have to enter the encryption password to get the temperature and humidity values from ada fruit library and again perform encryption AES256 and hash code. Encrypted data is uploaded to the thing speak cloud with the help of API key and analysis based on temperature and humidity using thing speak iot.

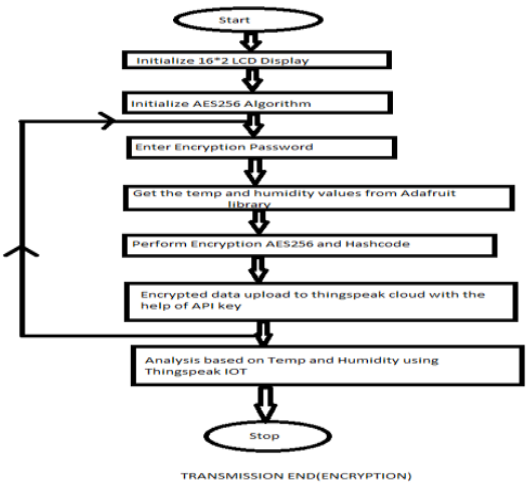


Figure9: Flow chart of data encryption on Transmitter side

B. Receiver End

On the receiver side we have to perform decryption, first we have to get the data from the thing speak with the help of channel id. The cipher text need to be converted into normal format text and apply AES 256 decryption algorithm to get the original data. Finally we get the original data.

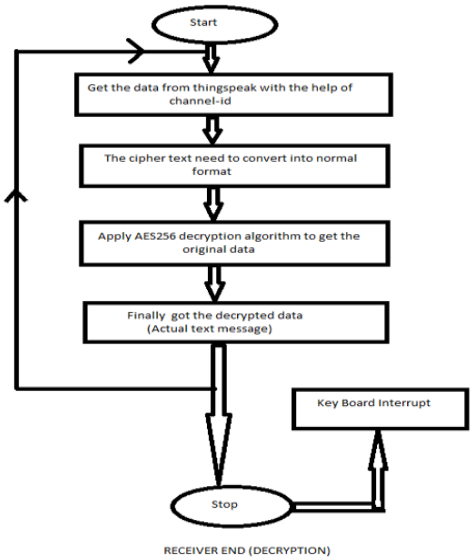
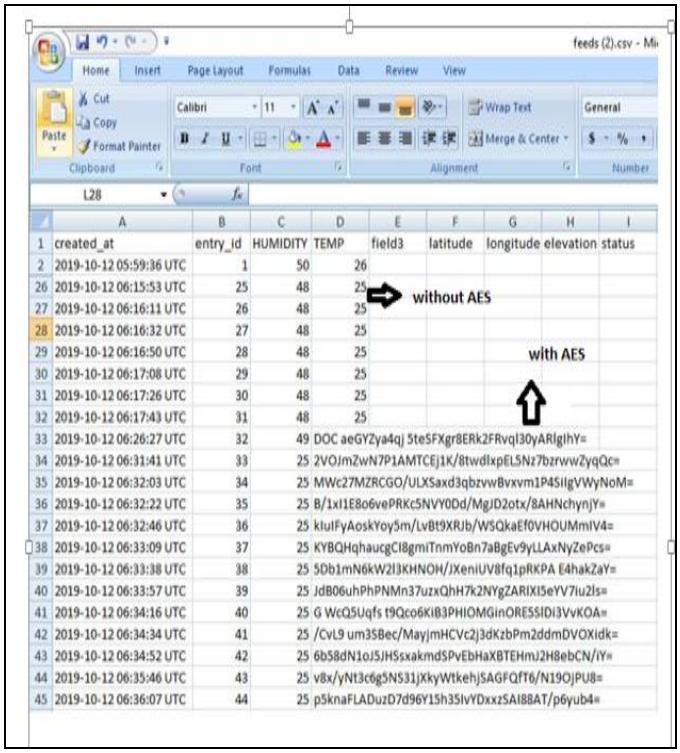


Figure10: Flow chart of data decryption on receiver Side

VI. RESULTS AND DISCUSSION



	A	B	C	D	E	F	G	H	I
1	created_at	entry_id	HUMIDITY	TEMP	field3	latitude	longitude	elevation	status
2	2019-10-12 05:59:36 UTC	1	50	26					
26	2019-10-12 06:15:53 UTC	25	48	25					
27	2019-10-12 06:16:11 UTC	26	48	25					
28	2019-10-12 06:16:32 UTC	27	48	25					
29	2019-10-12 06:16:50 UTC	28	48	25					
30	2019-10-12 06:17:08 UTC	29	48	25					
31	2019-10-12 06:17:26 UTC	30	48	25					
32	2019-10-12 06:17:43 UTC	31	48	25					
33	2019-10-12 06:26:27 UTC	32	49	DOC aeGYZya4qj 5teSFXgr8ERk2FRvql30yARlgihY=					
34	2019-10-12 06:31:41 UTC	33	25	2VOJmZwN7P1AMTCEj1K/8twdlxpEL5Nz7bzrvwZyqQc=					
35	2019-10-12 06:32:03 UTC	34	25	MWc27MZRCGO/ULXSaxd3qbzvwBvxvm1P45IlgVWyNoM=					
36	2019-10-12 06:32:22 UTC	35	25	B/1x1E8o6vePRKc5NVY0Dd/MgJD2otx/8AHNchynjY=					
37	2019-10-12 06:32:46 UTC	36	25	kIuIFyAoskYoy5m/LvBt9XRJb/WSQkaEf0VHOUMmIV4=					
38	2019-10-12 06:33:09 UTC	37	25	KYBQHqhaucgCI8gmiTnmYoBn7aBgEv9yLLAxNyZePcs=					
39	2019-10-12 06:33:38 UTC	38	25	5Db1mN6kW2l3KHNOH/JXeniUV8fq1pRKPA E4hakZaY=					
40	2019-10-12 06:33:57 UTC	39	25	JdB06uhPhPNMn37uzxQhH7k2NYgZARIXI5eYV7iu2ls=					
41	2019-10-12 06:34:16 UTC	40	25	G WcQ5Uqfs t9Qco6KiB3PHIOMGinORE5SIDi3VvKOA=					
42	2019-10-12 06:34:34 UTC	41	25	/CvL9 um3SBec/MayjmHCVc2j3dKzbPm2ddmDVOXidk=					
43	2019-10-12 06:34:52 UTC	42	25	6b58dN1oJ5JHSsxakmdSPvEbHaXBTEHmJ2H8ebCN/iY=					
44	2019-10-12 06:35:46 UTC	43	25	v8x/yNt3c6g5NS31jXkyWtkehjSAGFQfT6/N19OjPU8=					
45	2019-10-12 06:36:07 UTC	44	25	p5knaFLADuzD7d96Y15h35IvYDxxzSAI88AT/p6yub4=					

Figure 11:Original data and the encrypted data

Figure 9 describes initially plain text is taken as input after applying AES key it is converted into cipher text format which is not understandable by anyone until it is converted into plain text.

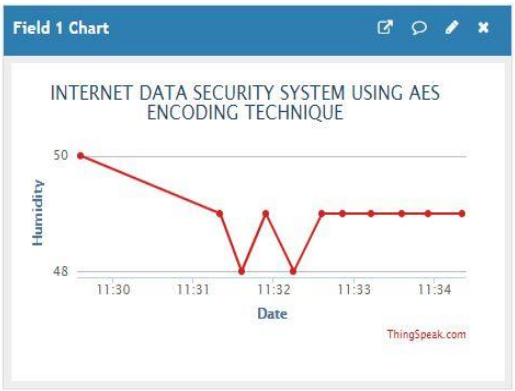


Figure 12:Date vs Humidity

Figure 12 describes the graph is plotted between date and humidity using thing speak id the humidity value varies according to the date initially the humidity value is high after sometime its value get decreasing and the fluctuation in the graph continues.

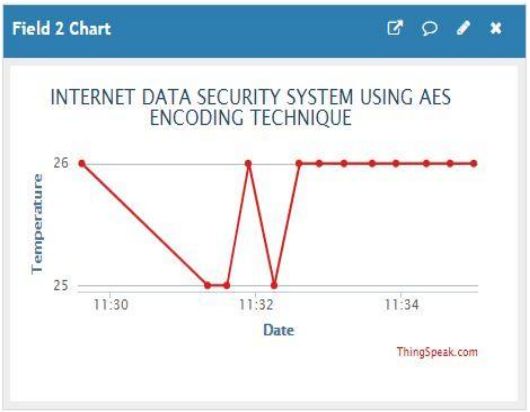


Figure 13:Date vs Temperature

Figure 13 describes describes the graph is plotted between date and temperature using thing speak id the temperature value varies according to the date initially the temperature value is high after sometime its value get decreasing and again gets increasing and this fluctuation in the graph continues

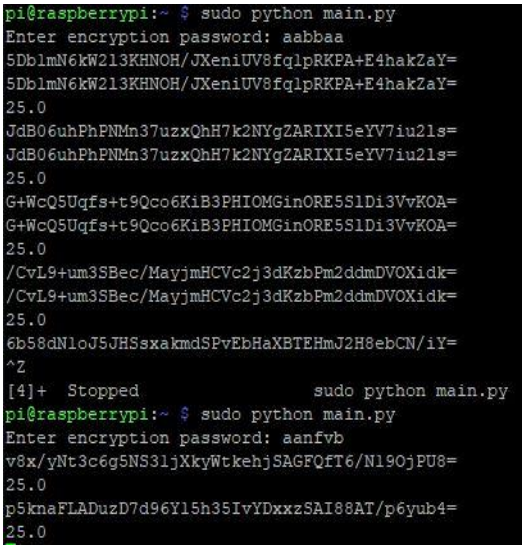


Figure14:Compilation Process

Figure 14 describes the entire compilation process After entering the password the given data is converted into cipher text.There is no size limit for the password.

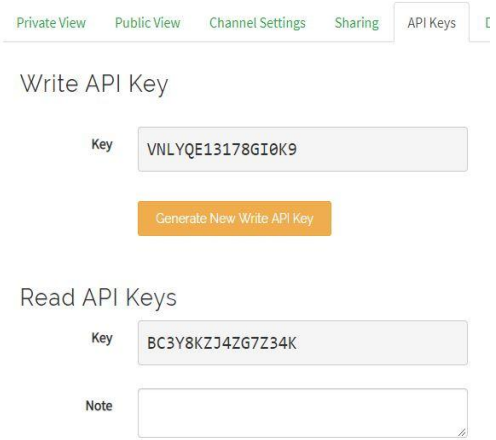


Figure15:Write and Read API keys

Figure 15 decribes the write keys and the read keys

created_at	entry_id	field1	field2	field3
2019-10-12 05:	1	50	26	
2019-10-12 06:	2	49	25	
2019-10-12 06:	3	48	25	
2019-10-12 06:	4	49	26	
2019-10-12 06:	5	48	25	
2019-10-12 06:	6	49	26	
2019-10-12 06:	7	49	26	
2019-10-12 06:	8	49	26	
2019-10-12 06:	9	49	26	
2019-10-12 06:	10	49	26	
2019-10-12 06:	11	49	26	
2019-10-12 06:	12	49	26	
2019-10-12 06:	13	49	26	
2019-10-12 06:	14	49	26	
2019-10-12 06:	15	48	25	
2019-10-12 06:	16	48	25	
2019-10-12 06:	17	49	26	
2019-10-12 06:	18	49	26	
2019-10-12 06:	19	49	26	
2019-10-12 06:	20	49	26	
2019-10-12 06:	21	48	25	
2019-10-12 06:	22	49	26	

Figure16: Record entry of field1 and field2

Figure16 describes the field1 indicate the humidity values and the field2 indicates the temperature values

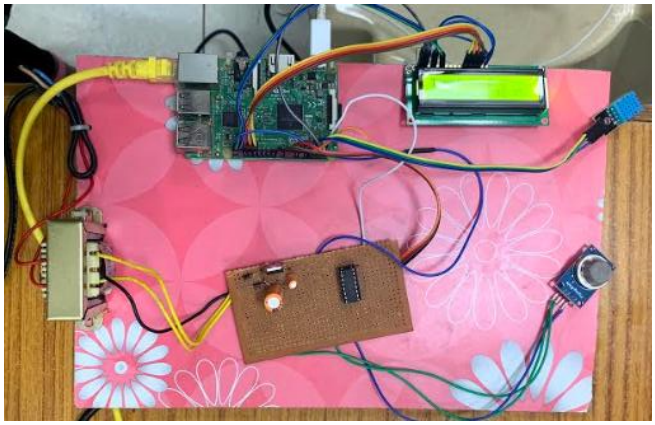


Figure17: Overview of the entire connection of the system

MQ2 is connected to ADC, then ADC is connected to the power supply. Power supply is given to the raspberry pi and the final result displayed on LCD.

Figure16: Output on LCD

Finally we get temperature and humidity on LCD display

VII. CONCLUSION

The AES (advanced encryption system) algorithm gives significant level security hacker does not know about the data that is hidden. In this manner the hacker will not have the option to retrieve the data. By utilizing this propelled encryption methods AES256 we can shield the web information from horseback riding. Since 60% of correspondence are done through web based as it were. Thus, we need to verify the information from this methods. Just the individual with appropriate confirmation will have the option to recover the data. Accordingly this framework can be utilized in different fields where the information must be transmitted in a verified manner.

REFERENCES

1. X. Jing, Z. Yan and W. Pedrycz, "Security Data Collection and Data Analytics in the Internet: A Survey," in *IEEE Communications Surveys&Tutorials*,vol.21,no.1,pp.586-618,Firstquarter2019
2. J. Lin and L. Liu, "Research on Security Detection and Data Analysis for Industrial Internet," *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Sofia, Bulgaria, 2019, pp. 466-470
3. Y. Hui and L. Zesong, "Research on Real-time Analysis and Hybrid Encryption of Big Data," *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, Chengdu, China, 2019, pp. 52-55.
4. G. R. Karsanbhai and M. G. Shajan, "128 bit AES implementation for secured wireless communication," *2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, Udaipur, 2011, pp. 497-501.
5. S. Manjula, M. Indra and R. Swathiya, "Division of data in cloud environment for secure data storage," *2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)*, Kovilpatti, 2016, pp. 1-5.
6. A. Pawar and V. M. Umale, "Internet of Things Based Home Security Using Raspberry Pi," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018, pp. 1-6.
7. N. S. Yamanoor and S. Yamanoor, "High quality, low cost education with the Raspberry Pi," *2017 IEEE Global Humanitarian Technology Conference (GHTC)*, San Jose, CA, 2017, pp. 1-5.
8. A. Pawar and V. M. Umale, "Internet of Things Based Home Security Using Raspberry Pi," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018, pp. 1-6.
9. . Margret Sharmila, P. Suryaganesh, M. Abishek and U. Benny, "Iot Based Smart Window using Sensor Dht11," *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, 2019, pp. 782-784.
10. A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636.
11. N. S. Yamanoor and S. Yamanoor, "High quality, low cost education with the Raspberry Pi," *2017 IEEE Global Humanitarian Technology Conference (GHTC)*, San Jose, CA, 2017, pp. 1-5.

AUTHORS PROFILE

Pamarthi Kanakaraja currently working as Assistant Professor in Koneru Lakshmaiah Education Foundation (Deemed to be University). He has 8 Years working experience On Embedded Designing & Programming Concepts. He is Technical EMBEDDED DESIGNING concepts Adviser for many Engineering and Polytechnic (DIPLOMA) Students. He also published papers in various international journals. He is a Regular Contributor in EFY (Electronic for You) International Technical magazine. His area of research is Embedded Designing, Internet of Things (IOT) & Artificial Intelligence (AI).

Vemuri Sahithi, studying B.Tech in Koneru Lakshmaiah Education Foundation, Department of Electronics and Communication Engineering.

Katari Ramyavani, studying B.Tech in Koneru Lakshmaiah Education Foundation, Department of Electronics and Communication Engineering. Done minor projects on home automation system using microcontroller.

Donepudi Richa studying B.Tech in Koneru Lakshmaiah Education Foundation, Department of Electronics and Communication Engineering.