IOT BASED SERVER ROOM MONITORING SYSTEM

[1] Navneet Kaur, [2] Dr.Abhinav Bhandari,
[1]Student, [2]Assistant Professor
[1] Department of Computer Engineering,
[1]Punjabi University, Patiala, India

Abstract : Internet of Things is one of the most hyped technologies around the world at the moment. IoT, along with cloud and automation is changing the world in which we live and attracting the researchers around the globe. Billions of new objects are connecting with Internet every year and the numbers are increasing at a very fast pace. With lots of benefits of this technology, it has some issues also regarding security and privacy. Information which is shared between sensors and applications over the network is very critical as it can be used by hackers to enter into some application which are controlling home or office devices connected with it. This paper includes the encryption standards used over the internet and a model that sends the humidity, temperature data values collected from the DHT11 sensor connected with an RPi3 and sends data to an application in encrypted form and that application controls the power to the servers according to a threshold level. It needs a lightweight encryption algorithm that works well with the clock cycles that it has.

***IndexTerms* – Internet of Things, Security, DHT11, Raspberry Pi, Relay, Encryption**

I. INTRODUCTION

Internet of Things is the revolutionary concept which is connecting billions of devices with the internet and making automation[1] happen in almost all types of things. It revolves around for parts, i.e. Sense, Collect, Analyze and then React. This concept of future internet is known as Internet of Things. Any independent web associated gadget that are controlled and checked from a remote area is called Internet of Things. The three shared Basic principles are defined by the US National Security and Telecommunications Advisory Committee(NSTAC) :

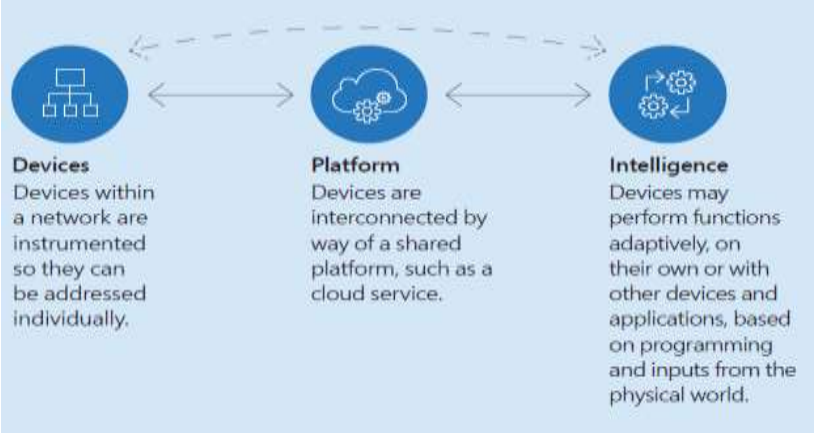


Figure 1: Three Common principles of IoT[4].

The IoT objects are embedded with sensors [6] and microcontrollers [2] and enable them to talk with each other. The objects in IoT can be an anything like people, devices, animals, buildings, vehicle and many more that which is the part of our daily life. For example from every device like mobiles to car, alarms to coffee maker are associated to internet via free source Ipv6[6] provide different identifiers and a transfer data without any help of person and computer interaction. Now thinks that IoT grant as the next advancement of the internet and it has ability to collect, analyze and share data that can helpful for user to gain information. IoT comprises of three things are people, processes and connectivity. It gives a variety of applications like intelligent transportation [5,8] smart cities, smart healthcare[11], smart home, smart buildings, digital farm, agriculture and etc. IoT offers on request continuous and helpful in saving time, resources and manpower. Everything swings to virtual, which means that each individual and things has its own particular place with a specific address on the Internet. These virtual characteristic things can generate and make utilize facilities and cooperate to a standard objective. Various remarkable barriers persist to manage the internet of things insight, amid certainty and safety. The users on the internet always face different threats continuously and the developing wealth crowded with the business models that erode the Internet's moral use which emphasis on exploiting the prevalent version's foundational delicacy. This does not predict well for IoT, which assimilate many constrained devices. The trial is to deflect the development of such models or to decrease their effect. Experiencing these difficulties needs better

understanding the elements and the advances that engage them. Mobile applications already attracting customers with this platform and the sensor devices are also in progress to provide multitude extent of information to enhance the user experience.

Current security and monitoring systems based on Internet of Things are only used for detection [1][2] and the application which is used for monitoring only stores data and send alarming signals to the authorized persons and in the web application UI. But with IoT, we need to have a self-healing system for some problems where manual intervention is needed. There may be issues like an alarm is generated because of temperature threshold reaches peak level and an alarm is generated, but the authorized person who received the alarm did not view that because of either any availability of internet, in case alarm mail is sent or his mobile is switched off, if a message is sent. So, if there is a self-healing system which automatically triggers the instruction to rectify the problem, it can be more secure. There is also needed to have a secure encrypted channel [4] of communication between the controller and the application running on the cloud which stores and processes the data and provides the instruction.

To this end, this paper makes the following contributions:

- To study different application based on Internet of Things.
- To implement IoT based monitoring of Server Room using Raspberry Pi.
- To implement AES, DES based encryption algorithm for sending Server Room's data on Cloud-Application.

II. LITERATURE SURVEY

Our work is inspired by several parallel studies that explore various security issues in IoT. Sawant et al. [1] proposed an intelligent high security for server rooms in industries with help of different sensors like temperature, humidity, light, door etc. They came to conclusion that their system is much better than the other systems that are used in industries now todays. They have provided additional functionality to server room system like live monitoring etc. Narkhede et al. [2] proposed a platform that helps to incorporate all the requirements while developing Hardware monitoring systems. The areas such as environment monitoring,

Pollution monitoring, energy and water management are interlinked to each other. Comparatively, increasing the air condition temperature setting and decreasing the air flow level may save on energy bills but increase the pollution level in the building. Sensor systems deployed for monitoring temperature and humidity may generate real time data but the system developed can readily provide configurations to raise the real time alerts. They compared different events and establishing correlation between various parameters to generate early warning signals such as indication of fire based on changes in the temperature and humidity levels. Abomhara et al. [4] analyzed numerous problems that must be identified for protective measures to be taken. They examined challenges and security problems to IoT. Main focused on to identify assets and document potential threats, attacks and vulnerabilities faced by the IoT. Security challenges, such as confidentiality, availability and integrity trust were examined. They proved that in order to establish more secure and available IoT devices and services, security and privacy challenges need to have unique identities. It was inspected that issues from knowledge offices and criminal gatherings are probably going to be more difficult to crush than those from singular programmers.

Make the patterns in literature survey like to bind the two or more papers related to cryptography schemes. Katagi et al. [3] proposed a Lightweight cryptography algorithm that contributes to the security of smart objects networks because of its efficiency and smaller footprint. We believe that lightweight primitives should be considered to be implemented in the networks. Especially, lightweight block ciphers are practical to use now. C. M et al. [5] analyzed different security frame works are used in IoT environment for providing greater security. They proposed a new method which provides security, privacy, integrity and authentication among peers in static devices. It is based on Zero knowledge protocol and key exchange algorithm. The proposed architecture guarantees perfect forward secrecy. It aims low power consumption and fast computation. Saurabh et al. [14] analyzed various types of lightweight cryptographic calculations that are anything but difficult to use for equipment and programming usage. Some cryptographic calculations are helpless against a few sorts of assaults, which we additionally portrayed in the paper. We likewise examined open issues as far as figure structure, usage, square size, key size, new assaults, and security measurements.

III. PROBLEM STATEMENT

Internet of Things is a charm for hackers as the playground to play. The problem is kind of same as in network i.e. related to CIA (confidentiality, integrity and availability). Devices acting as controllers are using communicating using plain text data in transport which is not secure at all for critical data. With the emergence of data getting important, Data Centers and Server Rooms are increasing at a brisk pace. Data is the most important part of any Industry and is most critical asset too. Data Centers and Server Rooms also needed to be maintained with proper security and alarm systems related with temperature and humidity, energy conservation etc. as services of the data center can be disrupted due to a little problem in monitoring of these entities also. There is also needed to have a secure encrypted channel [4] of communication between the controller and the application running on the cloud8which stores and processes the data and provides the instruction. The aim of this thesis is to enhance the security of server room with the help of IoT.

IV. METHODOLOGY

IoT is the next big thing in the technological sector. Previous IoT Review and Research Papers have been studied and a design is made for IOT based server room monitoring using Raspberry Pi, temperature, humidity sensor and relay. Then python is used

as a scripting language and connected with MySQL database. Temperature and Humidity is measured using Sensors and if the temperature drops below the threshold level, then relay stops the power and the server shuts down automatically. After testing the server room monitoring using RPi, Relay and Python scripting. After testing is made and sending the values in MySQL, data communication is secured. Encryption is a necessary part when sending the critical data over the internet. We have used python scripting to make a hybrid encryption with DES-AES integrated. Plain Text data is generated and before sending, it is converted in to 64 bit cipher and is further go through a 128 bit AES encryption. When the sensors send the data, then the data is sent in the encrypted manner which is being decrypted at the other end using the decrypting code.

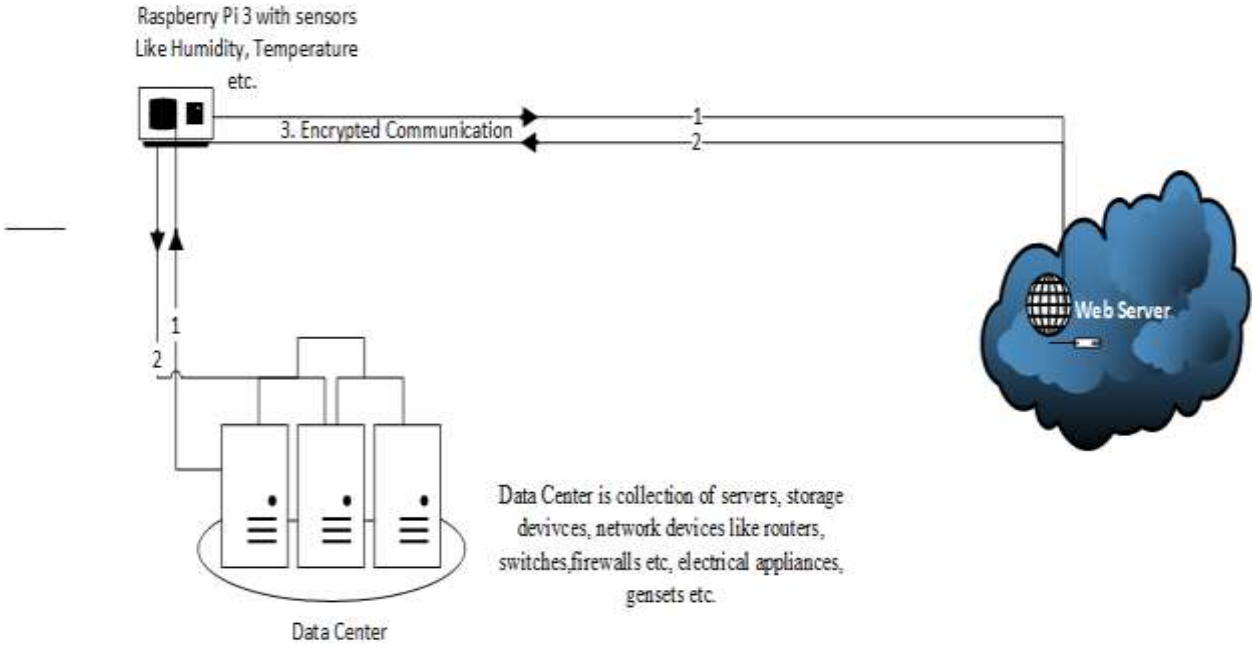
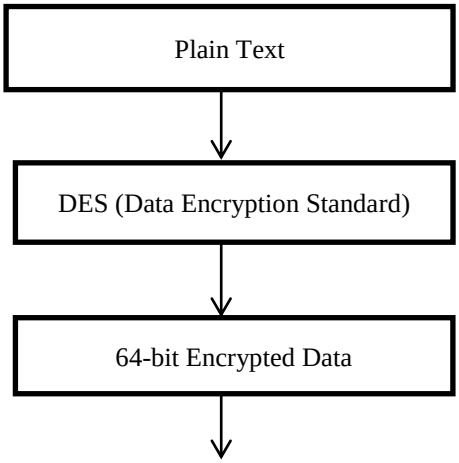
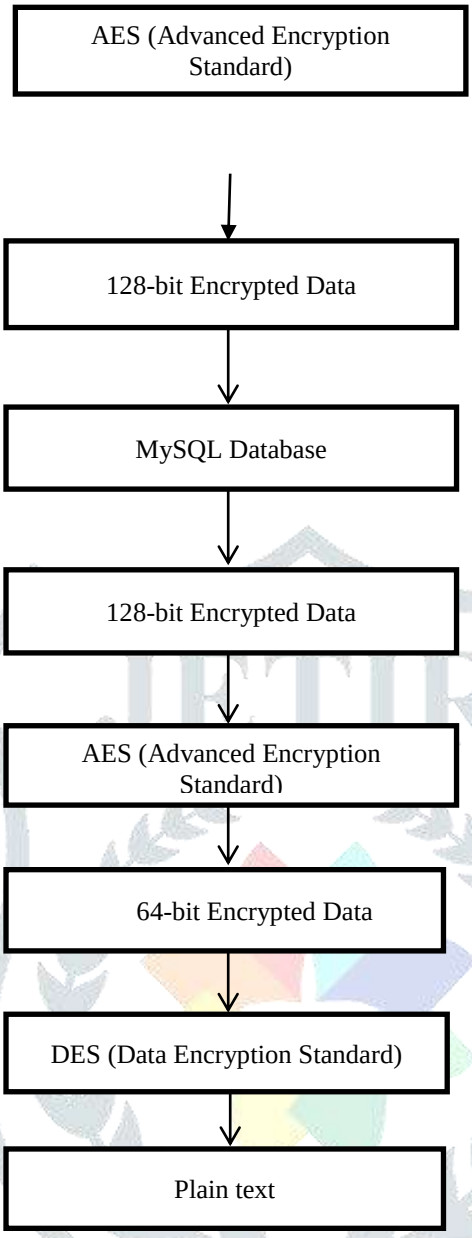


Figure 2: Architecture of IoT Server Room.

1. Raspberry Pi collects data related with temperature, humidity etc. and send it to cloud where a web application will be running.
2. Then that web application stores the data in its database and processes it, if the given parameters reached their peak threshold, then a instruction will be sent automatically to either repair, reload or make the backup device act as primary.
3. For example if there is problem related with temperature, then backup cooling system will come up by getting the instruction from web application.
4. All the communication between controller and application in the Cloud will be encrypted with an Hybrid Encryption Algorithm.

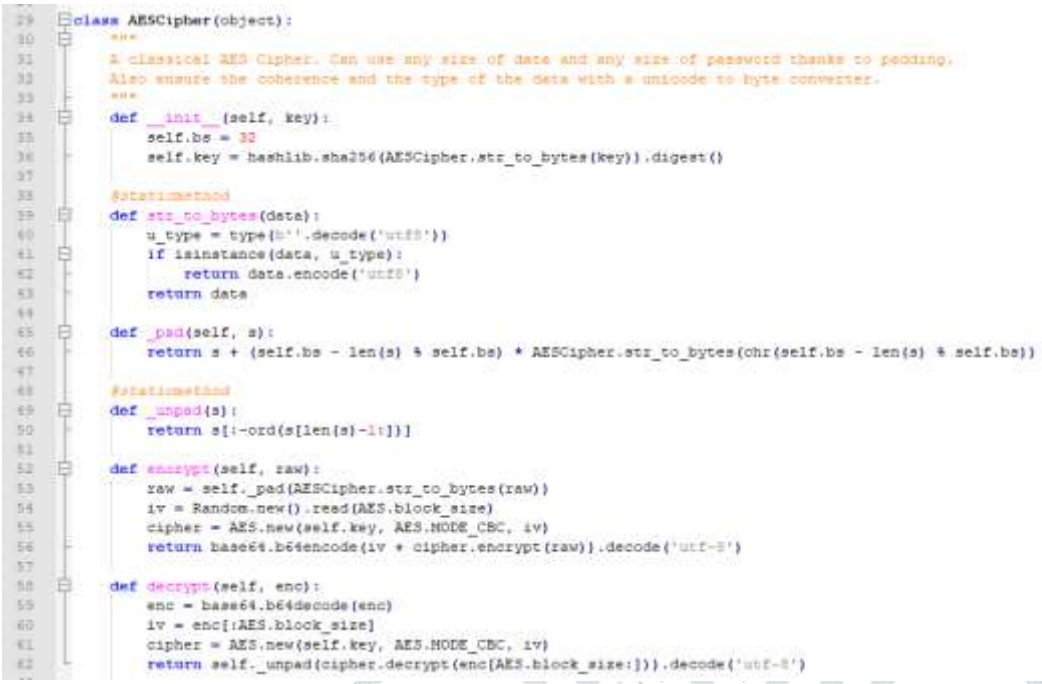
V. FLOW DIAGRAM OF ALGORITHM





Description:

The main idea of this algorithm is to combine AES with each loop of DES and what it does is that it will convert the plain text into 64 bit encryption first and after that the 64 bit cipher is converted into a 128 bit cipher by making it fall over AES. The formula used in this algorithm is:



```
class AESCipher(object):
    """
    A classical AES Cipher. Can use any size of data and any size of password thanks to padding.
    Also ensure the coherence and the type of the data with a unicode to byte converter.
    """
    def __init__(self, key):
        self.bs = 32
        self.key = hashlib.sha256(AESCipher.str_to_bytes(key)).digest()

    @staticmethod
    def str_to_bytes(data):
        u_type = type(b''.decode('utf8'))
        if isinstance(data, u_type):
            return data.encode('utf8')
        return data

    def _pad(self, s):
        return s + (self.bs - len(s) % self.bs) * AESCipher.str_to_bytes(chr(self.bs - len(s) % self.bs))

    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s)-1:])]

    def encrypt(self, raw):
        raw = self._pad(AESCipher.str_to_bytes(raw))
        iv = Random.new().read(AES.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return base64.b64encode(iv + cipher.encrypt(raw)).decode('utf-8')

    def decrypt(self, enc):
        enc = base64.b64decode(enc)
        iv = enc[:AES.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return self._unpad(cipher.decrypt(enc[AES.block_size:])).decode('utf-8')
```

Figure 3: Code of Hybrid Algorithm

The above set of equations is used over 10 set of each rounds.

The given data of 256 bits is divided into two halves. One is being left half and second being the right half. The XOR function is applied between left half and the right half and the key generated in each iteration. The left half in each iteration is equal to the right half in the previous step. The result of this XOR function is put into the AES algorithm. The output of the AES function represents the right half of the data. The AES function comprises of byte substitution, shift row, mix columns and add round key operations. The keys generated are in compliance with the keys schedule process. This loop is iterated for 10 times. The key schedule is taken from the AES function. It prevents the usage of different sets of AES. This increases the load on the computational density required to encrypt and decrypt the data. As a result, the number of steps formed by this algorithm becomes a varying parameter that is controlled by the user.

The number of layers formed due to the hybrid algorithm can be reduced or increased depending on the level of security required by the organization. It can be increased by increasing the number of layers and can be decreased by reducing the number of layers.

VI. EXPERIMENTAL RESULTS

IoT is evolving at a very rapid pace and is also used in data centers and server rooms where IoT can be used to monitor the humidity, temperature or intensity of the server room or inside the data center. With IoT, we can deploy sensors which can detect a certain rise in temperature, or humidity or intensity and do make decisions like turning off the server or creating alarms etc. The data can be sent every 3-4 seconds and the values of the temperature, humidity or intensity can be stored in the database in the form of tables. Data can be generated by the sensors connected with the Raspberry Pi with DHT11 sensor, who brings out the values of temperature, humidity and intensity and add them to the application connected with MYSQL database. Below are the components connected with Raspberry Pi :

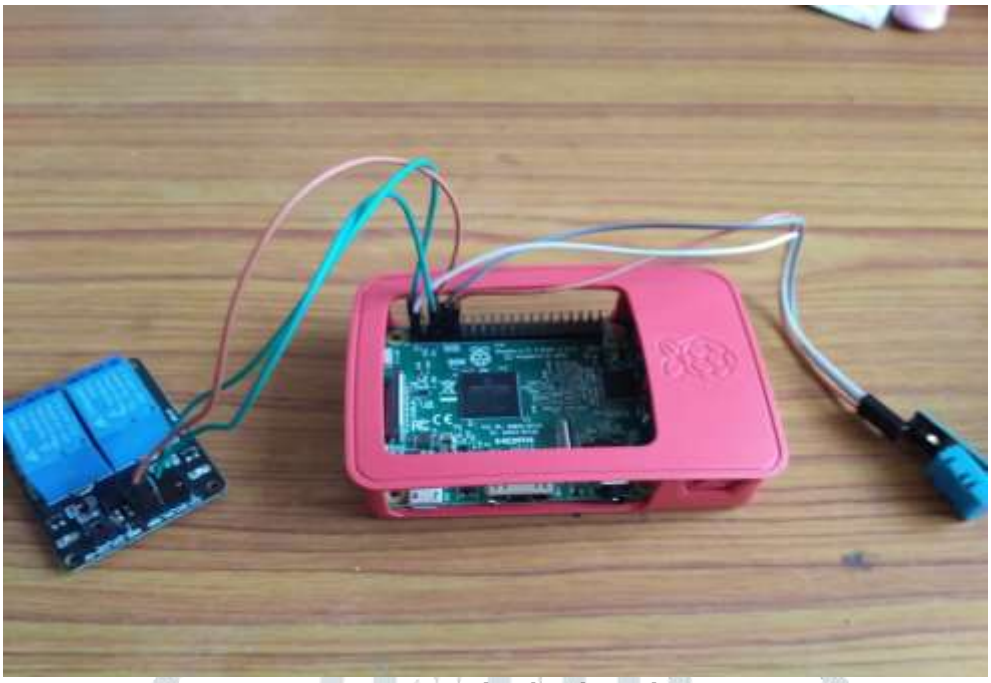


Figure 4: Rpi3 connected with Relay and DHT11 Sensor

Data Communication over internet is never secure and we have deployed an encryption algorithm to secure the channel that takes the data from one end to other. Data is secured over the internet and below is the screenshot taken of raspberry pi running python code to send temp, humidity values:

Figure 5: Output of temperature and humidity values sending via Python code.

We have made a policy where temperature greater than 28 means too bad and server is needed to be shut down in that case, output also displays if the server is off or on as per the temperature value. All the data that is generated by the sensor is going over internet and is encrypted using a lightweight encryption algorithm.

Figure 6: Web page display of data sent in encrypted form and displayed data values.

Data is stored in encryption format and is also decrypted at the other end. Below is the data stored in the MySQL database screenshot:

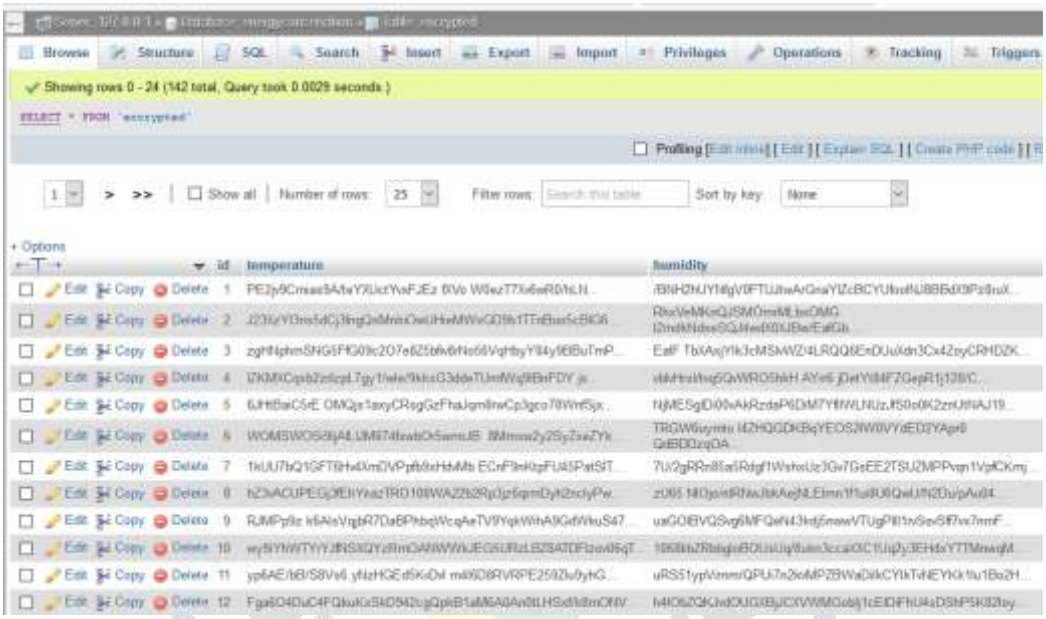


Figure 7: Data Values in encrypted form

As you can see above in the MYSQL database, values are stored inside the database in the encrypted form. By default when we send data over internet from sensor to application. It is not secure and is sent in plain-text form. RPI is an controller and does not work with high end calculations like AES-256, RSA etc. algorithms. Therefore a lightweight algorithm works best in our case, where controller is used, and sensors are embedded with its GPIO pins to generate data using DHT11 sensor for humidity, temperature etc.

VII. CONCLUSION

Data Centers and Server Rooms are the beating heart of the cloud computing. Applications data is stored inside the data center with in the storage units like NAS or SAN connected with the servers. Server Automation is one of the emerging fields with data centers and server rooms using lots of automation in the industry. There are policies which are made and scheduled which works if something specific happens like if the temperature rises above some specific threshold value, then the server is powered off. Data sent over internet is never secure and mainly sent in a plain text form and as controller is not a very fast machine, it needs a lightweight encryption algorithm that works well with the clock cycles that it has. DHT11 sensor, connected with RPi3 sends the data to the application which in turns controls the power services given to the servers. If the threshold level is breached, then the power to the server will be taken off and all this communication should be done in encrypted channel. As in future work we will consider, we will discussed different cryptographic suites such as Advanced Encryption Suite(AES) for confidential data transport, Rivest-Shamir-Adleman (RSA) for digital signatures and key transport and Diffie-Hellman(DH) for key negotiations and management. While the protocols are robust, they require high computation platform and a resource that may not exit in all IoT-attached devices.

REFERENCES

[1] Sagar Sawant,Jay Patel, Kiran Kokate, N.K. Kadale(2017). "IGuard: An Intelligent IOT based Security System for Server Rooms in Industries". International Research Journal of Engineering and Technology (IRJET).

[2] Prathamesh Narkhede, Bhushan Kiratkar, Bhushan Suryawanshi (2015)."Physical Conditions Monitoring in Server Rooms Internet of Things'. International Journal of Electrical and Electronics Research.

[3] Masanobu Katagi and Shiho Moriai, Sony Corporation (2014). Lightweight Cryptography for the Internet of Things.

[4] Køien, M. A. (2015). Cyber Security and the Internet of Things:: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 65-88.

[5] Saranya. C.M., Nitha K.P.(2015). Analysis of Security methods in Internet of Things: International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 4.

[6] S.SicariaA, R.-P. (2015). Security, privacy and trust in Internet of Things: The road ahead.

[7] Madakam, S. (2015). International Journal of Future Computer and Communication, Vol. 4, No. 4, August 2015. Internet of Things: Smart things, 2.

[8] Deeksha Jain, P. V. (2012). A Study on Internet of Things based Applications. CoRR, 6.

[9] Tuhin Borgohain of Assam Engineering College, Uday Kumar of Tech Mahindra, Sugata Sanyal of Tata Consultancy Services, "Survey of Security and Privacy Issues of Internet of Things",(2015), Int. J. Advanced Networking and Applications(IJANA).

[10] J. Satish Kumar, Dhiren R. Patel, SVNIT, Surat, "A Survey on Internet of Things: Security and Privacy Issues",(2014), International Journal of Computer Applications.

[11] Benedikt Abendroth, Aaron Kleiner, Paul Nicholas from Microsoft, "Cybersecurity policy for the Internet of Things", Microsoft(2017)

[12] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed from Red Sea University, Sudan, "Internet of Things Applications, Challenges and Related Future Technologies", World Scientific News(WSN)(2017)

[13] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja.The Internet of Things (Iot): A Scalable Approach to Connecting Everything, The International Journal of Engineering and Science 4(1) (2015)09-12.