IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **Volume 11, Sp.Iss 5 , 2022**

IOT BASED SECURITY AND PRIVACY IMPLEMENTATION IN SMART HOME

J. Rajasekhar[1], T. Thanusha[1], G. Naga Jyothi[1], and K. Tejaswi[1]

[1]Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram, Green fields, Guntur, Andhra Pradesh, India -522302
rajasekharemb@gmail.com

DOI : 10.48047/IJFANS/11/Sp.Iss5/064

Abstract - Internet-of-Thing's technology is being increasingly important in our daily lives. As IoT technology evolved, IoT devices faced a data protection hazard, particularly smart home IoT gateway devices, which became evident. The demand for a low-cost, secure smart home gateway device or router among smart home users. As the Internet of things (IoT) becomes more ubiquitous, there is a growing need to simplify wireless network control mechanisms. Because data collecting and the process includes monitoring, judging, and controlling processes are all involved in IoT, the control mechanism is challenging to simplify. Many internets of things technology offer memory and communication capabilities and are easily vulnerable to hacking due to the mobile software available at the tip of one's fingers to operate the linked gadgets to the web. In the Internet of Things, secure data transfer is always a concern. To increase safety in IoT and wireless networks, the current study introduces a unique RSA-based method and the AES algorithm, and the lightweight protocol message queue telemetry transport (MQTT).

Keywords: IoT, MQTT, SECURITY, AES KDSB ALGORITHM

1 INTRODUCTION

Internet technology is becoming increasingly important in people's lives, benefiting individuals of all ages, from children to the elderly. Different types of apps that mix internet technology will become an increasingly significant component of enhancing people's lives as innovation and the Web advance. The Internet of Things (IoT) is a network of interconnected devices. It allows users to easily access gadgets linked to a network. Furthermore, those IoT systems can be viewed and operated remotely via the web. A smart house is a collection of several home devices that simplify fundamental home functions and employ new protection vectors monitored via the web.

The potential of a harmful network attack or criminal behavior is growing more common as IoT technology improves and advances. As IoT systems are linked via the web known as the Internet, critical data will be transmitted via the Internet. As IoT technology improves, crime hackers may attempt to hack data sent from an IoT gateway, IoT devices, and an IoT network can access the Internet by exploiting flaws in gateway devices, Integrated denial of service, hacking, and other novel attack techniques. There would be a few issues with IoT. IOT consists of a large number of little data blocks that are exchanged between networks from components such as various types of sensors. Although the Internet Protocol has been utilized for most communication, TCP/IP or UDP/IP application protocols currently require Internet access.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **Volume 11, Sp.Iss 5 , 2022**

When the Hypertext Transfer Protocol (HTTP) is used for IoT connectivity, a huge number of small data blocks are sent, resulting in significant performance deterioration.

Furthermore, IP addressing varies depending on physical location, making network control challenging. To solve these issues. MQTT is a simple protocol for sharing IoT network resources. MQTT eliminates protocol overheads and allows for high-speed IoT connectivity.

So, in this paper, we implement the MQTT protocol to communicate between IT devices and the AES KDSB algorithm to transport data to the cloud securely. The objectives of this paper are:

• Use lightweight protocols to transmit the data between IoT nodes.

• To improve the IoT's security.

• Using the AES KDSB method to protect the sensed data

2 LITERATURE SURVEY

[1] This paper illustrates using the Raspberry Pi to secure wireless home automation. We use sensors for security purposes such as door theft protection and gas detection. In addition, the user can control the appliances in the home via the Internet via a mobile application from any location.**[2]** Gas leakage, temperature and humidity, and the on/off of lights and fans in the house are all monitored and managed in the proposed methodology. An alarm notification will be sent to our Gmail account if a gas leak is detected in residence.**[3]** Using PIR, LDR, and DHT11 sensors, this proposed system cost-effectively manages security-related issues. This sensor recognizes the face, captures the process with the Pi camera, and sends an email notification in a couple of moments.**[4]** An automated self-regulating mechanism is recommended that monitors the ambient temperature automatically. The fan speed control system, the heater, and the keypad adjust the fan speed depending on the current room temperature and predetermined preference settings. the heater, and the keypad. For the central control system, a Raspberry Pi is employed.**[5]** The air conditioner will detect and adjust the temperature by sensing the number of people in the room using sensors and cameras. If the number of people in the room increases, the temperature will automatically raise or decrease depending on the number of people in the room. Also, the data will be saved in the cloud.**[6]** In kitchen appliances, the gas sensor will detect the presence of gas and send an alert to our Gmail account; it can also send an alert without Wi-Fi if the data is stored in the cloud.**[7]** The authors have demonstrated a basic application of Raspberry Pi in smart things control via the Internet (Email) in a Raspberry Pi-based interactive home automation system via Email. The proposed

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **Volume 11, Sp.Iss 5 , 2022**

methodology reads the topic of the obtained Email, and the process reacts to the respective guidelines.**[8]** Home automation systems are built to automate operations such as remote control of home appliances. Wireless Sensor and Actuators Networks (WSANs) are becoming increasingly popular in-home automation**.[9]** In this work, we employ the MQTT protocol to secure the information that we exchange between devices. In the MQTT protocol, connected devices are known as "clients," They communicate with a server known as the "broker." The broker handles data communication between clients**.[10]** The user can communicate with the personal assistant through a WhatsApp chatbot or a Google Assistant chatbot, the most natural and convenient way of communication. **[11]** To increase the security of the smart home network, all data communication delivered by the smartphone, server, or host is encrypted with the RSA and AES encryption algorithms. In general, each component of a smart home system communicates via the Internet. However, communication between appliances is done using a cloud-based storage system rather than the Internet to reduce device power consumption.**[12]** The Internet is also used to provide remote control in smart home systems. For many years, the Internet has been widely utilized for browsing, looking for information, downloading, communicating, and installing software.**[13]** In this experiment, we use the Raspberry Pi as a Wireless Sensing node for Home Automation." This paper proposes utilizing the Raspberry Pi to construct a Sensor Web node as part of the Internet of Things (IoT) (RPi). The Raspberry Pi is a small computer that can be customized, fairly priced, and programmed. It has a wide variety of peripherals and can communicate via a network. Controlling, monitoring, and alerting devices was not possible before IoT technologies.**[14]** a computer with speech recognition software A computer may detect a user's word and transform it to text that appears on the monitor.**[15]** The proposed smart communication system configuration for communication between humans inside (Homeowner) and outside (Visitor) the space. The Raspberry Pi design was selected as the system's processing unit because of its user-friendly features and low cost.**[16]** According to previous research, the sensor nodes' performance is significantly reduced when there is a lot of traffic since they consume more energy. The adoption of less dependency and shorter transmission distances for nodes near the sink was a key aspect of the existing technology.**[17]** The Internet's availability of data-driven services has fueled the growth of wireless technologies. The next generation of wireless networks aspires to deliver device connectivity to everyone, everywhere. Data has expanded in recent years due to the emergence of the IoT. By connecting the sensors/things to the Internet, Consumers can obtain real-time updates. **[18]** primary aspects of Raspberry smart house IoT architecture will be encrypting engine, identification, and intrusion detection system. Raspberry encryption engine will request

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Sp.Iss 5 , 2022

Mac and Ip ids of IoT systems to match raspberry IoT device database. It will deny the connection request from that IoT device. The process will finish if the Mac and Ip addresses do not match the authorized Mac and Ip addresses.

3 PROPOSED WORK

The kitchen appliances will be controlled and monitored by the cloud (such as lights and fan, fridge ON and OFF), and all information or data will be stored in the cloud. In the proposed system we are using different MCU to monitor and control the room conditions and all this information is sent to the Raspberry pi and from there the data will be sent to the cloud Fig.1.shows the block diagram of the kitchen room in the kitchen room we are using the gas sensor MQ-6 to find any gas leakages in the room and notify the same to the cloud and automated to open the windows and door of kitchen as well as a notification to the mail The room temperature was measured using a DHT11 sensor. The DHT11 is a widely used temperature and humidity sensor for prototypes that monitor a specified area's ambient temperature and humidity. When the room temperature is raised, the information is automatically transferred to the cloud, and the kitchen exhaust fan is turned on. The exhaust fan will turn off automatically if the room temperature drops to a low level.

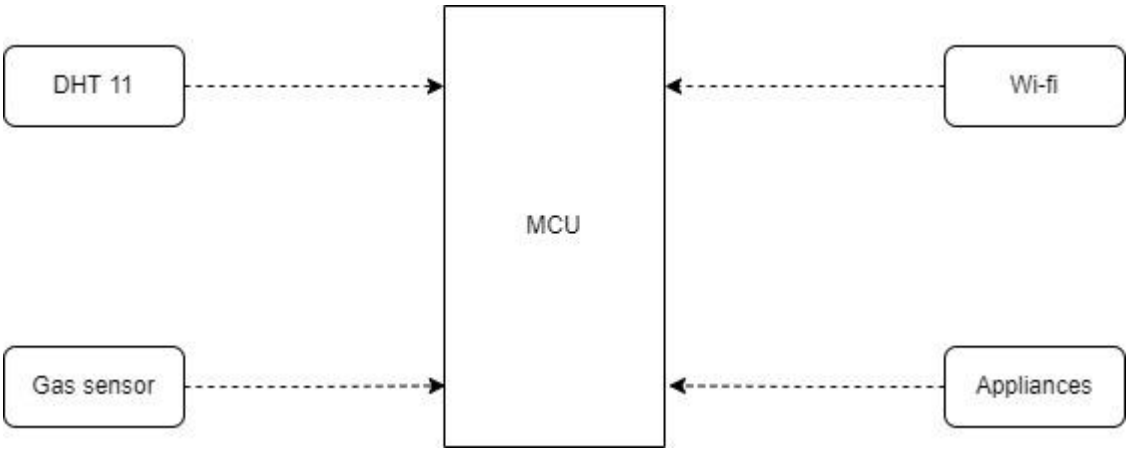

Fig.1 Block diagram of kitchen

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Sp.Iss 5 , 2022

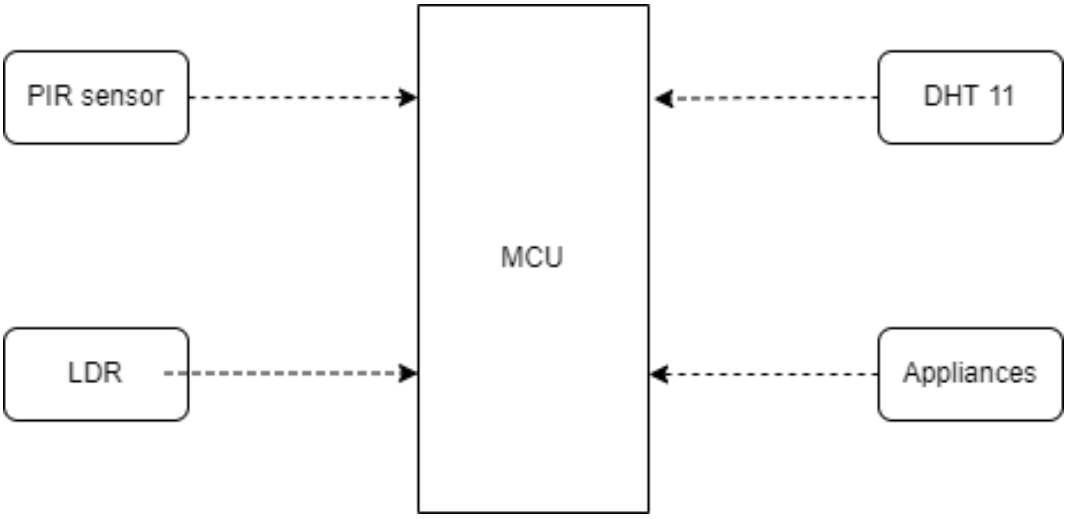

Fig.2 Block diagram of Bed Room

We use PIR, LDR, and DHT11 sensors in the bedrooms and main hall, as shown in Fig.2. The PIR sensors detect infrared energy emitted by objects in their area of vision. Because the human body is the most prevalent thing that a PIR sensor detects, these sensors are used in automatic light switches. As indicated in Fig.2, a PIR sensor will be linked to the server. This sensor is used to control equipment such as fans and air conditioners. If the number of people in the room increase, the AC temperature will rise, or the fan speed will increase. If the number of people increases, the temperature will be reduced according to the room temperature. The temperature will be controlled automatically when the PIR sensor detects the movement of a person. An LDR is a component with a resistance that varies in response to the amount of light. When light falls on the LDR, the resistance reduces, while in the dark, it increases. When an LDR is kept in the dark, it has a high resistance, but when it is maintained in the light, it has a lower resistance. The LDR sensor will control the lights in the room. If the light resistance is low, the lights will turn on automatically; conversely, the lights will turn off automatically if the resistance is large. When a person enters the room, the PIR sensor detects their movement, and the light is turned on with the help of the LDR sensor, and wisely, the lights will be turned off when the person has left the room. The relays are used to control room appliances. All sensors will be linked to the server, and the data will be saved in the cloud. In all other rooms, the same sensors and processes will be used. The Raspberry Pi will be used to connect all of the servers, and the information from the servers will be kept in the cloud.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Sp.Iss 5 , 2022

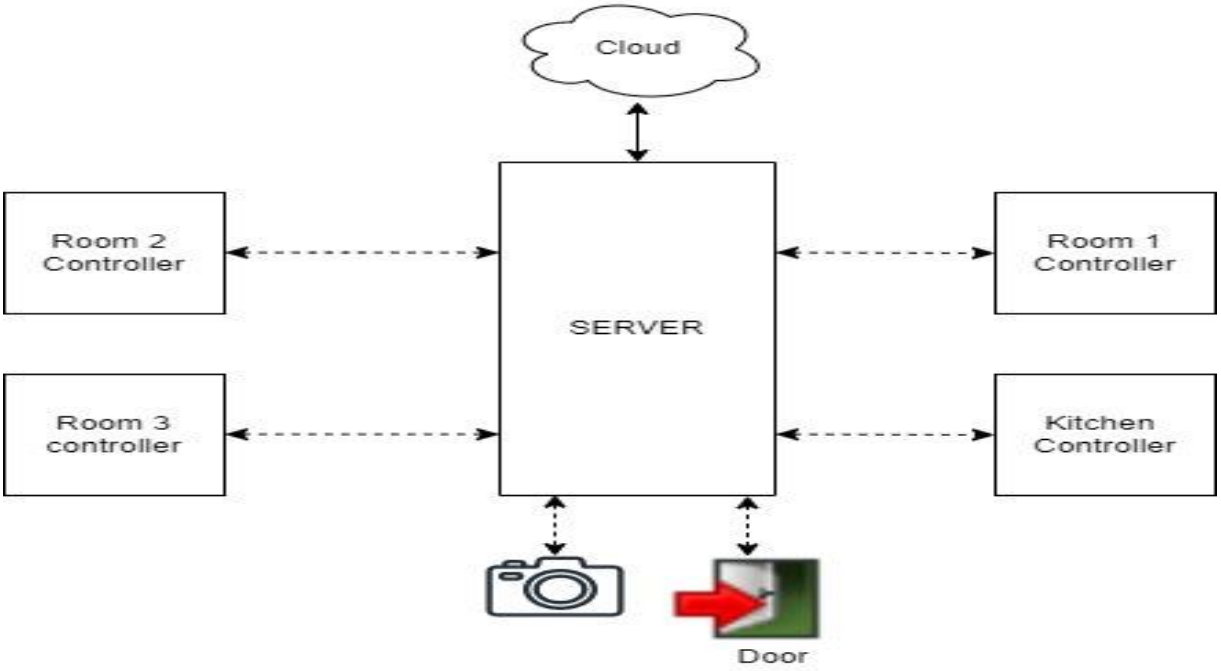

Fig.3 Block Diagram Server

Fig.3 This system will detect the presence of an intruder and quickly send an email notification to the user. In addition, a photo of the intruder captured with the Pi camera will be sent in this Email. A Raspberry Pi is in charge of the entire setup. This system can be installed at the front door of your home, and you can monitor it by Email from anywhere in the World. Here, we use cameras to open the door automatically. They can gain entry to the house by storing the known person database in the Raspberry pi SD card, and the camera will take a picture of that person and send it to the Raspberry pi, and from there, It will take a glance through the database. The door will be opened if a picture is found in the database. If an unknown person attempts to open the door, the camera will take a picture of that person and search in the database. If the image is not identified, an alert warning will be sent to the user's email address. The entire data will be preserved on the cloud. We store data in the cloud using Wi-Fi; however, once the data is saved, the appliances or sensors can work without Wi-Fi. The MCUs in Figures 1&2 are also connected to the server Raspberry Pi. From the sensor, data will be sent to the cloud, and those MCUs will be connected to the cloud, and from there we can monitor and control different rooms conditions, and we can control them from any whare

3.1 MQTT PROTOCOL

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Sp.Iss 5 , 2022

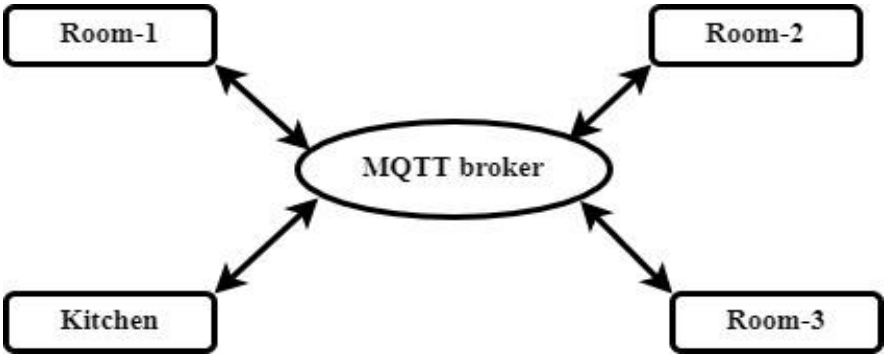

Fig.4 MQTT Broker Job

Fig.4 shows MQTT is a lightweight open messaging protocol that enables connectivity with limited bandwidth to transfer sensor information easily. Machine-to-machine (M2M) communication is enabled through the protocol, which follows a publish/subscribe communication structure.

3.2 AES KDSB BASED ALGORITHM

AES is a block cipher algorithm that has key and block lengths of 128,192and 256 bits. The methods are carried out in at most comparable rounds based on key length. For each round, AES has four sorts of transformations.Shift rows, add round keys, shift bytes, and mix columns are the four main operating modes. The shift rows represent the bytewise permutation, the six columns represent the four mixing operations, and the add round keys represent the XOR procedure of the state with the round keys. The non-linear exchange operation is specified as the sub bytes.

S-box design

It is referred to be the AES algorithm's soul. Because it provides strong security, the general public is unaware of the essentials of the s-box. Furthermore, the substitution process is both efficient and quick. Because of the static structure of the S-box, this basic data encryption was able to defeat the brute force attack. To solve the shortcomings, the suggested work employs a key-dependent s-box method. The key block and the user data block are the foundations of the schema. The data block is the algorithm's input.

4 EXPERIMENTAL RESULTS

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 11, Sp.Iss 5 , 2022

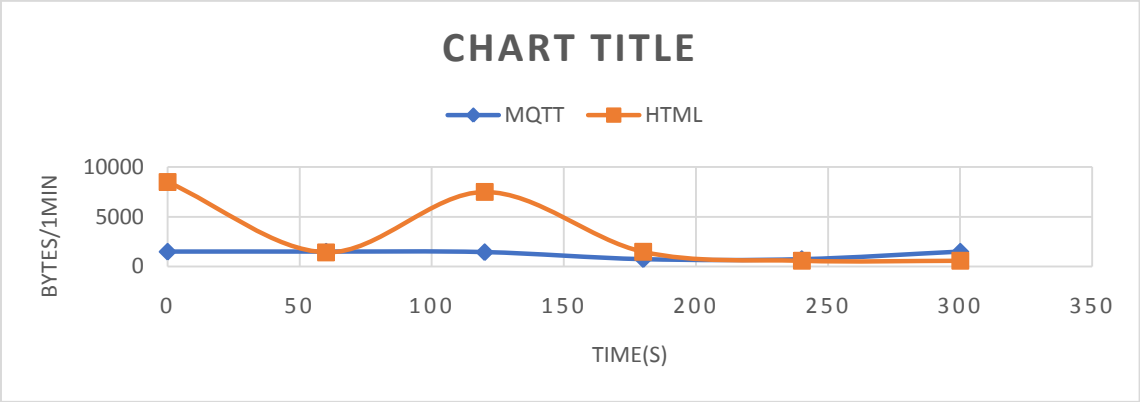

Fig.5 HTTP vs. MQTT protocol

According to the results provided in Fig.5 amount of data transferred per minute using the lightweight protocol, MQTT is around 1500 bytes, compared to HTPP is 7500 bytes (the highest value). The ratio for the number of bytes exchanged per minute is 1:5, implying the MQTT protocol sends one-byte data against five bytes when using HTTP. As a result, the lightweight protocol saves four bytes per minute in data transmission. One byte of data transported per minute equals one unit of electricity consumption. The lightweight protocol consumes one unit of power, whereas HTTP consumes five units. As a result, employing MQTT saves four units of power every minute of data transport. The percentage of money saved by implementing the lightweight protocol.

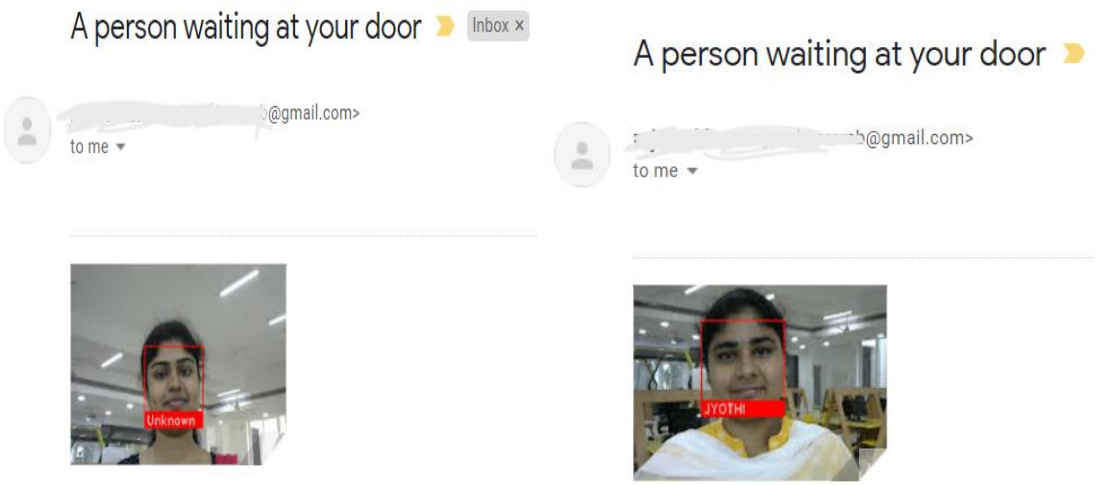

Fig 6. Image sent to the mail

Fig.6 shows the photographs of the persons who are waiting at the door delivered to the mail from the Raspberry Pi and all of the sensor data collected from the node MCUs, which will be sent to the Raspberry Pi and subsequently to the cloud. We use node MCUs as a controller with PIR and LDR sensors to detect human movements and use relays to control the appliances. We

ISSN PRINT 2319 1775 Online 2320 7876
Research paper **© 2012 IJFANS. All Rights Reserved**, Volume 11, Sp.Iss 5 , 2022

use an LPG gas sensor and a DHT11 sensor to measure temperature, humidity, and gas in the kitchen and rooms. And this information is transferred to the cloud. Figure 8 shows the data being transferred to the cloud and the devices being controlled, and we can check the state of the device and the room's condition from anywhere.

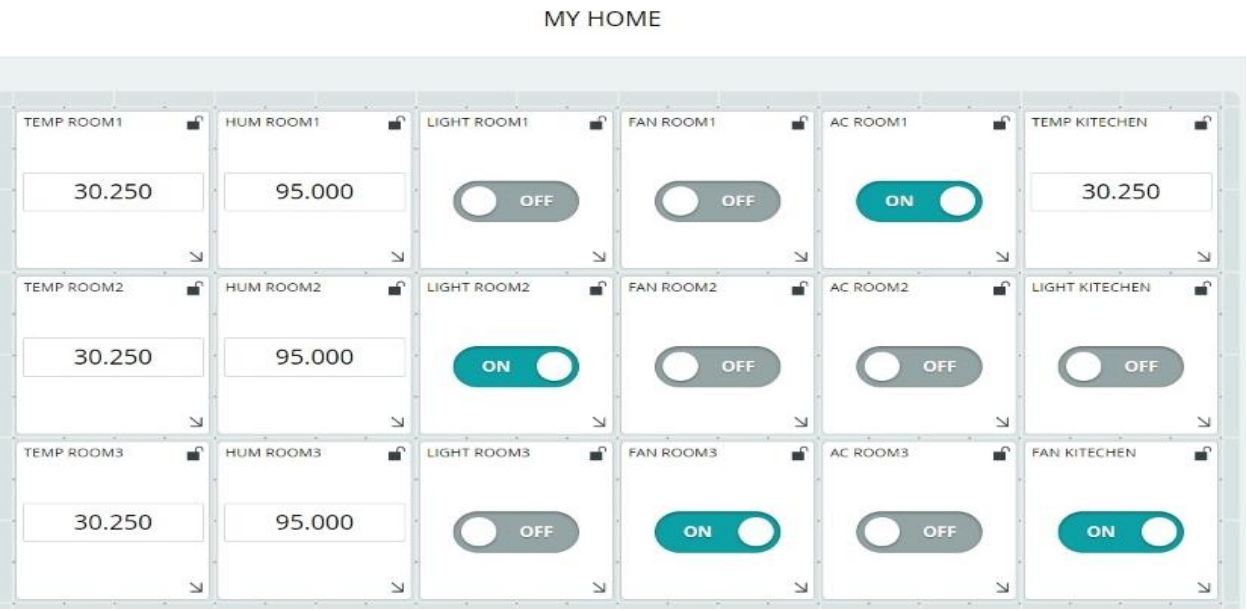

Fig 8. Data sending to the cloud

CONCLUSION

This paper has suggested a system that uses a unique RSA-based algorithm and the AES KBSB method. Data is transmitted between devices using the publish-subscribe communication architecture. MQTT, a lightweight protocol, is used to send data between the devices in an energy-efficient manner. When tested, the proposed system has shown some prodigious results. The persons registered in the cloud to unlock the door and the images have been sent to the user's mail-in many instances. Further, this system can be extended by building a software application, where the system directly takes action when a person intrudes.

REFERENCES

[1] S. M. Brundha, P. Lakshmi and S. Santhanalakshmi, "Home automation in client-server approach with user notification along with efficient security alerting system," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 2017, pp. 596-601, DOI: 10.1109/SmartTechCon.2017.8358441.

[2] J. Prabaharan, A. Swamy, A. Sharma, K. N. Bharath, P. R. Mundra, and K. J. Mohammed, "Wireless home automation and security system using MQTT protocol," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017, pp. 2043-2045, DOI: 10.1109/RTEICT.2017.8256958.

[3] G. M. Debele and X. Qian, "Automatic Room Temperature Control System Using Arduino UNO R3 and DHT11 Sensor," 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2020, pp. 428-432, DOI: 10.1109/ICCWAMTIP51612.2020.9317307.

[4] F. Budiman, M. Rivai, I. G. Bagus Prasta Raditya, D. Krisrenanto, and I. Z. Amirah, "Smart Control of Air Conditioning System Based on Number and Activity Level of Persons," 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2018, pp. 431-436, DOI: 10.1109/ISITIA.2018.8711311.

[5] Arpitha 2019 GasLD, title Gas Leakage Detection and Controlling System,author/K Arpitha and Madhu M Nayak and D. Rithika Rao and Anushree Shenoy,year2019

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **Volume 11, Sp.Iss 5 , 2022**

[6] International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 02 Issue: 03 | Jan-2015 www.irjet.net p-ISSN: 2395-0072

[7] A. Almarwani, L. Alqarni, H. Hakami, Z. Chaczko, and Min Xu, "Door wave home automation system," IET International Conference on Smart and Sustainable City 2013 (ICSSC 2013), 2013, pp. 98-103, DOI: 10.1049/cp.2013.1971.

[8] R. K. Kodali and S. Soratkal, "MQTT based home automation system using ESP8266," 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2016, pp. 1-5, DOI: 10.1109/R10-HTC.2016.7906845.

[9] P. Mathivanan, G. Anbarasan, A. Sakthivel, and G. Selvam, "Home Automation Using Smart Mirror," 2019 IEEE International Conference on System, Computation, Automation, and Networking (ICSCAN), 2019, pp. 1-4, DOI: 10.1109/ICSCAN.2019.8878799.

[10] T. Adiono, S. Harimurti, B. A. Manangkalangi, and W. Adijarto, "Design of smart home mobile application with high security and automatic features," 2018 3rd International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2018, pp. 1-4, DOI: 10.1109/IGBSG.2018.8393574.

[11] H. Bharathi, U. Srivani, M. D. Azharudhin, M. Srikanth and M. Sukumarline, "Home automation by using raspberry Pi and android application," 2017 International conference of Electronics, Communication, and Aerospace Technology (ICECA), 2017, pp. 687-689, DOI: 10.1109/ICECA.2017.8212754.