Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/44/20230067

IoT based security and privacy implementation in smart home

J. Rajasekhar[1], T. Thanusha[1], G. Naga Jyothi[1] and K. Tejaswi[1] and Laith Abualigah[2,3,4,5]

[1]Department of Electronics and Computer Engineering, Koneru Lakhmaiah Education Foundation, Vaddeswaram, AP, 522502, India;
[2]Computer Science Department, Prince Hussein Bin Abdullah Faculty for Information Technology, Al al-Bayt University, Mafraq 25113, Jordan.
[3]MEU Research Unit, Middle East University, Amman, Jordan.
[4]Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman 19328, Jordan.

[5]aligah.2020@gmail.com

Abstract. Internet-of-Thing's technology is being increasingly important in our daily lives. As IoT technology evolved, IoT devices face 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. The problem is that 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 processes such as monitoring, judging, and controlling 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, as well as 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 indeed a network of interconnected devices. Furthermore, those IoT systems can be viewed and operated remotely via the web. It allows users to easily access gadgets linked to a network. A smart house is a collection of several home devices that simplify fundamental home functions and employ new protection vectors that can be monitored via the web.

The potential of a harmful network attack or criminal behaviour 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

DOI: 10.54254/2755-2721/44/20230067

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 techniques of attack. IOT consists of a large number of little data blocks that are exchanged between networks from components such as various types of sensors. There would be a few issues with IoT. Although the Internet Protocol has been utilized for the majority of communication, TCP/IP or UDP/IP application protocols currently require Internet access. 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.

2. Literature survey

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 [1]. 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 the 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 Using 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 (E-mail) in a Raspberry Pi-based interactive home automation system via Email, in which the topic of the obtained e-mail is read by the proposed methodology 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

3. Proposed work

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. 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.

DOI: 10.54254/2755-2721/44/20230067

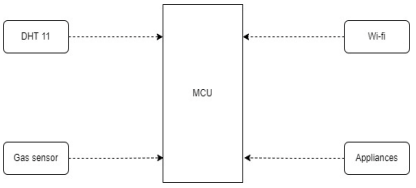

Figure 1. Block diagram of kitchen.

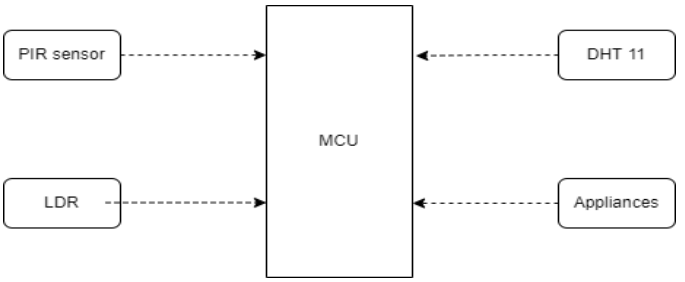

Figure 2. Block diagram of Bed Room.

In the bedrooms and main hall, we use PIR, LDR, and DHT11 sensors 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 is reduced, the temperature will be reduced in accordance with 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 it receives. 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 lights in the room will be controlled by the LDR sensor. If the light resistance is low, the lights will turn on automatically, conversely, if the resistance is large, the lights will turn off automatically. 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 of the 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.

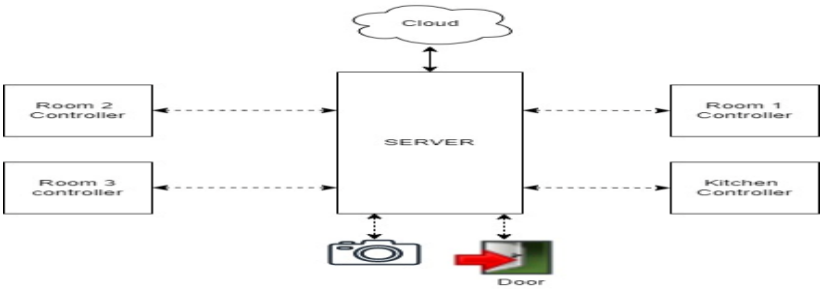

Figure 3. Block Diagram Server.

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 automatically open the door. They can gain entry to the house by storing the known person database in the Raspberry pi SD card, 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 would 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 it is not identified the image 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 in the cloud, the appliances or sensors can work without Wi-Fi. The MCUs in Figure 1&2 are also connected to the server Raspberry Pi. From the sensor data will be sent to the cloud and

DOI: 10.54254/2755-2721/44/20230067

those MCU's 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

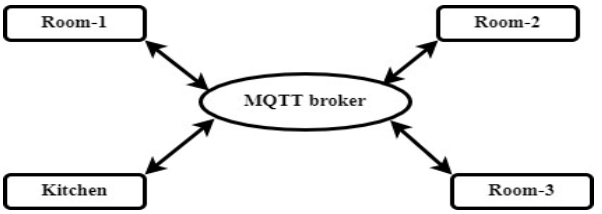

Figure 4. MQTT Broker Job.

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 cypher algorithm that has key and block lengths of 128,192and 256 bits. Based on key length, the methods are carried out in at most comparable rounds. 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 non-linear exchange operation is specified as the sub bytes. The bytewise permutation is represented by the shift rows; the four mixing operations are represented by the six columns, and the XOR procedure of the state with the round keys is represented by the add round keys.

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

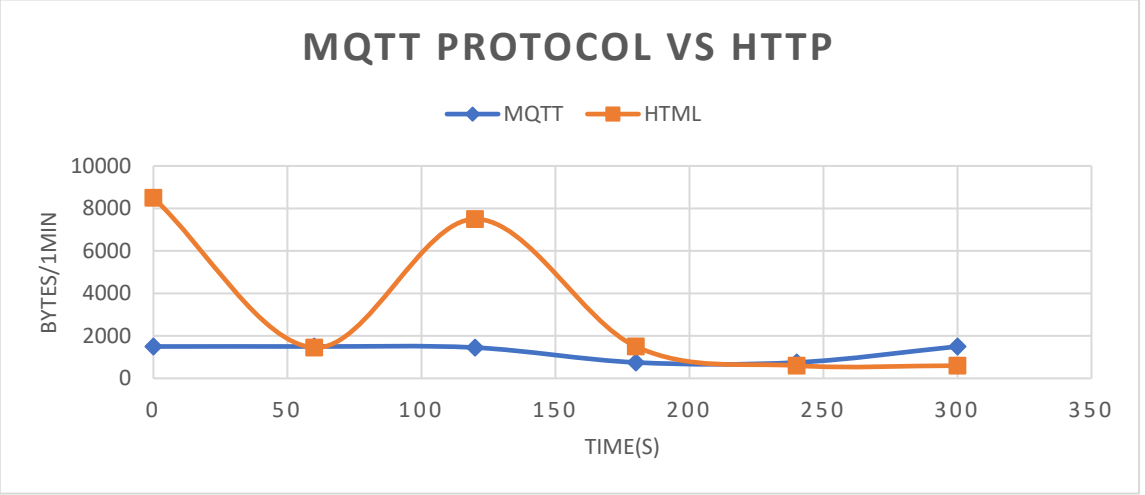

Figure 5. HTTP vs MQTT protocol.

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

DOI: 10.54254/2755-2721/44/20230067

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 is believed to equal 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.

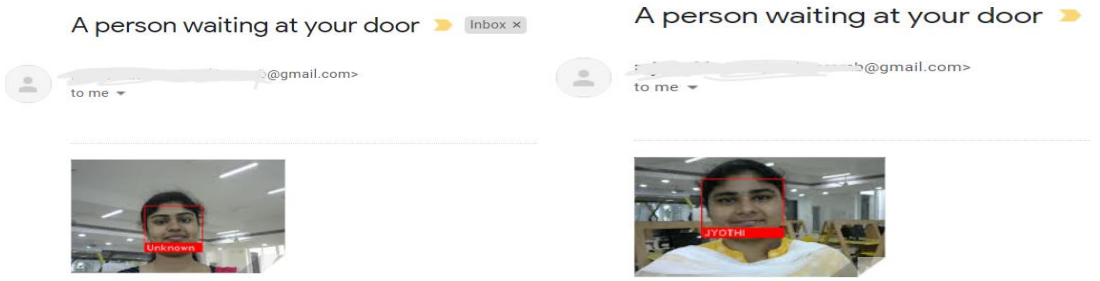

Figure 6. Image sent to the mail.

Fig.6 shows the photographs of the persons who are waiting at the door delivered to the mail from the Raspberry Pi, as well as 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 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 7 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.

Figure 7. Data sending to the cloud.

5. Conclusion

This paper has suggested a system that uses a unique RSA-based algorithm as well as the AES KBSB method. MQTT, a lightweight protocol, is used to send data between the devices in an energy-efficient manner. Data is transmitted between devices using the publish-subscribe communication architecture. The proposed system when tested has shown some prodigious results, the persons have been detected who are 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 an action when a person intrudes.

References

[1] Sathishkumar V E, Changsun Shin, Youngyun Cho, "Efficient energy consumption prediction model for a data analytic-enabled industry building in a smart city", Building Research & Information, Vol. 49. no. 1, pp. 127-143, 2021.

[2] Sathishkumar V E, Youngyun Cho, "A rule-based model for Seoul Bike sharing demand prediction using Weather data", European Journal of Remote Sensing, Vol. 52, no. 1, pp. 166-183, 2020.

DOI: 10.54254/2755-2721/44/20230067

[3] Sathishkumar V E, Jangwoo Park, Youngyun Cho, “Seoul Bike Trip duration prediction using data mining techniques”, IET Intelligent Transport Systems, Vol. 14, no. 11, pp. 1465-1474, 2020.

[4] Sathishkumar V E, Jangwoo Park, Youngyun Cho, “Using data mining techniques for bike sharing demand prediction in Metropolitan city”, Computer Communications, Vol. 153, pp. 353-366, 2020.

[5] Sathishkumar V E, Yongyun Cho, “Season wise bike sharing demand analysis using random forest algorithm”, Computational Intelligence, pp. 1-26, 2020.

[6] Sathishkumar V E, Myeongbae Lee, Jonghyun Lim, Yubin Kim, Changsun Shin, Jangwoo Park, Yongyun Cho, “An Energy Consumption Prediction Model for Smart Factory using Data Mining Algorithms” KIPS Transactions on Software and Data Engineering, Vol. 9, no. 5, pp. 153-160, 2020.

[7] Sathishkumar V E, Jonghyun Lim, Myeongbae Lee, Yongyun Cho, Jangwoo Park, Changsun Shin, and Yongyun Cho, “Industry Energy Consumption Prediction Using Data Mining Techniques”, International Journal of Energy Information and Communications, Vol. 11, no. 1, pp. 7-14, 2020.

[8] Ronggang Zhang, Sathishkumar V E, R. Dinesh Jackson Samuel, “Fuzzy Efficient Energy Smart Home Management System for Renewable Energy Resources”, Sustainability, Vol. 12, no. 8, pp. 1-15, 2020.