SECURED REALTIMESMART ROOMAUTOMATION USING AES ALGORITHM

Gouthame P , Dr.M.Manikandan

Abstract— **In the digital era, IoT plays a major role in taking up the standard of the digital world to the next level. The advancement in IoT provides better comfort to the human community a campus could be turned into a smart e-campus. The privacy and security have been becoming the most demanding tasks in the Internet of Things (IoT) network. This addsdeployment of an IoT framework on authentication enhances the IoT system and turns it to be an authorized or secured smart system.**

In this paper, an attempt is made to propose and implement a secured real-time smart automation of classroom using IoT in MIT campus, Anna University. TheIoT security issues with cloud access are addressed through a suitable standard and efficient algorithm like AES. The effectiveness of the proposed work is explicit from the outcome obtained, discussed in the results section of this paper. The major highlight of this work is that the IoT framework is designed in an indigenous manner suiting the existing scenario of the college campus.

Keywords— **Arduino UNO, ESP 8266 (wifi-module), AES algorithm,**

I. INTRODUCTION

The internet of things (IoT),is a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[1-3].

Despite these interesting features,IoT demands an appreciable security strength in its infrastructure. Henceforth .security should be treated as an add onfeature to improvise the overall performance of the IoT ecosystem [4].Satisfying the security requirements is a huge challenge due to the limitations associated with IoT devices concerning their capacity and capability to implement traditional security solutions.

Privacy in IoT is also challenging as it reflects acting on its behalf, to determine the degree to which it will interact with the environment. Communication Protocol for security can provide some solutions for privacyDevices should communicate only if it is necessary, to reduce privacy exposing themselves during communication[5]. Also, devices must be able to disconnect from the network if it is inactive to minimize the tracking of location information. The authorized device only allowed communicating and if it is turned on, it must re-authenticate itself to the network before start dealing with any information.[4,5]

Data confidentiality another requirement demands that when data is transmitted through the network should employ achieved using encryption techniques. Encryption in some cases, adds data to packets to provide tracing property as well.

In[4],the data collection modules of IoT systemsare implemented in a home automation environment, which runs on the home automation gateway and within the home automation cloud, and permits the connectivity to the already existing big data middleware platform. A Bluetooth module is also attached to the microcontroller chip which gives a message when the consumer is not in the proximity of his distanced gadget. The system gives statistics to the users or farmers about many conditions like the popularity of multiplied temperature, water content material in soil, and smoke via SMS on GSM network or via Bluetooth with good accuracy.

.The author of [4] been analyzed and implemented the home automation technology using Global System for Mobile Communication (GSM) modem to control home appliances such as light, air-conditioner system, and security system via Short Message Service (SMS). The reported research work is focused on the functionality of the GSM protocol. The field situation is dispatched to the farmer through mobile text messages. With this machine, sensor node failure and electricity saving are managed effectively.

In proposed, protection of GSM/Bluetooth based human-controlled irrigation machine. This device has set the irrigation time depending on the temperature and humidity reading getting from sensors and specific kinds of crops and might automatically irrigate the sector whilst required. Information is exchanged between the designed system through SMS on the GSM community.

. In Kun-lin Tsai, Yi Zhang et al, paper [2], Internet of Things Environment is tested using the Advanced Encryption Standard (AES) and compared it with the data encryption standard DES. The analysis shows that AES has better security and is, therefore, suitable for encrypting data in the IoT environment. This could be used for extensive data storage and analysis for the existing home automation solution.The highlight of this study is to practically realize IOT based smart applications in a college campus and sort out implementation constraints in the college environment without any security threats, to the best of our knowledge, this type of work has not been reported in the Indian scenario so far. Added to it, the IoT security issues with cloud access through a suitable standard algorithm like AES has not been carried out yet for such a unique setup.

Considering the above-stated limitations of the existing work, the objectiveof this paper is to propose a Secured Real-time Implementation of an IoT enabled smart classroom/ Laboratory. This core objective is accomplished through a collection of the listed out sub-objectives:

- To enable real-time smart switching of fan and lights(Electrical load)
- To transfer sensed data to the cloud through secured communication using AES
- To integrate both smart automation and secured data communication
- To perform analysis of secured data stored in the cloud and derive useful inference out of it

Section 2 deals with the block diagram and the working of the proposed system. Results and discussion are discussed in Section 3.Conclusion presented inSection 4

II. BLOCK DIAGRAM OF PROPOSED SYSTEM

The detailed overall block diagram of the proposed system is provided in Fig.1.The above-stated objectives are collectively met out in this proposed framework designed in an indigenous manner.

The presence of the people inside the classroom is first ensured smartly with a sensor to automatically switchon and off the electrical load in that proximity area. In this case, the electrical load is tested with fan and light which could be extended to any other gadget like an air-conditioning machine, multimedia projector, etc. For this study, the PIR sensor is selected and employed to capture the occupancy of the classroom for enabling smart switching of the electrical loads. This sensed data is passed onto the Arduino UNO board for further processing using the AES algorithm. Then using a wifi module (ESP8266), the data is securely transferred to the cloud for data collection and post-analysis of the same.

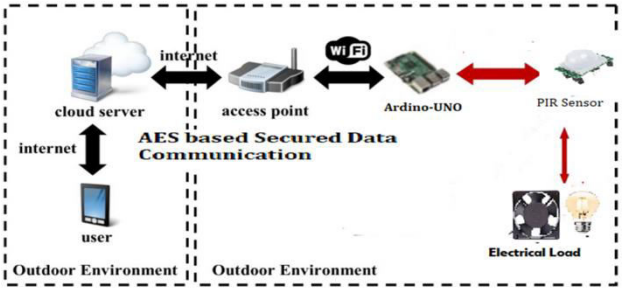

Fig1 Overall Block diagram of the proposed system

As shown in fig.2, A Smart Lighting and security solution uses buzzer, ArduinoUno microprocessor, PIR sensors, relay, and Arduino IDE (to write code for ArduinoUno microprocessor) are considered. As shown in the figure, whenthe PIR sensor detects any human motion, then using AT commands, Arduino UNOinstructs the relay that PIR detected some motion and inaction, the relay will turn on the electrical loads. If the room size is so big and if all lights have connected with the same PIR sensor then when someone enters the room all light will turn on. But an ideal situation is that when fewer people enter the room not all lights should turn on,

only lights near to that person must be turned on.Henceforth, in this study, more number of PIR sensors are placed equidistant in the test area based on the measurements.

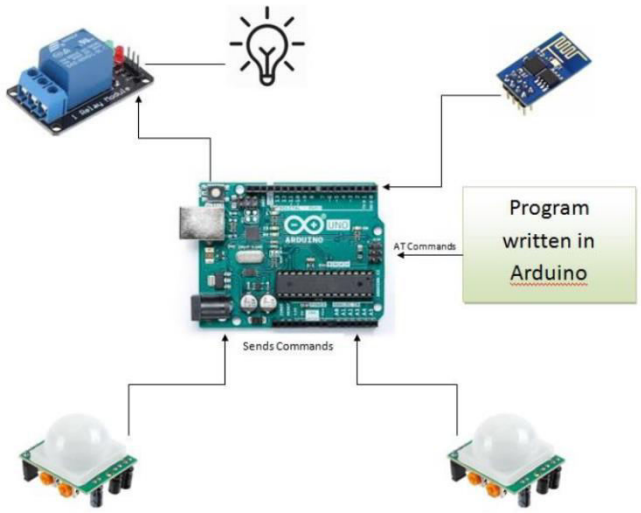

Fig 2Working Model

III. RESULT AND DISCUSSION

This study aims at the design of a workable framework for real-time implementation of smart classroom automation using IoT architecture.The various stages in the development of this studyare presented in detail with a sufficient number of snapshots/ photos taken during the design and working of it.

The proposed IoT framework is planned to be implemented in the laboratory – IoT lab of the Dept. Of Electronics Engineering, MIT campus at Anna University,Chennai. In this connection, the room measurements are taken to estimate the position and number of the PIR sensors required to automate the entire space of the laboratory. From the trial test, it was observed that 3 such PIR sensors driven by the microcontroller board would suffice the automation of the entire room. The measurements and positions of sensor deployment are indicated in the form of the layout diagram indicated in fig.3, the red dots indicate the sensor deployment positions. Fig 4 shows the snapshot of the room with the sensor mounted on the wall.

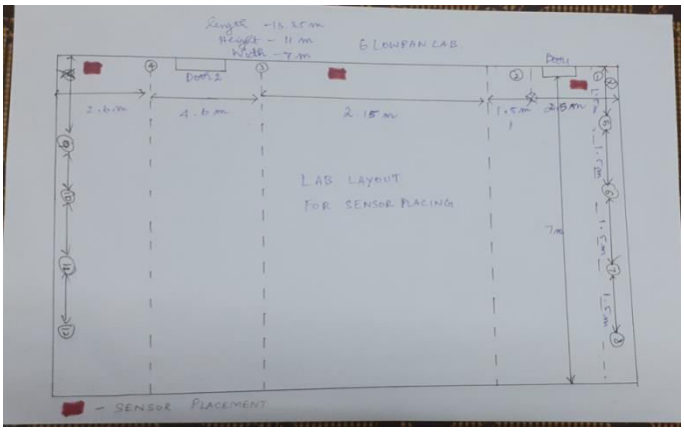

Fig 3 Layout of the lab where the hardware is planned for implementation.

Fig 4 Snapshot of the sensor mounted on the wall of the test lab.

Security is a primary concern for any kind of IoT application/deployment. AES has proven to be the best-preferred security algorithm in recent kinds of literature. AES -128 algorithms are used to provide authentication and integrity of packets to the network server and end-to-end encryption to the application server in the IoT environment.

A unique 128-bit Network Session Key shared between the end-device and network server. The AES code has been dumped into the Arduino-UNO and tested successfully for both encryption and decryption process. It is illustrated in the snapshots shown in Fig 5 and 6 respectively. Both encryption and decryption of AES 128 bit code are executed and the final test output is obtained in the serial monitor of Arduino software.

Fig. 5 is the snapshot of the implemented AES algorithm code in Arduino Uno for the encryption phase.Fig. 6 gives a sample snapshot of the

successful decryption phase output of theAES code in Arduino.

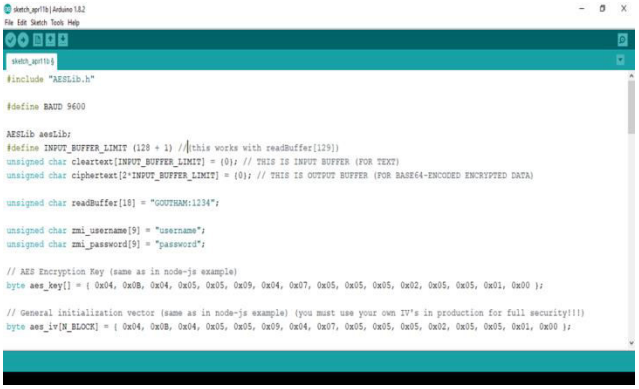

Fig 5 AES code dumped in Arduino Uno

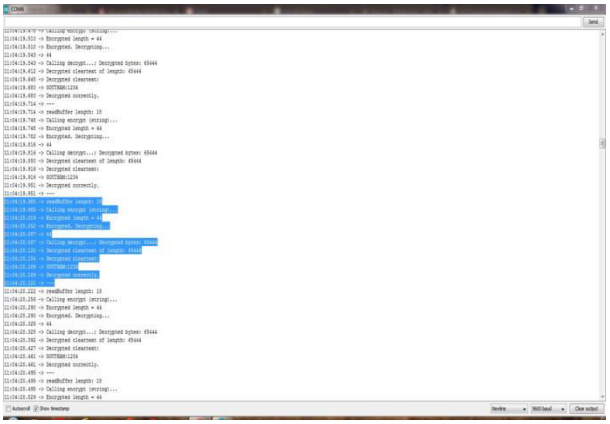

Fig 6AES final test output in the Arduino module

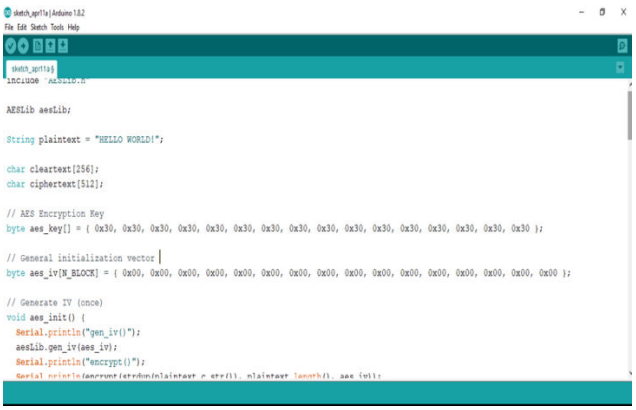

Fig. 7 AES coding in ESP8266

Figs. 7 and 8 depict the AES implementation into the wifi module, as it is this module, which transfers the sensed data to the cloud. Hence this wireless device needs to be protected from unauthorized commands from hackers. Fig.7 shows the AES code running in the ESP8266. Fig 8 portrays the successful AES tested decrypted output in the wifi module.

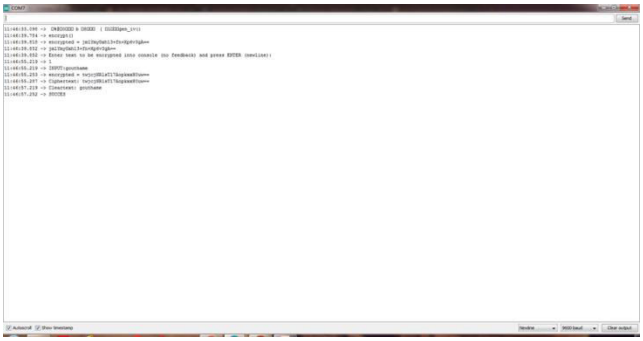

Fig. 8AES final test output in ESP8266 (wi-fi module)

IVCONCLUSION

The main motive behind this project is to practically realize IOT based smart applications and sort out implementation constraints in the college environment without any security threats, which has not been reported in the Indian scenario so far. Added to it, the IoT security issues with cloud access through a suitable standard algorithm like AES has not been carried out. The time to respond for automation has also been determined

This target is accomplished initially with the design of a prototype model. Later the actual real-time implementation of automated electrical load switching on and off with IoT is achieved. Along with this to enhance the security of the IoT environment, the AES algorithm for a secured data transfer with the real-time implementation of IoT with electrical loads has been achieved. AES algorithm is dumped into the Arduino board and interfaced with cloud (thing speak) for data storage and analysis. Automation testing was done for a smart laboratory on the college campus. The outcome of this experimental study has been very effective in terms of simplicity,security, and cost-effectiveness.

TABLE

The following tabulation is obtained from the time taken for various modules to respond. Modules include PIR sensor time and AES overall run time

Table 5.1 Response time

S.NO	MODULE	TIME TAKEN (seconds)
1	SENSOR RESPONSE TIME	1.5 milliseconds
2	ENCRYPT TIME	5
3	DECRYPT TIME	3
4	OVERALL AES RUNTIME	10

REFERENCES

[1] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoTmiddleware: A survey on issues and enabling technologies," IEEE Internet Things J., vol. 4, no. 1, pp. 1–20, Feb. 2017.

[2] A.Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," Future Gener.Comput. Syst., vol. 56, pp. 684–700, Mar. 2016.

[3] Mr. Pranay P. Gaikwad, Mrs. Jyotsna P. Gabhane, Mrs. Snehal S.Golait "A Survey based on Smart Homes System Using InternetofThings", 2015 International Conference OnComputation Of Power, Energy, Information AndCommunication, Pp.330-335.

[4] R. Piyare, "Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone," International Journal of Internet of Things, vol. 2 no. 1, pp. 5-11, 2013

[5] S. Kulkarni, S. Durg, and N. Iyer, "Internet of Things (IoT) security," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 821-824.

[6] F. J. D'sSouza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," 2017 International Conference on Computing, Communication, and Automation (ICCCA), Greater Noida, 2017, pp. 647-652.

[7] NikeshGondchawar, Prof. Dr. R. S. Kawitkar, "IoT based Smart Agriculture" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, ISSN (Online) 2278-1021 ISSN (Print) 2319 5940, June 2016.

[8] P. M. Varela, J. Hong, T. Ohtsuki, and X. Qin, "IGMM-based co-localization of mobile users with ambient radio signals," IEEE Internet Things J., vol. 4, no. 2, pp. 308–319, Apr. 2017.

[9] PrasoonRaghav, Rahul Kumar and Rajat Parashar, "Securing Data in Cloud Using AES Algorithm",International Journal of Engineering Science and Computing, 2016, ISSN 2321 3361,pp: 3672-3675.

[10] FisnikDalipi and SuleYildirimYayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges", 4th International Conference on Future Internet of Things and Cloud Workshops2016, pp: 63-68.

[11] Augustine Ikpehai, etal "Low-Power Wide Area Network Technologies For Internet-Of-Things: A Comparative Review" Ieee Internet Of Things Journal, Vol. 6, No.2, Pp 2225-2239,2019.

[12] Dina M. Ibrahim "Internet of Things Technology based on LoRaWAN Revolution" 10th International Conference on Information and Communication Systems (ICICS),pp 234-237, 2019.

[13] Takayuki Suyama, Yasue Kishino and FutoshiNaya "Abstracting IoT devices using a virtual machine for wireless sensor nodes", Internet of Things (WF-IoT), 2014 IEEE World Forum, Seoul,2014, pp. 367-368

[14] Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", IEEE SENSORS JOURNAL,OCTOBER 2013, VOL. 13, NO. 10, pp. 3846-3853.

[15] Andreas Jacobsson, Paul Davidsson "Towards a Model of Privacy and Security for Smart Homes", IEEE Conference,2015

[16] YAN Wenbo, WANG Quanyu, GAO Zhenwei "Smart Home Implementation Based on Internet and WiFi Technology", Proceedings of the 34th Chinese Control ConferenceHangzhou, China, July 28-30, 2015, pp. 9072-9077.