European Journal of Technique

journal homepage: https://dergipark.org.tr/en/pub/ejt

Vol.11, No.1, 2021

Design and Application of a Smart Home System Based on Internet of Things

Resul Daş[1*], **Taha Ababaker**[2]

[1*]Firat University, Software Engineering Department, 23119, Elazig, Turkey. (resuldas@gmail.com).
[2] Zakho University, Computer Science Department, Duhok, Iraq. (taha88eng@gmail.com).

ARTICLE INFO

Received: May., 01. 2021
Revised: July., 03. 2021
Accepted: July, 11. 2021

Keywords:
Smart home
IoT
AES
NodeMCU ESP8266
Arduino Uno

Corresponding author: *Name Surname*

ISSN: *2536-5010* | e-ISSN: *2536-5134*

DOI: https://doi.org/10.36222/ejt.931161

ABSTRACT

The Internet of Things plays a critical role in smart home systems techniques. A smart home system provides a major change in the life of humans that gives home appliances intelligent operation. This encouraged us to create a solution for controlling certain home appliances, such as door and lights. This system is used to monitor the status of the door, window, temperature, humidity, and measuring distance by using various sensors such as IR, DHT22, and ultrasonic sensors. NodeMCU ESP8266, Relay module, and Arduino Uno have been used as the main parts in this paper. The system presented in this paper able to monitor and control home appliances from any corner of the world at any time and efficiently utilize the power by properly controlling the appliances. Ubidots IoT platform and Blynk application were used to check and read data from sensor modules placed in the home and, also to control home appliances by turning ON/OFF relay switches such as door and lights. The paper also focused on protecting user's data by using the AES method to ensure that a system encrypts and encodes Wi-Fi information before sending it to a destination, eventually, to restore the original data, it decrypts and decodes the data.

1. INTRODUCTION

The Internet of Things (IoT) has recently turned into a human lifestyle of great potential. Due to the development of modern wireless communication technology, the IoT concept is a revolutionary concept that has gained popularity. In different areas, comprehensive IoT-related research and applications are currently underway. The fundamental formation of this concept is to create applications that allow human life to interact with each other through the objects in the world [1]. One of the more prevalent IoT technologies is a smart home. Both digital and mechanical devices are interconnected in a smart home to create a network that interacts and creates collaborative space between the user and others [2]. This involves everything from smartphones, lamps, washing machines, coffee makers, sensors, actuators, and computers to the internet, where devices are intelligently connected to allow new ways of communication between people and almost everything else between them. These can be controlled and accessed at any time remotely from any computer, smartphone, or tablet [3]. With the increasing amount of devices connected to the IoT, security and privacy problems are being noticed and more pronounced [4]. Since IoT devices are expected to make their data available to stakeholders, doing so in a managed manner has become the key problem [5]. The data transmitted can include sensitive information relating to behaviors, privacy, activities, and relationships of users, all of which relate to the privacy of individuals [6]. Therefore, IoT systems must ensure data integrity and confidentiality and also user's anonymity and privacy [7]. This paper explores how a framework for the monitoring and controlling of home appliances using Arduino Uno, NodeMCU, and relay module as the main hardware parts. Also, the Ubidots IoT platform and Blynk application have been introduced in this paper to allow the use of IoT. The various sensor modules data in the home environment are sent through the Arduino Uno and Arduino exchange the data with NodeMCU. The NodeMCU is coded via Arduino Integrated Development Environment (IDE) with the USB to tell the NodeMCU what to do. NodeMCU controls three channels of relay kit and receives instructions to show the temperature, humidity, door status, window status, and distance measurements from Blynk mobile application and Ubidots IoT platform web application and processes them to monitor the sensors and control actuator circuit of home appliances. Also, implementing an Advanced Encryption Standard (AES) is needed to increase confidentiality in data security. All the information in the system will be encrypted and decrypted by the AES method. The remainder of this article is structured as follows, the related work in this area is mentioned briefly in section two. The system design is described in section three. Section four presents the implementation of the performed method. Section five discusses and shows the application

results. This paper is concluded in section six and describes future work.

2. RELATED WORK

To thoroughly understand the definition of smart home and IoT technologies, we have gone through many articles, studies, conference papers, and project reports. The following are some of the suggested and current smart home systems.

The design and implementation of a smart home for the elderly and disabled were proposed by Das et al. [8], the presented system was a sample of smart home technology applications consisting of a variety of networked sensors. While it was just a very clear example of smart homes, it illustrates that smart homes can impact the elderly and disabled in all aspects of everyday life. Mandula et al. [9], suggested a home automation based on IoT using an android mobile application. Two kinds of home automation Bluetooth-based and Ethernet-based were used in their article. The custom mobile android application was used to control home appliances such as air-conditioning, TV, fan, etc. however, the prototype data sources were not transparent, leading to an impasse when several android phones attempt to access the same website. Tuna [10], proposed a secure smart home systems web-based communication frame for elderly and disabled people. To ensure safe internet communication first, the RSA algorithm was used to encrypt the data and then transmit and sent the encrypted data to the receiver. For security purposes, signs of contact should be removed after the receiver reads the encrypted content. The proposed system was able to allow confidential messaging between smart home residents and individuals they want to communicate with. The platform can also be conveniently built into clever home control panels or web-based smart home systems. Reddy et al. [11], have presented a home automation based on IoT using an android application. The authors used android mobile via the Wi-Fi module to send commands to the Arduino and Arduino processes all the home devices to be monitored and controlled. The voltage levels of electrical appliances were regulated in their framework such as lamps, fans, etc. On their android cell phone, they get the status of their home appliances. A smart automated home framework using IoT with the Blynk application was developed by Durani et al. [12], their study included the functionality of NodeMCU ESP8266 that is connected with the house appliances such as lights, water pump, fan, etc. with the help of online coding and hosting using a web server. The entire functionality was handled by a mobile application created in the android application from which house applications were managed with the support of the internet. The focus of their study was also on wireless control of circuit devices by NodeMCU and the Blynk application.

A smart incubator with IoT has been proposed by Sivamani et al. [13], their paper explores the cost-effective existence of an embedded incubator baby monitoring system in real-time. All the information and data were stored in the Ubidots user's account and then a message of parameters value send as a notification to the signed user when Arduino has Wi-Fi access. Every second the values can be verified. It gives precise values, which are synchronized every second. A smart home automation system based on IoT with a sensor node was proposed by Singh et al. [14], in their paper, a smart home integrated various electrical appliances in the house and automated them without human intervention. Their system was able to monitor the various environmental variables and directs devices to function according to the user's requirements. By using IoT technology they achieved the development of smart homes. Imam [15], have proposed a simple smart home based on IoT using NodeMCU and Blynk. Based on the results of the review of all data obtained by testing a smart home with an IoT-based NodeMCU, it showed that it can be built with different hardware and software support components so that it can be incorporated into a smart home system that is functioned by the Blynk android application according to what is intended to control some of the performance of home electronics, such as lights, fan, early warning system, etc. A healthcare monitoring system based on IoT by using NodeMCU and Arduino was introduced by Wai et al. [16], the proposed patient monitoring system was designed to minimize the time. Results demonstrated that the doctor can test his/her patient anytime and anywhere. The nurses or doctors could conveniently use the computer to search and store them in the database. Also, the doctors were able to use mobile phones and with the help of NodeMCU can be incorporated into a global network. Data security and challenges in smart cities have been presented by Farahat et al. [17], the suggested system prevents attackers from attacking citizen data by encoding and then encrypting them through the AES technique when they are transmitted wirelessly from any source to any destination. The destination decrypts and decodes the data for the approved user to recover the original sensor data. A mechanism of authentication was used to avoid others from accessing the data of the person. Table I introduce a comparative summary from the previous studies and compared with our work:

TABLE I
Comparative summary for the literature studies

Ref.	Purpose	Technology	Application	Results
[8]	Design a smart air conditioning application for smart home services	Raspberry Pi, M2M	Control of an air conditioner	Successfully design a smart air conditioner
[9]	To implement an IoT based home automation system through data processing	Arduino Uno, NodeMCU ESP8266 and Arduino Nano, IoT	Home control and monitoring system detect the presence of harmful gas and measure temperature and humidity	Successfully can control the proposed system remotely by android smart phone via internet
[10]	To eliminate potential information security threats	Web-based smart home interfaces	Secure smart home for the elderly and disabled	The system is capable of using confidential messaging between smart home inhabitants and people they would like to communicate

[11]	To control and monitor home appliances using android application over internet	Arduino Mega, IoT, Wi-Fi	Home control and monitoring system	The system capable solution has proved to be controlled remotely, provide home security and it is low cost as compared to the previous systems
[12]	To present a small IoT system designed and created by utilizing a WLAN network based on Node MCU ESP8266	NodeMCU ESP8266, IoT	Real-time home security, automation, monitoring, and controlling of remote systems	Successfully implemented an intelligent, comfortable, and energy-efficient system
[13]	To design a cost-worthy of an embedded device for real-time monitoring of newborn babies in the incubator	IoT, Arduino, NodeMCU, Wi-Fi	Monitor's oxygen supplementation and pressure levels, monitors the temperature, radiation, pulse activity, and air humidity, gas around the environment	Successfully monitor and maintain environmental conditions suitable for a newborn baby, store data, and check the values every second
[14]	To develop a new solution which controls some home appliances	NodeMCU ESP8266, IoT Arduino UNO	Provides information about the energy consumed, check the level of gas detects the human object	The system achieved the development of smart home by using the IoT
[15]	To presents a simple prototype of smart home, or the easy way and low cost to control loads by Wi-Fi connection generally	NodeMCU ESP8266, IoT	Home control and monitoring system	Based on the results of analysis of all data obtained by testing the smart home, the system accomplished successfully
[16]	To constantly monitor the patient's physiological parameters	NodeMCU ESP8266, IoT Arduino UNO	Healthcare monitoring system	The system achieved the desired result
[17]	To secure the WiFi-based data transmission system that encrypts and encodes data	IoT	Smart sensors data encoding, Smart cities, Real time data security	The system successfully avoids any attackers to attack the citizen's personal data when it is wirelessly transmitted from any source to any destination
[18]	Provide essential security to homes and associate control operations	Raspberry Pi	Home control and monitoring system	The smart home system successfully designed and implemented
[19]	To design and implement a cost-effective IoT based autonomous alarm and access control system	Ethernet module, IoT	Control the states of the alarm, set an alarm, lock, and unlock the door, monitor the state of the door	The aim of developing a cost-effective IoT based autonomous alarm and access control system is accomplished
[20]	To give ease in everyday life, provide comfort, authentication and security, and additionally spare power and human endeavor	Arduino Mega 2560, Arduino UNO, GPRS, ESP8266, Ethernet Shield, Router	Controlling and indicating electrical and electronic devices in houses and buildings	The implementation of the system was managed successfully, the system can work with all its pieces through the internet properly
[21]	To provide secure data transmission among several associated sensor nodes in the network	Intel Galileo Board, Wi-Fi Module (N-2320), IoT	Secure data transmission, facilitate energy-efficient data encryption	The proposed TBSA algorithm consumed less energy in comparison with some existing methods
[22]	To study and evaluate a suitable set to develop a smart door lock which is intended to offer high security, easy access, and control	IoT, Microcontroller, Bluetooth beacons	Smart door lock	A fully functional smart door application was accomplished, and the result of security implementation of the product was an overall, more robust
[23]	To explores the Android OS as a medium to manage and operate different sensors embedded within smartphones	IoT	Extract the data from sensors, data in the local database, Transfer data via HTTPS to Ubidots	The Android application completed successfully all the tasks that were programmed
[24]	To solve the problem of the popularity of smart homes due to high costs in real life	NodeMCU ESP8266	Smart home control system	The system worked normally, and the monitoring data can be reflected in the monitoring interface in real-time
[25]	To optimize performance and saves unnecessary wastage of power	NodeMCU	Home control and monitor	Proposed a user-friendly system that can be used for benefiting the mass. Also, the cost of the system is within reach
[26]	To present a cost reduced and flexible home control and monitoring system	Raspberry Pi, IoT	Accessing and controlling devices and appliances remotely	The projects achieved desired results and can be said to be done successfully
[27]	To monitor the status of the door, controlling the door, and increasing security in a house	ESP32, IoT	Door security system	The motion detection sensor can detect movement accurately up to 1,6 meters ahead, and messages published encrypted properly
[28]	To switch to automated state controlling the appliances automatically as per the sensors' readings	IoT, NodeMCU, Raspberry Pi	Home control and monitoring system	The project was designed and implemented successfully

[29]	To design a system to help reduce the energy consumption	Arduino, IoT	Monitor electricity consumption and trace the history of electricity consumption data	The system successfully worked to control the monitoring of the amount of electrical energy usage through IoT
Our work	To create a prototype for an IoT-based smart home system to monitor and control electrical equipment and to protect the system's data from hackers and intruders while connecting with the internet	Arduino Uno, NodeMCU ESP8266, IoT	Home control and monitor remotely from a smartphone application and web application, Door unlock, Door status, Window status, system encryption, and decryption	Our work accomplished to designs a smart home system that enables homeowners to control and monitor appliances remotely, and also the data of the system was encrypted and decrypted properly

Based on Table I, we can analyze that every author comes with different technology and concept for the smart home system. With these different technologies, designs, and algorithms. The common purpose of every author's work was to smoothen the lives of homeowners, the old aged, and disabled people, save electricity, provide comfort, authentication, and security, a cost-reduced and flexible home control and monitoring system, and additionally spare power and human endeavor. Compared to the above smart home system applications, our system can be more secure with the AES technique by encrypting and decrypting the entire system parts and being more protected and more secure from hackers and intruders connecting with the internet. Furthermore, our system can be monitored and controlled remotely from anywhere and anytime by mobile application and web application.

3. SYSTEM DESIGN

The designed system has two main parts: hardware design and software design. The hardware part is constructed by arranging microcontrollers, actuators, and sensors while programming written and uploaded into the microcontrollers is included in the software part. The system performed in this paper displays microcontrollers connected to household devices for monitoring and controlling sensor modules and actuator modules. The general block diagram of the performed system is shown in Figure 1. This design section demonstrates how various components of the hardware are set up. The system uses an IoT platform and mobile application to control three loads and to monitor four sensor modules.

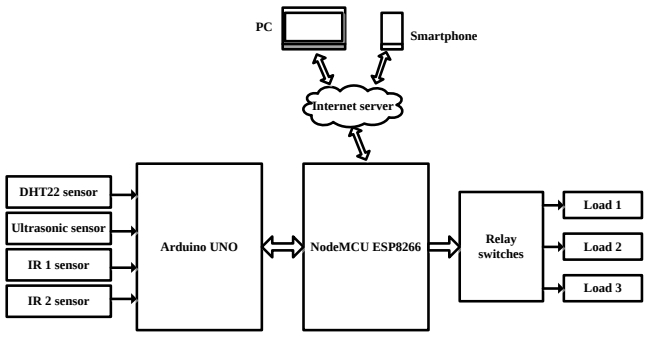

Figure 1. The general block diagram of the performed system

The requirements, data relating to different components and different functional units used in the performed system are listed below:

3.1. Arduino Uno

Arduino is an open source hardware and software platform that encourages ease of use. It has an electronic circuit board (Known as a microcontroller), and a ready to use a program called Arduino IDE to write a program code and upload it to the physical platform. Arduino boards can read and transform analog or digital input signals from various sensors into outputs such as triggering a motor, turning ON/OFF LED, connecting to the cloud, and several other activities. Using Arduino IDE, you can control your board functions by sending a series of instructions to the board microcontroller [30]. In this system, Arduino reads the sensor modules data and send them via serial communication UART protocol to NodeMCU.

3.2. NodeMCU ESP8266

NodeMCU is a Lua-based open-source firmware and development board specifically designed for IoT-based applications. It includes firmware running on Espressif Systems' ESP8266 Wi-Fi SoC, and ESP-12-based hardware. By connecting it to any microcontroller using the serial UART or directly as a Wi-Fi enabled microcontroller by programming a new firmware using the SDK, the ESP8266 can be used as an external Wi-Fi module. This microcontroller has built-in Wi-Fi networking support to send and receive mobile data via a web server [31]. In this paper, it receives sensor data from Arduino Uno and sends them to the Blynk mobile application and Ubidots IoT platform, and then receives instructions to control home appliances from them. It then drives the relay module to power the appliances.

3.3. Sensor modules

The sensor modules gather their information about the current state of the environment in the home and submit that in turn to the Arduino board and then Arduino transfer the data by UART serial communication protocol to NodeMCU. Three types of sensor modules are used in the project, the HC-SR04 ultrasonic sensor for distance measurements, DHT22 temperature and humidity sensor to detect room ambient temperature and humidity, and IR1 and IR2 obstacle avoidance sensor to monitor the status of the door and window respectively.

3.4. Relay module

It is a 5V relay interface board, it has a standard interface that a microcontroller can control directly. In this study, three switches are used, two are used to turn ON/OFF the lights and the other one is used for unlocking/opening the solenoid door lock. The NodeMCU output signal activates and deactivates the relay for switching.

3.5. Solenoid electric door lock 12V

The solenoid is electromagnets. As electricity is applied, the coil of copper wire inside is energized and magnetized. In the performed system the solenoid is used to unlock/open the door.

3.6. Blynk

Blynk is an IoT platform that enables remote control of electronic devices using android and IOS software. It offers a dashboard that allows the user to build a graphical interface with various widgets. Sensor data can also be stored and displayed by Blynk [32]. Blynk provides libraries to the most common hardware platforms like SparkFun, Arduino, Raspberry Pi, ESP8266, etc. Libraries, server, and application are the three most significant components in the Blynk. The application can assist to construct the GUI. All the communication between the hardware and application is the server's responsibility. And libraries use the commands to enable the communication between the server with hardware. NodeMCU is the main component of this project. It is connected with an external power source with cable and also receives sensor module data from Arduino. Relay is the next critical component. The door and lights are connected with NodeMCU through the relay. We can run all devices via the Blynk server using the Blynk application. Different buttons are added in the Blynk application, using certain buttons that can turn ON/OFF the switches.

3.7. Ubidots

Ubidots platform is also used in this paper which is a cloud storage system that uses IoT to store a vast amount of information and record several values for every second. Each Ubidots user has the API credential to be included in the code. Then Ubidots are linked to the hardware, and hardware-measured data is sent to the IoT platform. The device in Ubidots is a virtual representation of data sources [33]. It transmits data from the sensor to the cloud of Ubidots through a connection protocol. When the device is built, it receives hardware data and is displayed inside the device in a variable. This is achieved in the code by using variable names. It is applied to the dashboards as a widget to visualize the data after data is presented in a variable. Users may display data as a table, indicator or graph, etc.

3.8. Advanced Encryption Standard

The AES is a symmetric key algorithm. AES used a 128, 192, 256-bit block length. AES is centered at the top of the network of permutations and substations. AES used a block size that was set. AES acts on a 4x4 bytes column-major order matrix. It is fast to implement hardware and software in equal measure. AES offers high and fast security [34]. Low power consumption is used by AES.

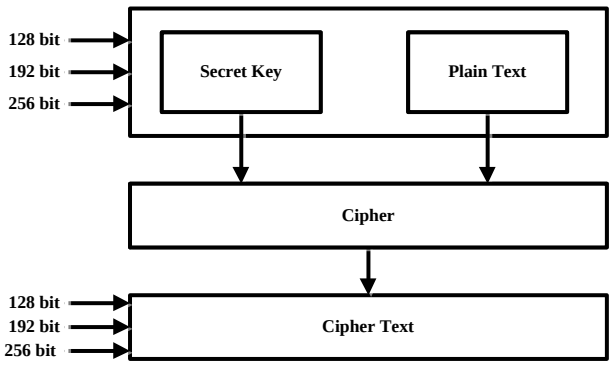

Figure 2. AES design

The AES conducts byte-based computations. 128 bits of a plaintext block is used as 16 bytes by AES. These 16 bytes are divided into four rows and four columns. AES is a variable depending on the key length. The AES cipher specifies the number of conversions round repeats that the input exchange is called plaintext, and the cipher text is called the final output [35]. In this study, we provide a secure data mechanism, using the AES method to improve data security. The AES technique encrypts and decrypts data before sending it from one device to another. Figure 2 shows the AES technique design.

4. SYSTEM IMPLEMENTATION

The performed system allows users to monitor and control their home appliances remotely at any time, using smartphones, tablets, and PCs. Using a mobile application and IoT platform, the user is able to control his or her home appliances easily through the internet by reading sensor data in their mobile application and IoT platform webpage. Figure 3 shows the schematic diagram of the performed system.

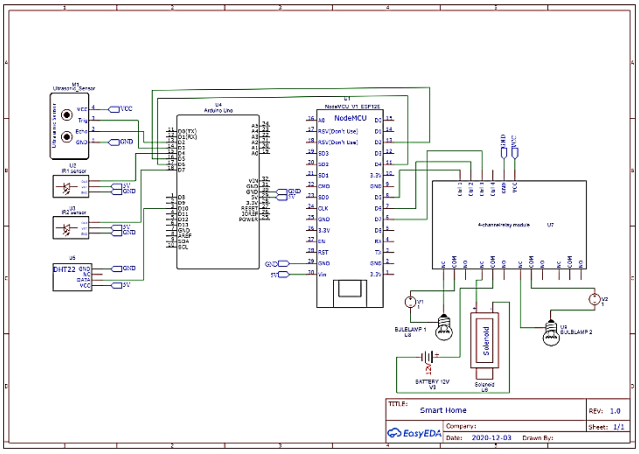

Figure 3. Schematic diagram of the performed system

NodeMCU needs to be identified to the SSID, the password, and token code letting the server of Blynk and Ubidots connects them. Sensors send variable data to Arduino Uno regarding environmental conditions and then Arduino Uno transfer the data to the NodeMCU via serial communication UART protocol. The user receives this information from the internet server in his/her mobile application and IoT platform and then decides on his/her behavior to control the appliances. NodeMCU ESP8266 receives the instruction from the internet server when pressing the required button in the application and platform and provides the actuator circuits with an output signal. When the relay is switched high, the power from the source is obtained by the devices. The switching circuit is used for turning lights ON/OFF and unlocks the door. Furthermore, the Blynk application and Ubidots IoT platform webpage show the temperature and humidity so the user can read the information on the DHT22 sensor, monitor the status of door and window by IR1 and IR2 sensors and, also the ultrasonic sensor displays the distance measurements of an object in the house. In order to achieve the desired performance, the encryption part involved, it consists of several processes and techniques. Encrypting all the data through the server and ESP8266 is the main concept. The processes that were involved in this project are encrypting and decrypting using AES-128

and also encoding and decoding the encrypted data to make it more secure. The process starts by ESP8266 at first gets the original sensor modules data from the Arduino with the original load's data connected with NodeMCU. This data will be encrypted into a string by the AES algorithm, only the system knows what are these generated data means and after the data are encrypted, it will be encoded until it is sent to the server for the session to start. By decrypting and encoding, the server processes the data. The connection between the ESP8266 and the server must be authenticated. After all, data is encrypted and encoded, the strings will be sent to the server. The strings obtained by the server will be decrypted and decoded and the relation authentication will be recognized as a credential between the server and ESP8266. The complete flowchart that gives the entire performed system operation is shown in Fig 4.

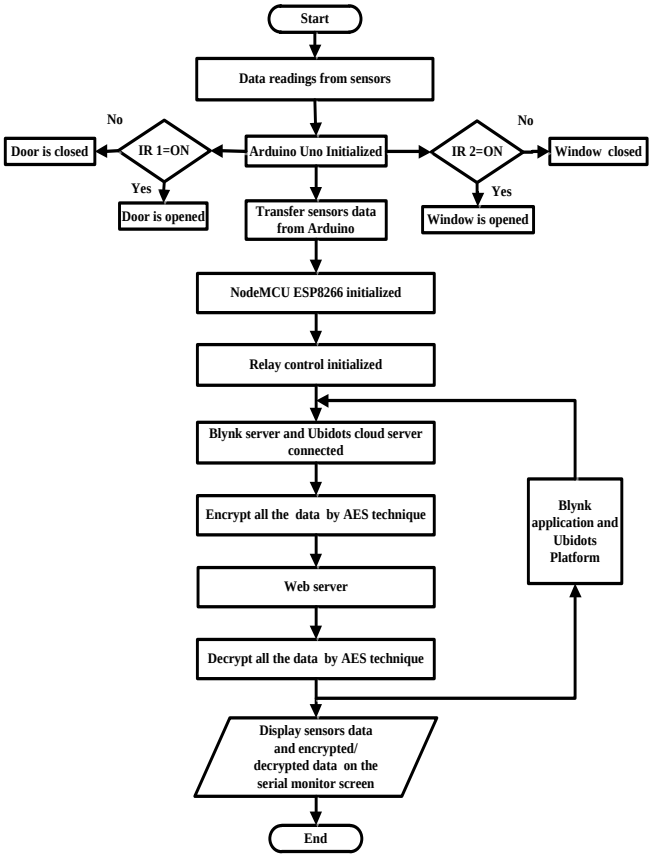

Figure 4. Flowchart diagram of the performed system

To display the value of sensor modules on the Blynk application and Ubidots IoT cloud platform, NodeMCU ESP8266 returns the output values of the sensor modules to the Blynk application and Ubidots platform, the remaining process are only commands send from ESP8266 to the mobile application and web application to control the appliances. Figure 5 and Figure 6 show and explain the Blynk and Ubidots operations respectively.

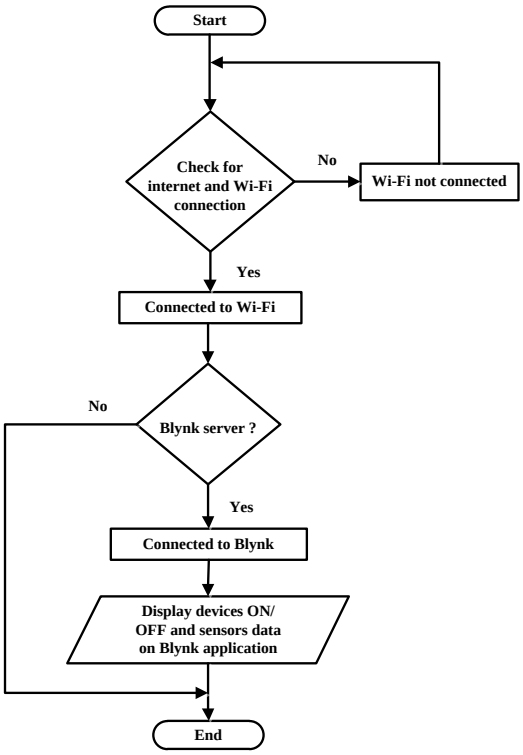

Figure 5. Flowchart diagram of Blynk operation

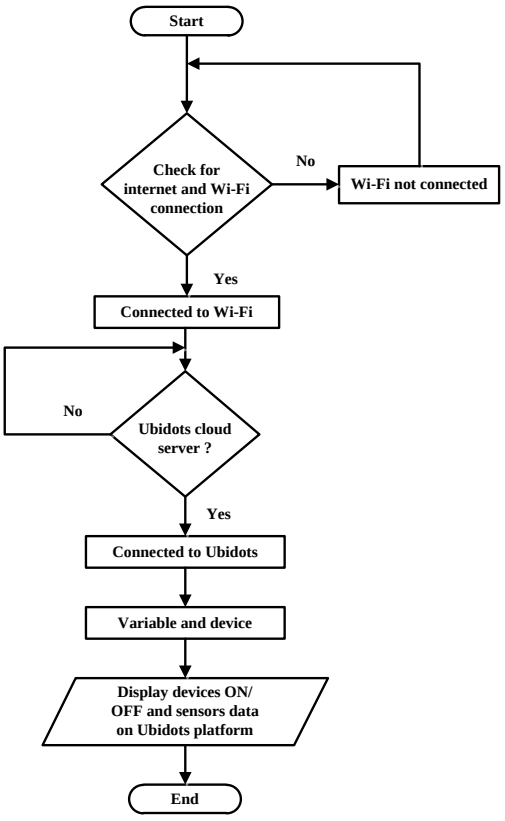

Figure 6. Flowchart diagram of Ubidots operation

5. APPLICATION RESULT

In the performed system, all hardware components were first verified and tested to ensure that all systems operate properly. Also, the key important parts of the system were tested to see

if they worked properly such as the connection between Arduino and NodeMCU for exchanging sensors data. Figure 7 shows the entire setup of the performed system.

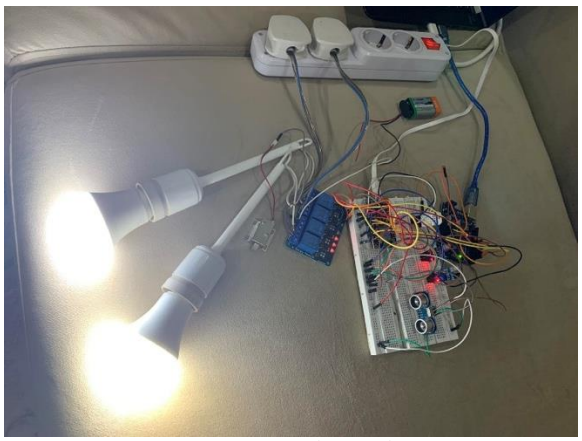

Figure 7. The entire setup of the performed system

Besides, the connectivity of the ESP8266 Wi-Fi module with the internet was tested to ensure that the connection was properly made. Figure 8 illustrates the sensor readings data on the serial monitor.

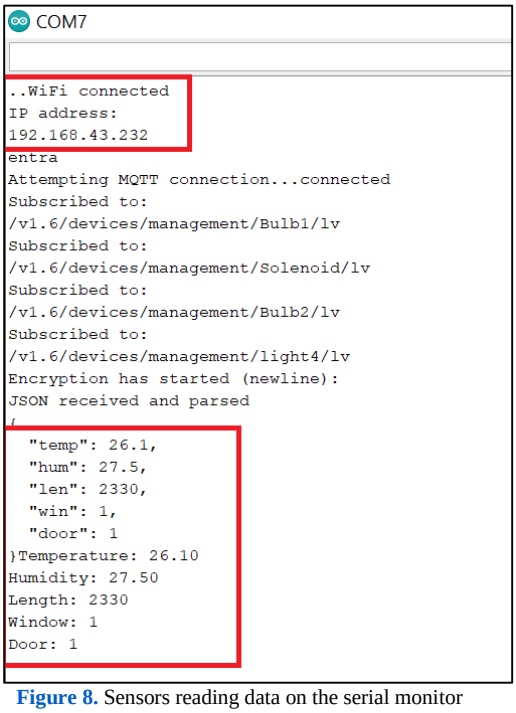

Figure 8. Sensors reading data on the serial monitor

The results on the serial monitor screen, shows that the Wi-Fi ESP8266 is connected to the internet and the IP address has been obtained. And also, the figure shows the data readings of the sensors, which read the temperature and humidity degrees in real time and their incoming data comes from the sensor DHT22, the ultrasonic sensor which is known as the “length” in the Arduino IDE code to measures the distance of an object, and the status of the door and window is called "win" and "door", which indicates their status if the door and window are closed, "0" will be displayed, and "1" will be displayed if it is open and their data comes from IR1 and IR2 sensors respectively. Results are acquired after the system hardware and software implementation and can be viewed on the internet created by the Blynk android application and Ubidots IoT cloud platform webpage.

The Blynk application provides the facility for easy monitoring, reading of sensor data, and controlling appliances. There are three different tabs for the three appliances namely solenoid, light 1, and light 2 also, there are display widgets that show sensor modules readings from Arduino Uno to NodeMCU via the Blynk server which is named length, temperature, humidity, door status, and window status. On the button widget, the current ON/OFF status of the system is displayed. The home appliances can be operated from any remote location by pressing the virtual button on the smartphone. The results of the designed system obtained on the Blynk android applications are shown in Figure 9.

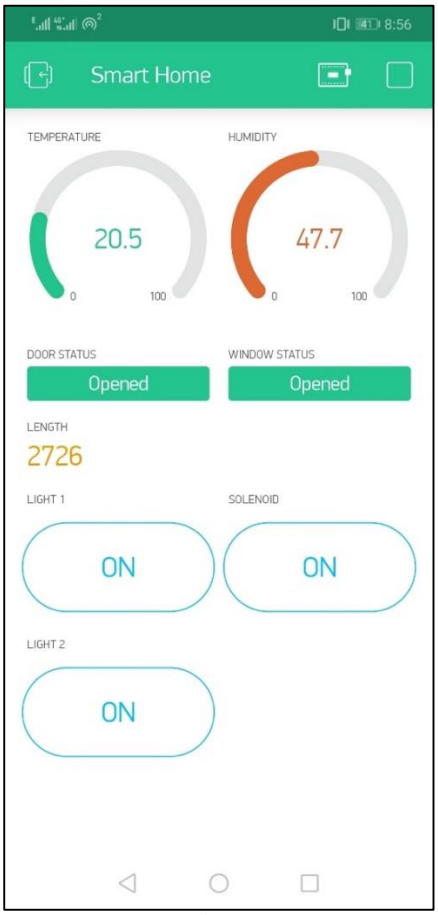

Figure 9. Screenshot of the Blynk application

The Ubidots IoT cloud platform is the best connection for the IoT. Ubidots provides developers with a platform that allows them to quickly capture sensor data and convert it into helpful information and also control appliances in an easy way. Using the Ubidots platform to send data to the cloud from any web-enabled device. The dashboards use widgets such as metrics, indicators, tanks, thermometers, and button switches to display the data. The dashboard generated in the platform uses thermometer and tank widgets to visually show the temperature and humidity degrees reading in real-time, and their incoming data comes from the DHT22 sensor. The indicators used on the IoT platform dashboard named door status and window status to show and monitor the status of the door and window if it's open or closed and their data comes from IR1 and IR2 sensors. The distance of an object measured by the ultrasonic sensor

using a metric widget identified as a length on the dashboard and finally, three button switches generated on Ubidots platform dashboard to switch ON/OFF relay board which is connected to bulb1, bulb2, and solenoid to unlock the door. Figure 10 illustrated all the widget used in Ubidots platform webpage.

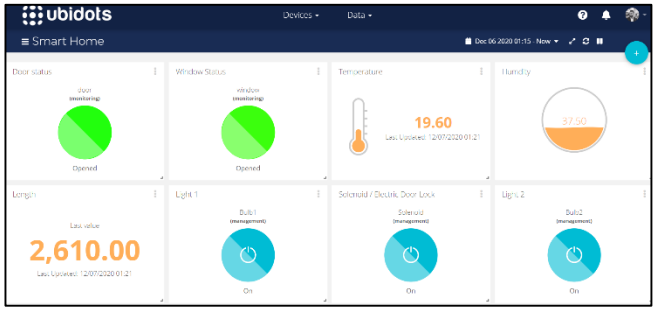

Figure 10. The system web page of Ubidots IoT platform

Figure 11. Data encrypted and decrypted by AES displays on the serial monitor

Encryption is a mechanism that transforms the actual information into an encrypted data. The results are shown on the serial monitors in Figure 11, in the beginning, all the incoming data from ESP8266 are encrypted into a string by the AES algorithm, only the system knows that what is this generated data means. And, it also relies on the size of the information which requires to be processed. After that, this information is sent to the ciphertext. Finally, all the encrypted data are encoded and sent to the server.

Decryption is a mechanism for converting encrypted information returns to their original data. When the server receives encrypted and encoded data, the server decrypts the data first and then go through the decoding process to get back to the original data.

6. CONCLUSION

The performed system in this paper is a simple design of an IoT-based smart home system. The performed system is designed and successfully implemented. In this project, all sensor modules data are sent to NodeMCU by Arduino Uno, and home devices are connected to NodeMCU by relay module which then sends to the Blynk server and cloud server of Ubidots by ESP8266 Wi-Fi. The data can be monitored and controlled on the Blynk application and Ubidots platform webpage. Also, all the data are encrypted through ESP8266 and the server by using the AES method. The process that was involved to secure the data is encrypt/decrypt using AES-128. To prevent others from accessing the user's data, an authentication method is used. This system refers to the real-time automation, monitoring, and control of remote systems.

Future studies will concentrate on incorporating the proposed system into essential smart home services. By using various sensors and various home appliances, this work can also be further improved.

REFERENCES

[1] J. Y. Kim, H.-J. Lee, J.-Y. Son, and J.-H. Park, "Smart home web of objects-based IoT management model and methods for home data mining," *in 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2015, pp. 327-331.

[2] K. Agarwal, A. Agarwal, and G. Misra, "Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT," *in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 629-633.

[3] L. Salman, S. Salman, S. Jahangirian, M. Abraham, F. German, C. Blair, et al., "Energy efficient IoT-based smart home," *in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 526-529.

[4] R. Sarmah, M. Bhuyan, and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," *in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 59-63.

[5] V. D. Vaidya and P. Vishwakarma, "A comparative analysis on smart home system to control, monitor and secure home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation," *in 2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 2018, pp. 1-4.

[6] M. Baykara and S. Abdullah, "Designing a Securable Smart Home Access Control System using RFID Cards," *Journal of Network Communications and Emerging Technologies (JNCET), vol. 10, 2020.*

[7] T. Alaswad, "An Investigation into the Security Challenges and Implications Surrounding Smart Home Technologies," *Cardiff Metropolitan University*, 2017.

[8] R. Das, G. Tuna, and A. Tuna, "Design and Implementation of a Smart Home for the Elderly and Disabled," *International Journal of Computer Networks and Applications (IJCNA), 2(6), p.242-246*, 2015.

[9] K. Mandula, R. Parupalli, C. A. Murty, E. Magesh, and R. Lunagariya, "Mobile based home automation using Internet of Things (IoT)," *in 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2015, pp. 340-343.

[10] G. Tuna, "Secure Web-Based Communication Framework For Smart Home Systems Designed For The Elderly And Disabled," *in Proceedings of International Academic Conferences*, 2016.

[11] P. S. N. Reddy, K. T. K. Reddy, P. A. K. Reddy, G. K. Ramaiah, and S. N. Kishor, "An IoT based home automation using android application," *in 2016 International conference on signal processing, communication, power and embedded system (SCOPES)*, 2016, pp. 285-290.

[12] H. Durani, M. Sheth, M. Vaghasia, and S. Kotech, "Smart automated home application using IoT with Blynk app," *in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018, pp. 393-397.

[13] D. Sivamani, R. Sagayaraj, R. J. Ganesh, and A. N. Ali, "Smart incubator using internet of things," *International Journal for Modern Trends in Science and Technology, vol. 4, pp. 23-27*, 2018.

[14] H. Singh, V. Pallagani, V. Khandelwal, and U. Venkanna, "IoT based smart home automation system using sensor node," *in 2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, 2018, pp. 1-5.

[15] A. H. Imam, "A Simple Smart Home based on Iot Using Nodemcu and Blynk," *Universitas Muhammadiyah Surakarta*, 2019.

[16] K. T. Wai, N. P. Aung, and L. L. Htay, "Internet of Things (IoT) Based Healthcare Monitoring System using NodeMCU and Arduino UNO," 2019.

[17] I. Farahat, A. Tolba, M. Elhoseny, and W. Eladrosy, "Data security and challenges in smart cities," *in Security in smart cities: Models, applications, and challenges, ed: Springer*, 2019, pp. 117-142.

[18] A. H. Hassan, A.-f. Y. Awad, and A. H. El-Amin, "Smart Home: Home Monitoring & control System using Simple Mobile App," *Sudan University of Science and Technology, 2015*.

[19] L. P. Akhtar, "IoT based autonomous office alarm and access control system," *Master's Thesis, Technical University of Denmark, 2017*.

[20] I. Mohammed and E. Duman, "Implementation of a smart house application using wireless sensor networks," *in 9th International Conference on Networks & Communications. Computer Science & Information Technology, 2017*, pp. 53-70.

[21] S. Pirbhulal, H. Zhang, M. E. E Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y.-T. Zhang, et al., "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, p. 69, 2017.

[22] M. Almosawi and K. Djupsjö, "IoT Security Applied on a Smart Door Lock Application," ed, 2018.

[23] J. Alonso, C. Bayona, O. Rojas, M. Terán, J. Aranda, H. Carrillo, et al., "Iot solution for data sensing in a smart campus using smartphone sensors," *in 2018 IEEE Colombian Conference on Communications and Computing (COLCOM), 2018*, pp. 1-6.

[24] T. Qiang, G. Guangling, C. Lina, and W. Han, "Nodemcu-based Low-cost Smart Home Node Design," *in IOP Conference Series: Materials Science and Engineering, 2018*, p. 012013.

[25] R. Mahindar, M. Prakash, S. Ghosh, S. Mukherjee, and R. Ghosh, "IoT-based home appliances control system using NodeMCU and Blynk server," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, pp. 16-22, 2018.

[26] R. Majhi, "IoT: Home Automation," 2019.

[27] C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door security system for home monitoring based on ESp32," *Procedia Computer Science*, vol. 157, pp. 673-682, 2019.

[28] B. Bohara, S. Maharjan, and B. R. Shrestha, "IoT based smart home using Blynk framework," *arXiv preprint arXiv:2007*.13714, 2020.

[29] A. Surriani, A. Pradana, M. Arrofiq, J. Putra, M. Budiyanto, and L. FSubekti, "Design of Power Monitoring Application," *in IOP Conference Series: Materials Science and Engineering, 2020*, p. 012069.

[30] S. A. Arduino, "Arduino," *Arduino LLC, vol. 372*, 2015.

[31] D. A. Aziz, "Webserver based smart monitoring system using ESP8266 node MCU module," *International Journal of Scientific & Engineering Research, vol. 9*, pp. 801-808, 2018.

[32] M. S. Osman, "Smart home meter reading using IoT with Blynk app," *in AIP Conference Proceedings*, 2019, p. 020109.

[33] L. Enciso and A. Vargas, "Interface with Ubidots for a fire alarm system using WiFi," *in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 2018, pp. 1-6.

[34] R. Daş and G. Tuna, "Design and implementation of a simple, AES-based secure messaging platform," *in The International Conference on Engineering and Natural Sciences (ICENS)* 2016, Sarajevo, May 2016, pp. 47–52. [Online]. Available: https://www.icens.eu/album/icens-2016

[35] S. Heron, "Advanced encryption standard (AES)," *Network Security, vol. 2009*, pp. 8-12, 2009.

BIOGRAPHIES

Resul Das received his B.Sc. and M.Sc. in Computer Science from Firat University in 1999, 2002 respectively. Dr. Das received his Ph.D. degree from the Electrical and Electronics Engineering Department at the same university in 2008. He is currently a Professor and Chair of the Software Engineering Department at Firat University, Turkey. He has authored several papers in international conference proceedings and refereed journals and has been actively serving as a reviewer for international journals and conferences. His current research interests include complex networks, computer networks, web mining, knowledge discovery, information and network security, software design and architecture, and IoT/M2M applications.

Taha Ababaker received his B.Sc. in Electrical and Computer Engineering from the University of Duhok, Iraq in 2011. He is currently an M.Sc. student at Firat University, Turkey department of software engineering. He has interests in Computer Networking, Computer Programming, IoT, Computer Organization, and Digital Image Processing. He can fluently speak English and Arabic.