A New Home Gateway Design and a Sensor-Based Smart Home Application Including Privacy Protection

Araştırma Makalesi/Research Article

Murat DENER

Computer Sciences and Engineering, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, Turkey
muratdener@gazi.edu.tr

(Geliş/Received:26.06.2018; Kabul/Accepted:05.12.2018)
DOI: 10.17671/gazibtd.437339

Abstract— In this study, a new SIM900 GSM / GPRS module card has been designed. Also, a new home gateway has been designed and implemented by combining the newly designed module with sensor nodes previously developed by us. In addition, this home gateway and sensor nodes are used together to implement a smart home application. In the application, temperature-humidity, light, air, water and motion sensors are used. Users can control and monitor both location-based and sensor-based. A secure communication is established between the sensor nodes and the home gateway with AES encryption algorithm. The work is an originality because it includes both a new home gateway design, smart home application and privacy protection. This work will be beneficial to smart home users and practitioners.

Keywords— home gateway, smart home, privacy protection, AES, sensors

Gizlilik Koruması İçeren Yeni bir Ev Ağ Geçidi Tasarımı ve Sensör Tabanlı Akıllı Ev Uygulaması

Özet— Bu çalışmada, yeni bir SIM900 GSM/GPRS modül kartı tasarlanmıştır. Yeni tasarlanan modül ile daha önce tarafımızdan geliştirilen sensör düğümler birleştirilerek yeni bir ev ağ geçidi elde edilmiştir. Ek olarak bu ev ağ geçidi ve sensör düğümler birlikte kullanılarak bir akıllı ev uygulaması yapılmıştır. Uygulamada sıcaklık-nem, ışık, hava, su ve hareket sensörleri kullanılmıştır. Kullanıcılar hem mekan bazlı hem de sensör çeşiti bazlı kontrol ve takip yapabilmektedir. Sensör düğümler ve home gateway arasında ise AES şifreleme algortiması yardımıyla güvenli bir iletişim kurulmuştur. Yapılan çalışma, hem yeni bir home gateway tasarımı, hem akıllı ev uygulaması hem de gizlilik koruması içerdiğinden dolayı bir özgünlük oluşturmaktadır. Bu çalışmanın, akıllı ev kullanıcılarına ve uygulayıcılarına yararlı olacağı değerlendirilmektedir.

Anahtar Kelimeler— home gateway, smart home, privacy protection, AES, sensors

1. INTRODUCTION AND RELATED WORKS

With the progress of technology and the decrease in the prices of materials in semiconductor technology, today it is becoming possible to see more smart home technologies. Sensors are becoming cheaper, larger data storage servers, big data and cloud technologies offer a significant contribution to the increase of smart home systems. Smart home systems are systems that enable home-use materials to be integrated into an automation system, which in turn makes life easier at the highest level [1]. Together with smart home technology, our home lighting, climate, and other needs are monitored and controlled over a single center. With the scenario feature, many systems can move at the same time. Raw material of smart home systems is sensor nodes. Sensor nodes are nodes that fulfill the tasks assigned to them by a collaborative effort with communication-computation-sensing capabilities despite limited processor-memory-energy [2]. Gateways are where the sensor nodes send the information they perceive. Communication between the user and the sensor nodes is established by the gateway. In smart home systems, it is very important to design a home gateway that collects information from all the sensors and keeps in touch with them, and also

communicates with the sensors to the server or directly to the users according to the degree of importance they receive. Thanks to the home gateway, the home is centrally managed.
One of the most important elements in a home is security. Especially the security needs of smart homes are more than those of other homes [3].

Intelligent devices are notified directly in the event of a security breach or natural disaster, thanks to sensors and visualization systems placed in appropriate parts of the home during situations such as theft, earthquake, fire, flood. Because the devices inside the home communicate wirelessly, the Communication bus is air. In this case, according to the wired connections, it is necessary to consider more security in wireless connections. An attacker who has leaked information circulating inside the home, sabotes the operation of the system or send the wrong information to the network and jeopardize the security of the users by sending different notifications to the home network. Therefore, the security of the system should be considered along with the comfort in smart home systems.

The home gateway designs and experimental studies in the literature are as follows.
The authors [4] designed an internet gateway for the smart home using the Raspberry Pi Model B device. The designed gateway is cheap and energy efficient. Temperature, humidity, carbon monoxide and PIR motion sensors are used in the study. In another study [5] it was aimed by the authors to help people. The proposed system collects the sensor data and sends them to the server. The system has Round robin scheduling to guarantee 3G interface, load balancing mechanism and transmission. The system is Raspberry Pi based. In another study [6], authors designed and implemented an embedded secure gateway. The hardware platform is based on two S3C6410 processors and an EP1C18F4620 FPGA. The software is based on Linux Kernel 3.0.1. In another study [7] the authors propose a new system architecture for managing and reducing energy use in their work. The developed prototype system consists of cloud platform, Raspberry Pi type B single board computer as home gateway and various sensors. In another study [8], the authors designed a new gateway based on the CC2530 single-chip-solution, using the ZigBee Light link wireless protocol. In addition, they have developed a small-scale lighting system. In another study [9] the authors developed a new gateway prototype with ZigBee and Bluetooth interfaces. The architecture they have developed is based on session initiation protocol and allows all devices to be controlled by a specific PC. In another study [10] the authors designed and implemented the Smart Home system based on the next generation network protocol IPv6. Thus, smart household goods can be connected directly to the Internet, which gives the user an experience. The home gateway is designed and implemented using the RIPng protocol. It is based on linux system and ipv6.In another study [11] the authors propose a new integrated access gateway architecture. The home gateway's operating mode and parameter configuration can be configured using a web portal. In another study [12], the authors describe the architectural components to be combined in the consumer electronics to implement the Network Connectivity Proxy function running in the home gateway. In addition, the effectiveness and scalability of the solution is discussed with the assessment of the potential benefits for consumers. In another study [13] the authors designed a secure home sensor node with a multi-sensor support such as PIR motion sensor, temperature-humidity sensor, NDIR CO2 sensor and fire sensors. The designed gateway can be connected to the CoAP device or to the CoAP gateway via the RS232 interface. In another study [14], the authors developed a scenario in which many in-home sensors communicate with an intelligent gateway over the Bluetooth low energy protocol and collect RF energy wirelessly transmitted via a private radio interface from the network. In another study [15], the authors investigated the problem of smart gateway deployment in intelligent home systems. This problem has been formulated and the complexity is reduced by applying a new method. In another study [16], authors propose a new home gateway. The recommended home gateway supports operations such as automatic configuration for restricted devices and device discovery for web services. Also, Home Gateway provides lightweight information delivery using MQTT-Message Queue Telemetry Transport protocol. Finally, in another study [17], the authors designed a new home gateway. The designed Smart Home gateway provides a transfer station between the family internal network and the external network. The home gateway consists of the main hardware controller S3C2440ARM9, Ethernet interface, SDRAM, NANDFLASH, power / reset module and KNX module.

In this study, a new SIM900 GSM / GPRS module card has been designed. Also, a new home gateway has been designed and implemented by combining the newly designed module with sensor nodes previously developed by us. In addition, this home gateway and sensor nodes are used together to implement a smart home application. In the application, temperature-humidity, light, air, water and motion sensors are used. Users can control and monitor both location-based and sensor-based. A secure communication is established between the sensor nodes and the home gateway with AES encryption algorithm.

Other parts of the work are as follows. In the second chapter, circuit diagrams and detailed explanations of the Home gateway are presented. In the third chapter, developed smart home application is explained. In the fourth chapter, the operations performed for privacy protection are mentioned. The fifth section contains the test and the results of the study. In the sixth chapter, the general results of the study are given.

2. HOME GATEWAY DESIGN

Home Gateway Node consists of WiSeN sensor node [18] and SIM900 GSM/GPRS node. The WiSeN sensor node has already been developed by us [18]. In this study, a new SIM900 GSM/GPRS node was developed and thanks

to the integration with the WiSeN sensor node, a new home gateway node was obtained.

The MSP430G2553 is used as a microprocessor in the WiSeN sensor node (Figure 1). In order to provide communication, the IEEE 802.15.4 CC2530 ZigBee module was used. In addition, the desired sensor can be connected to the WiSeN sensor node due to the communication interface. The WiSeN sensor node has the following elements:2.4 GHz IEEE 802.15.4 CC2530 ZigBee module, MSP430G2553 microcontroller, AT24C128 EEPROM, SHT11 temperature-humidity sensor, LED 1 green (ZigBee GPIO1), LED 2 yellow (MSP430 P1.0), LED 3 red (MSP430 P2.6), Button 1 (MSP430 S1 Reset), Button 2 (MSP430 S2 P1.3), Button 3 (ZigBee Reset), UART1 connector (for SIM900 node connection), UART2 connector (for monitoring serial port outputs), TEST connector (Programming), AN1 connector (MSP430 and ZigBee pin connection), I^2C 1 connector (SCL, SDA, GND, VDD), I^2C 2 connector (SDA, SCL, GND, VDD), I^2C 3 connector (SDA, SCL, GND, VDD, P2.6), J1 connector (Battery connection), J6 connector (EEPROM active - jumper), AIN/P1.4 (Analog input selection connector), On/Offswitch (Battery on/offswitch).

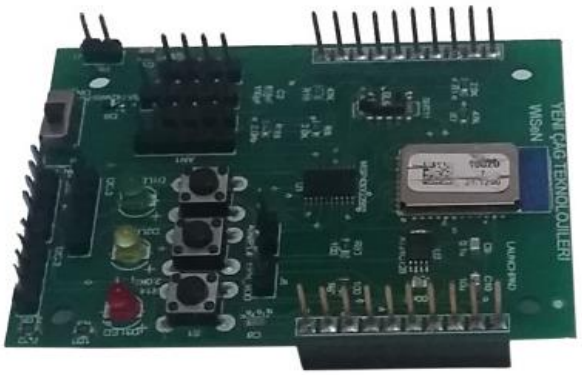


Figure 1. WiSeN Sensor Node

The corresponding pins of the WiSeN sensor node are connected to the corresponding pins of the newly developed SIM900 GSM/GPRS node to obtain the home gateway node. The newly designed SIM 900 GSM/GPRS node and the home gateway node are shown in Figure 2.

The Home Gateway Node can communicate with the outside via the SIM900 GSM / GPRS module while receiving information about the network in the environment via the ZigBee module. At the WiSeN Gateway Node, the circuit elements and functions included with the SIM900 GSM / GPRS Module are given below.

UART1 connector: Using this connector, the connection can be established with UART protocol. The RX, TX, GND and PWRKEY terminals of the SIM900 module are connected to the UART1 connector. The PWRKEY pin connects to the P2.1 pin of the MSP430G2553 microcontroller. The module opens when the PWKEY pin of the SIMPLE module of the MSP430G2553 microcontroller and the PWKEY pin of the SIM900 module are held at logic "0" and subsequently received at logic "1". For the SIM900 module to remain open, PWRKEY pin logic "1" must be applied.

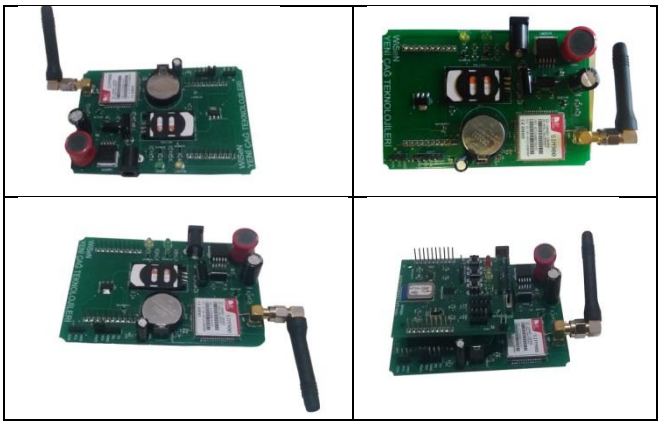


Figure 2. Newly designed SIM 900 GSM/GPRS node and the home gateway node

12V connector: It is a connector to be used to energize the Gateway Node. DC 12 V voltage must be applied. The voltage source to be used must be able to supply 2000mA current.
ANT1 connector: It is a connector used for antenna connection.
SC1 SIM Card Slot: It is a connector to plug SIM card. The PIN code must be removed from another phone before the SIM card is inserted. The SIM card should be the largest type (2FF).
Micro or Nano SIM card should not be.
BAT1:VRTC is the voltage to be used to obtain the voltage. The voltage required for the operation of the SIM900 module's internal clock is provided by this battery. In this way, it is ensured that the SIM900 module does not lose time information.
PWRKEY: The SIM900 module is the signal to be used to turn the MSP430G2553 microcontroller on and off. In the WiSeN Sensor Node, the P2.1 pin of the MSP430G2553 microcontroller is connected to the PWRKEY terminal on the WiSeN Gateway Node via the UART1 connector. The SIM 900 module will be turned on if PWRKEY is applied logic "0" (0 Volt) and then logic "1" (VDD) is applied again.

The dimensions of the designed SIM900 GSM / GPRS node are 100,3mmx67,8mm.In addition, the Schematic Capture and PCB Layout of the developed SIM900 GSM / GPRS node is shown in Figure 3-4.

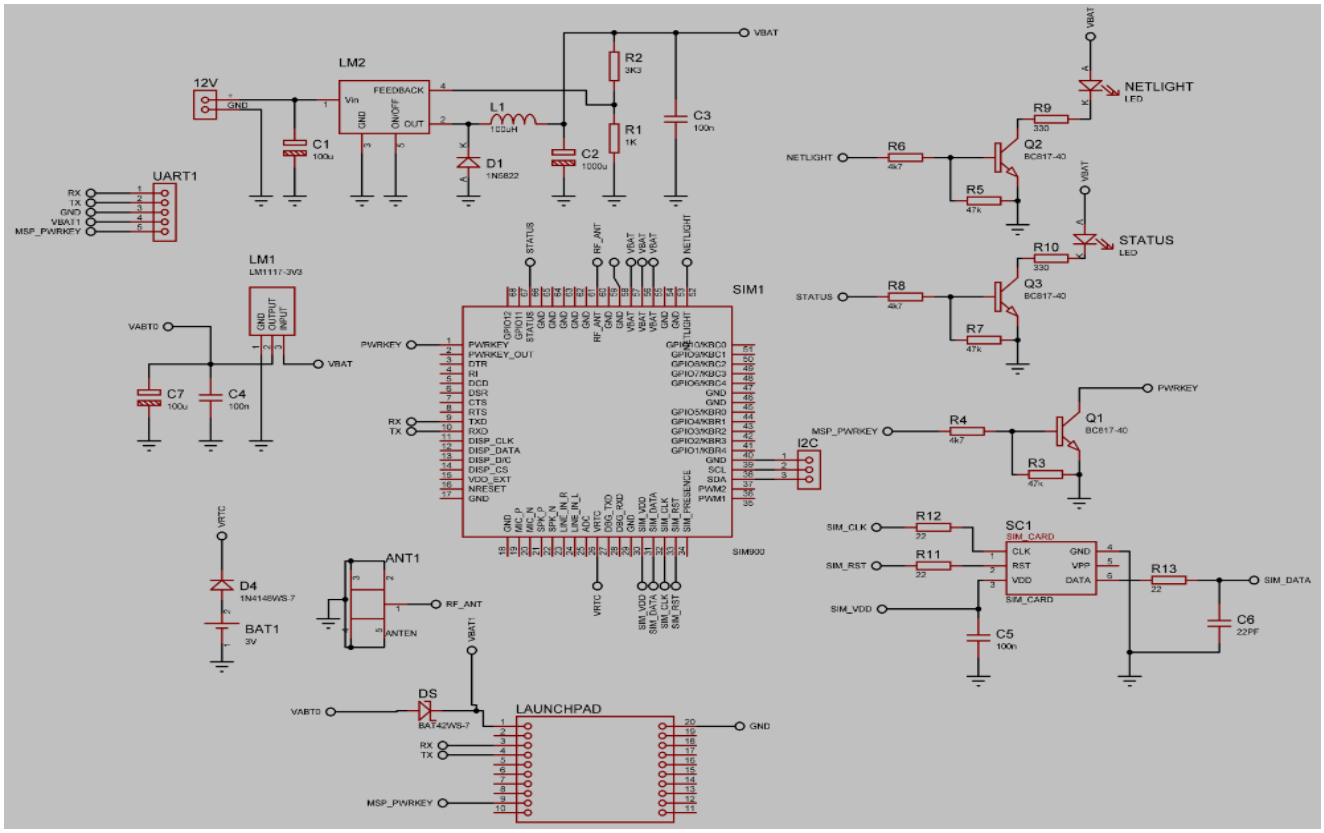


Figure 3. Schematic Capture of SIM900 GSM/GPRS node

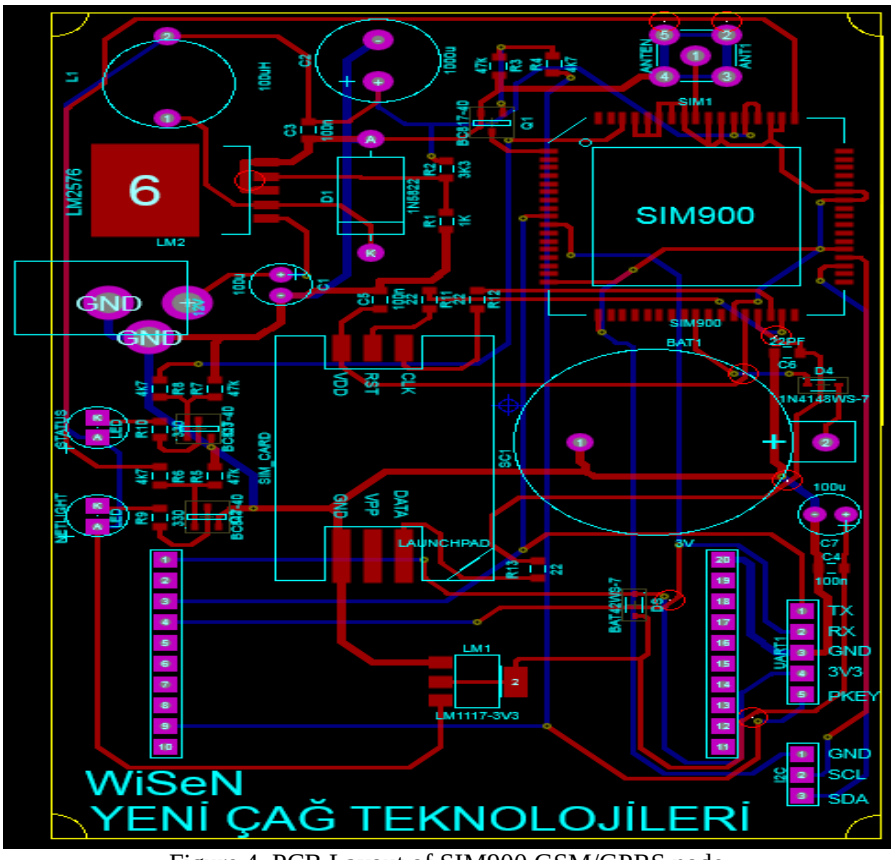


Figure 4. PCB Layout of SIM900 GSM/GPRS node

The Texas Instruments MSP-EXP430G2 Launch Pad [19] is used to program the developed home gateaway. The WiSeN sensor node and WiSeN gateway node can be connected directly to the MSP-EXP430G2 Launch Pad pins. In this way nodes can be easily programmed.

Texas Instruments MSP-EXP430G2 Launch Pad Features are as follows.14-/20-pin DIP (N) socket, Built-in flash emulation for debugging and programming, 2 programmable LEDs, 1 power LED, 1 programmable button, 1 reset button, Enables development on any MSP430 Value Line device with 14- or 20-pin DIP (N) packages, The LaunchPad's integrated emulator interface connects flash-based MSP430 Value Line devices to a PC for real-time, in-system programming and debugging via USB. In Figure 5, the programming card and the connection between programming card and designed nodes are given.

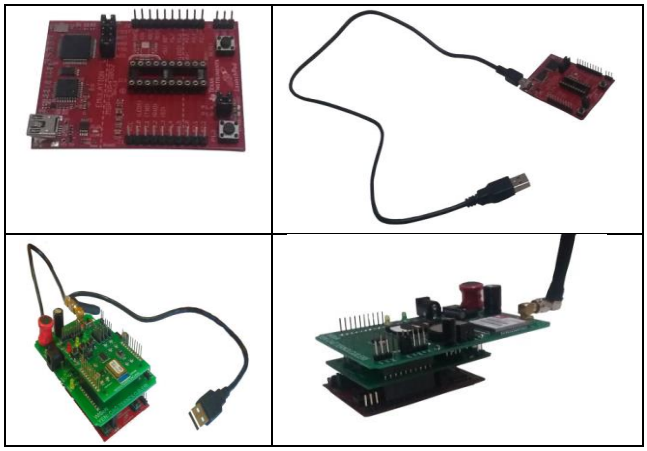


Figure 5. Programming card and the connection between programming card and designed nodes

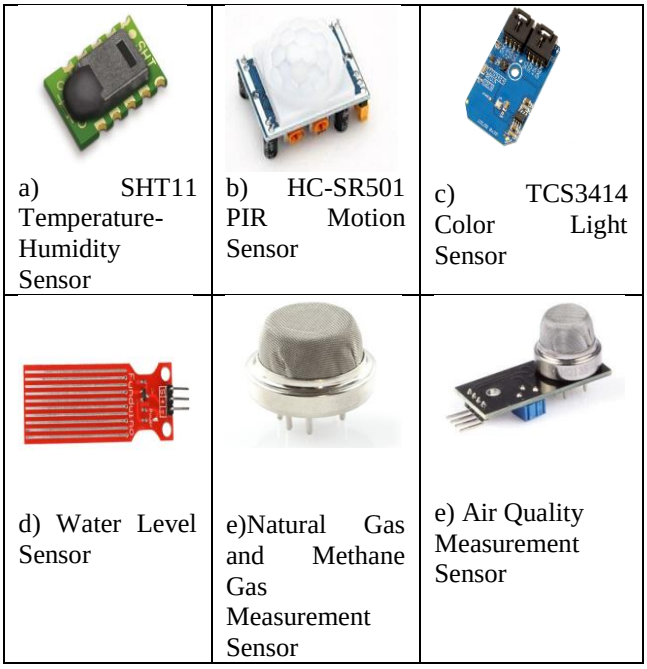
With these features, the Home Gateway can be reprogrammed in the direction of the user's request and can be used for various applications easily. It is a great privilege for the users to integrate the desired sensor into the wisens sensor node and to program the sensor node including the home gateway as desired.

3. SENSOR-BASED SMART HOME APPLICATION

In the study, Temperature and Humidity Sensor, Motion Sensor, Light Sensor, Water Sensor and Air Sensor (Figure 6) were used. The Temperature and Humidity Sensor is integrated into the Wisen sensor node. Other sensors are connected to the Wisen sensor node using the I2C communication bus and used in this way.

The models and information of the used sensors are given below.

Temperature and Humidity Sensor [20]: The temperature and humidity sensor used in study is the SHT11 sensor. This sensor is integrated into the Wisen sensor node. The SHT11 has a 14-bit AD converter and serial communication unit.The temperature value is 14 bit resolution (default value, 12 bits can be selected when requested), and the humidity value is 12 bit resolution (default value, 8 can be selected when requested) are transmitted to the microcontroller. Temperature measurement with ± 0.5 °C error between -40 °C and +128 °C, humidity measurement with ± 3.5% error. It provides low energy consumption. With this sensor, temperature and humidity values in the home are measured.At this point, the temperature and humidity level of the rooms in the home can be easily detected.



a) SHT11 Temperature-Humidity Sensor

b) HC-SR501 PIR Motion Sensor

c) TCS3414 Color Light Sensor

d) Water Level Sensor

e)Natural Gas and Methane Gas Measurement Sensor

e) Air Quality Measurement Sensor

Figure 6. Sensors used in smart home application

Motion Sensor [21]: The motion sensor used in study is the HC-SR501 sensor. This sensor is a sensor used to detect live motion in an environment. This sensor, which has a digital output, gives a logic 0 when it can not detect motion in the environment and a logic 1 when it detects motion. There are two potentiometers, Sx and Tx, on the sensor. The Sx potentiometer changes the visual range of the sensor from 3 to 5 meters.The Tx pot sets how long the sensor will output a logic 1 (3.3V) output from the output pin. With this sensor, a movement will be detected in the home or in the door-windows. This will contribute to the safety of the home.

Light Sensor [22]: The TCS3414 digital color light sensors are designed to accurately derive the color chromaticity and illuminance of ambient light and provide a digital output with 16-bits of resolution. It includes an 8 × 2 array of filtered photodiodes, analog-to-digital converters, and control functions on a single monolithic CMOS integrated circuit. All I2C Mini Modules are designed to operate at 5VDC.

Water Sensor [23]: This sensor can be used both as water level (up to 40mm) measuring sensor and as rain sensor for shallow waters. An analogue value can be read on the water sensor output pin of the conductive lines drawn in parallel with each other. Working Voltage is 5V. Current consumption is less than 20mA.

Air Sensor [24,25]: Two different sensors are used here. These are natural gas and methane gas measurement sensor and air quality measurement sensor. Natural gas and methane gas measurement sensor accurately measures Natural Gas, Methane Gas (CH4) concentration. The measurement range of the sensor is 300-10000 ppm. It can also measure smoke and alcohol with low sensitivity. The air quality measurement sensor accurately measures the concentration of sulfur, benzene, water vapor, smoke

and other harmful gases (NH3, NOx, Alcohol, CO2, etc.).The operating voltage on both sensors is 5V DC.The output voltages vary proportionally to the gas concentration in the air.Microprocessor compatible TTL outputs available.Sensors with a long operating life and stability have fast response times. A total of 25 sensor nodes were used in the smart home application. The distrubition of the sensors to the rooms are given in Table 1.

Table 1. The distrubition of the sensors to the rooms

Sensors with integrated sensor node	Room	Sensor Node id	TOTAL
Temperature-Humidity + Light sensor	Living room Bedroom Guest room Children's room Kitchen Bathroom Toilet	Sensor Node (SN) 1 SN 2, SN 3, SN 4, SN 5, SN 6, SN 7	There are one in every place in the home. Total = 7
Motion sensor	The windows and exterior doors in each room.	SN 8, SN 9, SN 10, SN 11, SN 12, SN 13, SN 14, SN 15	There are one in the doors and windows that are located in the home and open to the outside. Total = 8
Water sensor	Kitchen Bathroom Toilet	SN 16, SN 17, SN 18	There are places where there is water in the home Total = 3
Air sensor1 + Air sensor2	Living room Bedroom Guest room Children's room Kitchen Bathroom Toilet	SN 19, SN 20, SN 21, SN 22, SN 23, SN 24, SN 25	There are one in all the location to control the air of the home. Total = 7 Grand total = 25

4. PRIVACY PROTECTION

Sensor nodes, which are the raw materials of intelligent systems, are subject to many security hazards due to reasons such as constraints, wireless communication environment and so on. It is imperative that the perceived information is conveyed confidently while coming to the home gateway. Data privacy [26] guarantees that access to the collected data is prevented by unauthorized persons. Otherwise, information circulating within the network can be retrieved by an attacker and used in an abusive manner. For example, in a system that is looking directly at the relevant units for a malfunction that can occur at home, such as a fire-flood, these values can be injected into the network at a low rate and many security problems can occur. For these reasons, it is necessary to establish a secure communication channel for data transmission in smart home systems. The standard approach to keeping sensitive data secret is to encrypt the data with a secret key [27]. For data privacy, block encryption algorithms, which are generally symmetric encryption algorithms, are used due to the limited processor-memory-power denomination of the sensor nodes. In this study, the AES encryption algorithm which has international validity [28] was used. A secure end-to-end channel is provided for the home gateway and sensor nodes in the home.

In the AES algorithm, the length of the input block, the length of the output block, and the length of the status block are 128 bits. The block size is represented by 4. This reflects the number of 32-bit words on the block. However, the length of the encryption key is 128, 192 or 256 bits. Key lengths can be 4, 6, or 8, and this encryption reflects the number of 32-bit words in the key. The number of rounds to be made during the execution of the algorithm depends on the length of the key.This information about AES is given in Table 2.

Table 2. Information about AES

AES	Key Length	Block Size	Number of Round
128	4	4	10
192	6	4	12
256	8	4	14

In study, the data is encrypted as AES-128 bits. The overall structure of the AES in 128 bit ciphering is shown in Figure 7, the operations taking place in a round in AES are shown in Figure 8.

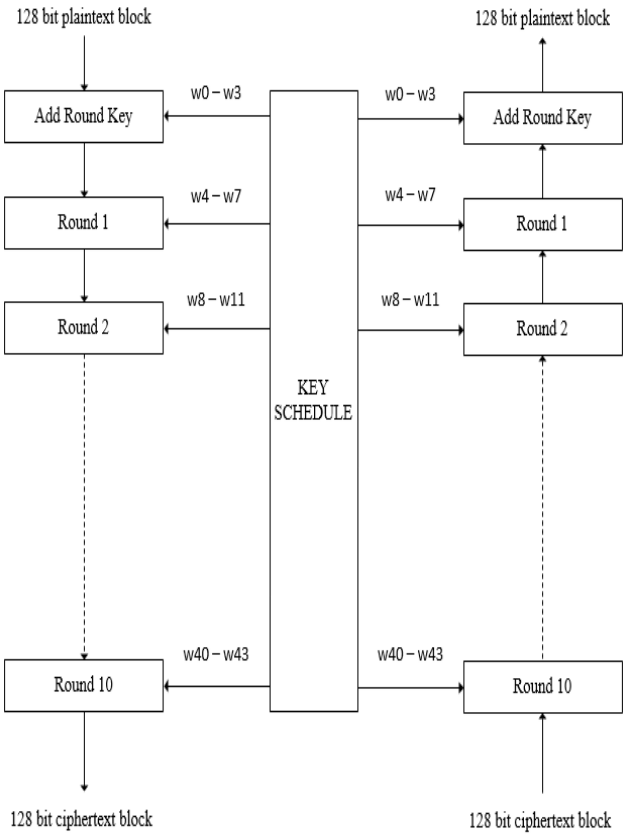


Figure 7. The overall structure of the AES in 128 bit ciphering

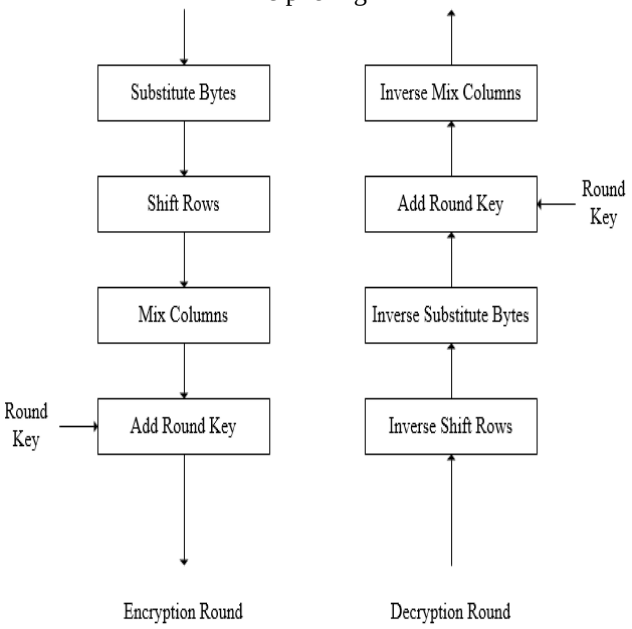


Figure 8. The operations taking place in a round in AES

For encryption and decryption operations; The AES crypto algorithm uses a round function consisting of 4 different conversion functions based on the replacement of byte sequences. The operations performed in Round function are as follows.SubBytes: Substitution of byte locations using substitution table. ShiftRows: Shifts the rows in the status table according to different offset values.MixColumns: Mixing the data in the columns in the status table. AddRoundKey: Addition of round keys.

AES algorithm; it takes the encryption key and implements the round key generation function to generate the key list that the 32-bit words that form the round keys with the sequential combination bring to the table. The Round Key Generation function generates a total block size (number of rounds + 1) words.

The conversion operations used in the encryption process are reversed and then used directly in the decryption process for the AES Algorithm. The conversion operations used in decryption can be listed as InvShiftRows, InvSybBytes, InvMixColumns, and AddRoundKey.
InvShiftRows: Reverse of the ShiftRows process.InvSubBytes: This is the opposite of changing the bytes in the status array according to the S-Box table. InvMixColumns: The inverse of the Mixcolumns transformation. This completes the inverse transformation process by performing a separate operation on each column in the status table. AddRounKey: XORing with the round key of the state sequence. Therefore, if the result array is processed again with the same round key, AddRounKey is applied in reverse order.

5. TESTING AND RESULTS

In this section, tests and results are presented with related to both the designed SIM900 GSM/GPRS node, smart home application and privacy protection.

General features of the SIM900 GSM/GPRS node are given in Table 3. The results given in Table 3 were obtained from the SIM900 GSM/GPRS datasheet [29]. In addition, tests were per- formed on the home gateway. This information was verified. The experimental results of the wisen sensor node [18] are already in their own paper.

The architecture of the study is given in Figure 9. As seen from the architect, the information obtained from the sensors located in the home is transmitted to the home gateway.

The information coming from the home gateway is stored in the database by connecting to the server via GPRS. The data stored in the database is the date attachment.In this way, historical data can be reached and statistics can be reported.With the web portal, users can see the information in the home after logging in with the user name and password. This information can be seen on both web and mobile platforms.In this way, people can realize the central management of their homes independently of time and place. If the threshold values set by the user are passed, the sms is transmitted directly to the user. However, a telephone number that the user specifies is called.In web portal, selection and analysis can be done according to sensor and room.

Table 3. General features of the SIM900 GSM/GPRS node

General features	
Quad-Band	850/ 900/ 1800/ 1900 MHz
GPRS multi-slot class	10/8
GPRS mobile station	class B
Compliant to GSM phase 2/2+	Class 4 (2 W @850/ 900 MHz)
	Class 1 (1 W @ 1800/1900MHz)
Supply voltage range	3.2 ... 4.8V
Low power consumption	1.0mA(sleep mode&BS-PAMFRMS=9)
Dimensions	24* 24 * 3 mm
Control via AT commands	(GSM 07.07 ,07.05 and SIMCOM enhanced AT Commands)
SAIC (Single Antenna Interference Cancellation) support	
Operation temperature	-40°C to +85 °C

Specifications for GPRS Data	
GPRS class 10	max. 85.6 kbps (downlink)
PBCCH support	
Coding schemes CS 1, 2, 3, 4	
PPP-stack	
Specifications for SMS via GSM/GPRS	
Point to point MO and MT	
SMS cell broadcast	
Text and PDU mode	
Specifications for Voice	
Tricodec	Half rate (HR)
	Full rate (FR)
	Enhanced Full rate (EFR)
AMR	Half rate (HR)
	Full rate (FR)
Hands-free operation（Echo suppression）	

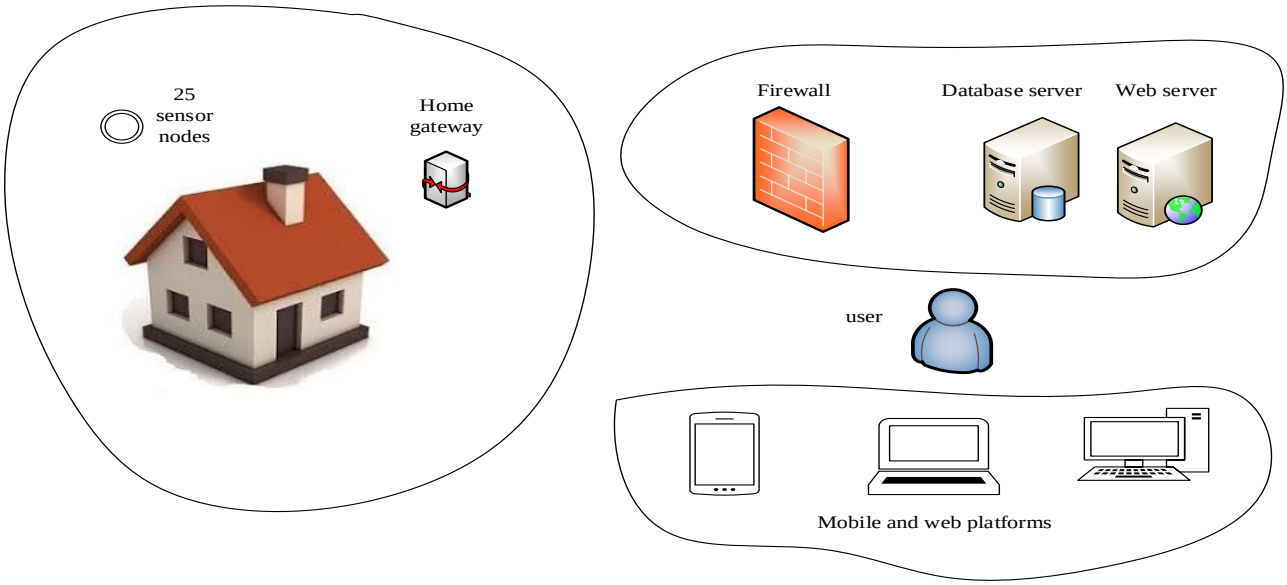


Figure 9. Smart home application architecture

The user can set the threshold value for each node. When the threshold values are reached, the user is informed via sms/call. However, as shown in Figure 10, there are screens that allow the user to receive information. In one of these, a room selection is made and the information of the sensors in the related room is shown to the user simultaneously. On the other screen, by selecting the type of sensor, the rooms in which these sensors are located are listed and values can be seen. Values other than the temperature are presented as low, normal, high, yes-no so that they are more easily to the user.

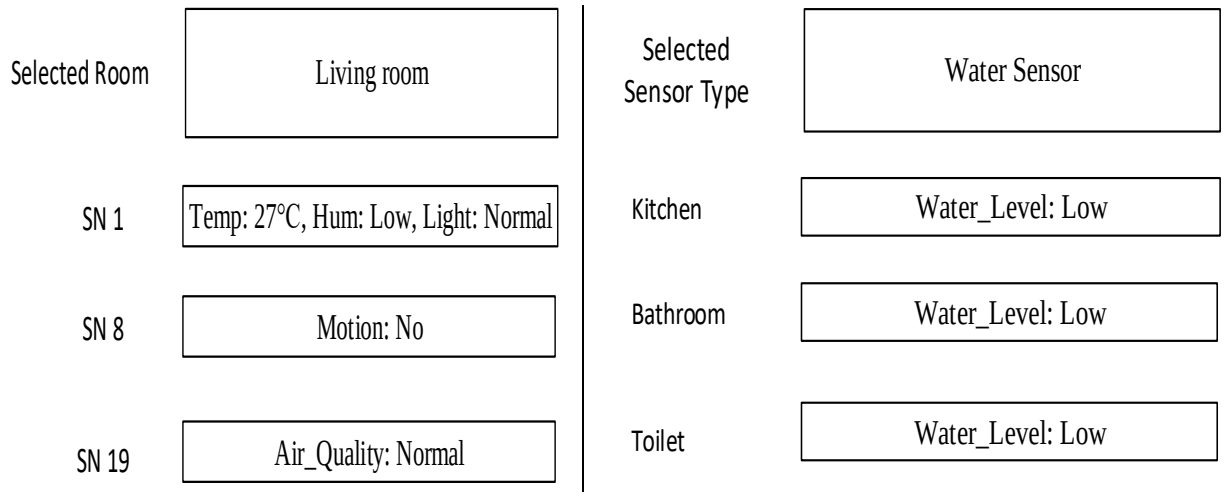


Figure 10.Screens for info

An end-to-end privacy protection is provided by the AES encryption algorithm, which is used for secure communication between home gateway and sensor nodes. Energy and delay criteria from the additional loads introduced by the AES have been addressed in several articles [30, 31, 32, 33, 34, 35]. As seen from the work done, the key setup, encryption and decryption execution times of AES are at micro level, and the energy consumption in these processes is at micro joule level. Home gateways used in smart systems are connected to a power. Other sensor nodes are battery powered. That's why there is no energy problem for the home gateway. Other sensor nodes, under normal conditions, take up to 2 years of energy. Because of this, due to high security requirements, delays and extra energy consumption can be neglected [36]. Because a loss in microjoule level for a node in the house will result in a loss of about 1-2% from node life. There is also a negligible increase in time. It will be seen that this delay is also negligible when it is considered that the alarms are already given at the threshold values.

6. CONCLUSIONS

Smart home technology is no longer a luxury, but a necessity. Although this is the case, these systems are still not common today. The reasons for this can be their cost, the lack of access to users, and the lack of user-friendly products. In the work done, a home gateway is proposed to overcome all these disadvantages. The recommended home gateway is the sensor node base we developed earlier. It can be used easily in smart systems. Both end nodes and gateways that people need are presented with this article. In addition, a smart home application was implemented with these nodes and the results presented. In the developed application, the temperature, humidity, light, motion, water level and air quality information can be obtained on the basis of the location in the home and the user is informed. Each sensor has an id and the threshold value is determined, and when these threshold values are exceeded, the user reaches emergency information by sms/call. Since the system is sensor-based, a threshold level can be established for each sensor node. With the advantages of the system, users can design their own smart systems with the help of the programming card which can be acquired easily and they can apply the applications they wish. Finally, the fact that the system is end-to-end encrypted is a huge plus. The developed system is modular, user friendly, and includes top security level. The system is totally usable on each place.

REFERENCES

[1] L. Hongri, "Design and Implementation of Smart Home System under the Framework of Android and ZigBee Technology", *Agro Food Industry Hi-Tech*, 28 (3), 244-248, 2017.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", *IEEE Communications Magazine*, 102-114, 2002.

[3] C.G. Garcia, D. Meana-Llorian, B. C. P. G-Bustelo, J. M. C. Lovelle, N. Garcia-Fernandez, "Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes", *Future Generation Computer Systems-The Internatıonal Journal of Escience*, 76, 301-313, 2017.

[4] A. Grguric, M. Mosmondor, D. Huljenic, "Development of Low Cost Energy Efficient Home Sensing Internet Gateway: A pilot study", **International Black Sea Conference on Communications and Networking**, IEEE, Varna, Bulgaria, 1-5, 6-9 June, 2016.

[5] K. C. Chen, Q. Wu, "The Design and Implementation of A Multi-homing Gateway in Wireless Sensor Networks", **3rd IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW),** IEEE, 83-84, 2016.

[6] Y. H. Shi, J. Z. Shen, L. Zhang, Q. Zhang, S. F. Lin, "Design of Security Gateway Based On Dual-Homed Architecture", **International Conference on Robots & Intelligent System (ICRIS)**, IEEE, 159-163, 2016.

[7] N. Vastardis, M. Kampouridis, K. Yang, "A user behaviour-driven smart-home gateway for energy management", *Journal of Ambient Intelligence and Smart Environments*, 8(6), 583-602, 2016.

[8] S. Y. Sun, J. G. Shi, J. S. Yu, "Design and Implementation of ZLL-DALI Gateway for Home Lighting", Electronics, Communications and Networks, *Lecture Notes in Electrical Engineering*, 382, 153-159, 2016.

[9] R. G. Garroppo, L. Gazzarrini, S. Giordano, M. Pagano, L. Tavanti, "A SIP-Based Home Gateway for Domotics Systems: From the Architecture to the Prototype", *Computer Networks, Communications in Computer and Information Science*, 608, 344-359, 2016.

[10] Z. H. Xu, "Design and Implementation of Intelligent Gateway for Smart Home**", Chinese Control and Decision Conference**, IEEE, 4713-4718, 2016.

[11] F. Ding, A. G. Song, E. Tong, J. Q. Li, "A Smart Gateway Architecture for Improving Efficiency of Home Network Applications", *Journal of Sensors*, 2016.

[12] R. Bolla, M. Chiappero, R. Khan, M. Repetto, "Saving Energy by Delegating Network Activity to Home Gateways", *IEEE Transactions on Consumer Electronics*, 61(4), 445-453, 2015.

[13] H. S. Kim, J. S. Seo, J. Seo, "Performance Evaluation of a Smart CoAP Gateway for Remote Home Safety Services", *KSII Transactions on Internet and Information Systems*, 9(8), 3079-3089, 2015.

[14] O. Galinina, K. Mikhaylov, S. Andreev, A. Turlikov, Y. Koucheryavy, "Smart home gateway system over Bluetooth low energy with wireless energy transfer capability", *Eurasip Journal on Wireless Communications and Networking*, 2015.

[15] P. C. Lin, "Optimal Smart Gateway Deployment for the Internet of Things in Smart Home Environments", **IEEE 4th Global Conference on Consumer Electronics GCCE**, 273-274, 2015.

[16] S. M. Kim, H. S. Choi, W. S. Rhee, "IoT Home Gateway for Auto-Configuration and Management of MQTT Devices", **IEEE Conference on Wireless Sensors ICWiSe**, 12-17, 2015.

[17] G. W. Wang, D. F. Pang, S. L. Lu, R. R. Wu, "The Design of Smart Home Gateway Based On KNX Bus", *Advances in Intelligent Systems Research*, 117, 1225-2558, 2015.

[18] M. Dener, "WiSeN: A New Sensor Node for Smart Applications with Wireless Sensor Networks", *ELSEVIER Computers and Electrical Engineering*, 64, 380–394, 2017.

[19] Internet: LaunchPad Value Line Development kit, MSP430, http://www.ti.com/tool/MSP-EXP430G2, 2017.

[20] Internet: SHT11 sensor, https://www.robotistan.com/sht11-isi-ve-nem-sensoru-karti, 2018.

[21] Internet: Motion sensor, https://www.robotistan.com/hc-sr501-ayarlanabilir-ir-hareket-algilama-sensoru-pir, 2018.

[22] Internet: Color sensor, https://shop.controleverything.com/products/tcs3414-16-bit-digital-color-sensor-with-programmable-analog-gain, 2018.

[23] Internet: Water level sensor, https://www.robotistan.com/su-seviyesi-yagmur-sensoru-water-level-rain-sensor, 2017.

[24] Internet: Natural gas and methane gas measurement sensor, https://www.direnc.net/mq-4-dogal-gaz-ve-metan-gazi-olcumleme-sensoru, 2018.

[25] Internet: Air Quality Measurement Sensor, https://www.direnc.net/mq-135-hava-kalitesi-olcum-modulu-air-quality-module, 2018.

[26] M. Dener, Ö. F. Bay, "TeenySec: a new data link layer security protocol for WSNs", *Security and Communication Networks*, 9(18), 5882-5891, 2017.

[27] M. Dener, "Security Analysis in Wireless Sensor Networks", *International Journal of Distrubuted Sensor Networks***,** 2014, 9, Article ID: 303501, 2014.

[28] J. Daemen, V. Rijmen, **The Design of Rijndael: AES - The Advanced Encryption Standard**, Springer-Verlag, 2002.

[29] Internet: SIM900 GSM/GPRS Module, http://www.propox.com/download/ docs/SIM900.pdf, 2018.

[30] F. Zhang, R. Dojen, T. Coffey, "Comparative performance and energy consumption analysis of different AES implementations on a Wireless Sensor Network Node", *International Journal of Sensor Networks*, 10 (4), 192-201, 2011.

[31] M. Panda, "Performance Analysis of Encryption Algorithms for Security", **International conference on Signal Processing, Communication, Power and Embedded System**, IEEE, 278-284, 2016.

[32] M. Abirami, S. Chellaganeshavalli, "Performance Analysis of AES and Blowfish Encryption Algorithm", *International Journal of Innovative Research in Science Engineering and Technology*, 2(11), 7052-7059, 2013.

[33] A. Odeh, S. R. Masadeh, A. Azzazi, "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (Sws)", *International Journal of Network Security & Its Applications (IJNSA)*, 7(3), 31-38, 2015.

[34] A. Verma, S. Kaur, B. Chhabra, "Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish", *International Research Journal of Engineering and Technology*, 3(10), 660-674, 2016.

[35 S. D. Rihan, A. Khalid, S. E. F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES", *International Journal of Engineering Research & Technology*, 4(12), 151-154, 2015.

[36] M. Dener, Ö. F. Bay, "Medium Access Control Protocolsfor Wireless Sensor Networks: Literature Survey", *G.U. Journal of Science*, 25(2), 455-564, 2012.