Journal of Theoretical and Applied Information Technology
20th July 2015. Vol.77. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RF MODULE BASED WIRELESS SECURED HOME AUTOMATION SYSTEM USING FPGA

[1]B MURALI KRISHNA, [2]J SRI VARSHINI [3]A NARAYANA MURTHY, [3]N ANIL SANTOSH, [3]G SAI PAVAN KUMAR, [3]B SAI VENKATESWARA RAO

[1]Asst. Professor, Department of ECE, K L University
[2]Student, M.Tech VLSI, Department of ECE, K L University
[3]Student, B.Tech, Department of ECE, K L University
E-mail: [1]muralikrishna@kluniversity.in, [2]varshinijs@gmail.com , [3]anm13991@gmail.com

ABSTRACT

Smart wireless home automation and security technique is one of the emerging technologies for intelligent building surveillance. Wireless technologies like Bluetooth and Wi-Fi have been used in contemporary home security systems using low cost, low power, less complexity RF module. It uses multi-hop communication for data transfer. This multi-hop technique gives out an unlimited range of communication thus giving it an edge over the other wireless technologies. Here the radio frequency transmission system employs ASK technique with transmitter and receiver operating at 433MHz. due to high frequency, we can transmit data to a sufficient distance without attenuation. FPGA modules are highly suitable and compatible for the evolving technology of software defined radios (SDR) due to their configurability, programmability and security. This project arises when we want the data communication to be protected from corruption and unauthorized access. The security to the data can be provided by using certain Encryption techniques. If one of the stations is stationary, then we can use this application as of automation. Finally our aim is to transmit certain data wirelessly with high security and also to control output load from any remote place. Hence, to make this practically work we need a compact Transmitter and receiver modules which can operate at 433MHz.

Keywords: *RF Module, FPGA, Secured Home Automation, Wireless Technology, Multi-Hop Communication, ASK Technique, Encryption.*

1. INTRODUCTION

Security [1] is given utmost importance in present day situation. The need for security has been rapidly increasing from the past few decades. The industrial revolution that took place in the 1900's has made path for the evolution of security systems. Every individual does not like others to see his/her data so they commonly use encryption while sending the data and the receiver has to decrypt the data to retrieve the initial data. Thus the data will be protected in every way by following the encryption and decryption standard formats. With the development of algorithms, the security systems have become more sophisticated and easy to secure the data. There are many types of algorithms but in this paper we are mainly focusing on the SDES algorithm.

The process of encrypting data to make it unauthorized for the access of individuals is called as cryptography. It also includes decryption. It involves two basic operations namely encryption and key management. By using cryptographic algorithm with various keys, we can encrypt data. The amount of security provided by the encrypted data depends on the number of keys used in the algorithm. They should be kept secret from the other individuals as the data can be hacked only with the help of the keys. These keys area always kept secured from the hacker and are known as secret key. Key plays an important role in encryption process, which is a main part of cryptography. If the key is manipulated or corrupted then the data will not be recovered. So the transportation of key should be highly secure. The frequency of use of a cryptographic key always has a direct link to how often the key should be changed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In present day scenario almost all the electronic funds are being carried out online. So to protect the same and maintain the privacy of the users, for better security, either the number of keys used or the existing key length is increased. So in the above two cases to reduce the overheads, the sub-keys are used. Sub-keys are used only for the nodes which are often attacked by the hacker. The sub keys are always derived from the main key which helps in reducing the overheads.

The Xilinx FPGA is used for implementation of simplified DES algorithms. The Xilinx ISE 14.5 tool is used for developing Synthesizing SDES Algorithm. A FPGA is a reprogrammable logic device used as a reprogrammable alternative to ASIC Chip devices. FPGAs can be used as controller and its behavior depends on the complexity of the I/P data. Verilog HDL is used to develop Algorithm and Simulation using ISE Simulator. In this paper FPGA to provide security for the data at the end sources using Encryption and Decryption.

Here the frequency range used by us is 434 MHz, so we are considering RF-Module. The RF-Module consists of a transmitter and receiver. The frequency range of a RF-Module is 433 MHz The RF-transmitter transmits an encrypted data. The data transmitted will be received by the RF-receiver and it is decrypted with the help of FPGA.

2. FPGA

An FPGA is a device that contains a matrix of reconfigurable gate array logic electronic equipment. Once a FPGA is organized, the inner electronic equipment is connected in a very means that makes a hardware implementation of the software package application. In contrast to processors, FPGA [2] use dedicated hardware for process logic associate degreed doesn't have software. FPGAs are actually parallel in nature therefore totally different process operations don't need to contend for identical resources. As a result, the performance of 1 a part of appliance isn't affected once further process is additional. Also, multiple management loops will run on one FPGA device at totally different rates. FPGA –based management systems will enforce essential interlock logic and may be designed to forestall I/O forcing by associate degree operator. However, in contrast to hard-wired computer circuit board PCB styles that have fastened hardware resources, FPGA-based systems will virtually wire their internal electronic equipment to permit reconfiguration when the system is deployed to the sphere. FPGA [3] devices deliver the performance and responsibility of dedicated hardware electronic equipment. A single FPGA will replace thousands of separate parts by incorporating legion logic gates in a very single computer circuit (IC) chip. The inner resources of associate degree FPGA [4] chip include a matrix of configurable logic blocks. Signals are routes among the FPGA matrix by programmable interconnect switches and wire routes

FPGAs contain programmable logic parts a referred to as "logic blocks", and a hierarchy of reconfigurable interconnects that permit the blocks to be "wired together"—somewhat like several (changeable) logic gates which will be inter wired in (many) totally different configurations. Logic blocks will be organized to perform advanced combinatory functions, or just easy logic gates like AND/XOR. In most FPGAs, the logic blocks conjointly embody memory components, which can easy flip-flops or additional complete blocks as memory

3. RF MODULE

Transmitter: A simple RF transmitter consists of a 433 MHz license exempt transmitter module and an encoder IC. It is designed in such that, one can operate any appliance remotely staying within the range. A general RF transmitter has a range of about 400m according to the manufacture. This module consists of four pins. Apart from "data" and "Vcc" pin, it has a common ground (GND) for data and supply. Last is the RF output pin (ANT). For the transmission of a unique signal, encoder is crucial. For this, here we are using renowned encoder IC HT12E. It is capable of encoding information which consists of "N" address bits and "12N" data bits. Each address/data bit can be set to one of the logic states.

Journal of Theoretical and Applied Information Technology
20th July 2015. Vol.77. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig.1: RF transmitter module

Receiver: the above circuit represents the receiver section. This circuit picks up the transmitting signals at the frequency of 434MHz receiver module. This integrated RF module [5] has turned to a frequency of 433.92MHz, approximately same as transmitter. Here, on-off keyed modulation is done by receiver then demodulates it for next decoder stage. This receiver module is based on single conversion super-heterodyne receiver. Here to perform this, we use IC HT12D. It is capable of decoding the information received from the transmitter.

Fig.2: RF receiver module

Types of RF Modules used:

1. 4-BIT Module
2. 8-BIT Module

In this paper we used the above modules for the transmission/reception purpose. Here the RF module [6] is interfaced with FPGA for a secured transmission. HT12E and HT12D ICs are series of CMOS LSIs for remote control system applications. These ICs are paired with each other for the proper operation. The decoder receives the serial data and address from its corresponding decoder, transmitted by carrier using RF transmission medium and hence gives out the output.

4. CRYPTOGRAPHY

Encryption-Decryption techniques are used to avoid an unsecured access of the data. It helps to provide security, accuracy and also confidentiality. The following four kinds of people have contributed their efforts in this technique:

i. Military
ii. Communication system
iii. Diplomatic corps
iv. Diarists

We can provide security to the data or plain text by applying the algorithms to them using various keys. Security of the cryptography system not only depends upon the algorithm but also keys used for encryption. Cryptography [7] is mainly used to provide privacy for the users. For better security purposes we can increase the key length or can use more number of keys.

Types of Cryptography:

The process of changing data into encrypted data is called Encryption. This encryption[8] can be done in various techniques:

i. Data Encryption Standard
ii. Triple Data Encryption Standard
iii. International Data Encryption Algorithm
iv. Blowfish Algorithm
v. Pretty Good Privacy (PGP)
vi. Public Key Infrastructure
vii. Simplified Data Encryption Standard

In this paper we propose S-DES algorithm implementation using 8-bit RF module interfaced with FPGA.

S-DES Overview:

Journal of Theoretical and Applied Information Technology
20th July 2015. Vol.77. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The S-DES [9] consists of 8-bit plain text and 10-bit key as input; it gives out the output as 8-bit cipher text. This algorithm consists of five functions like Initial Permutation (IP), Complex Labeled function (fK), which depends on 10-bit key and requires permutation and substitution operations, function that switches the two equal halves of the data, and again the function fK, finally inverse of initial permutation (IP-1) as shown in below fig.1. By this the encryption process is done. In this we use main key and sub key.

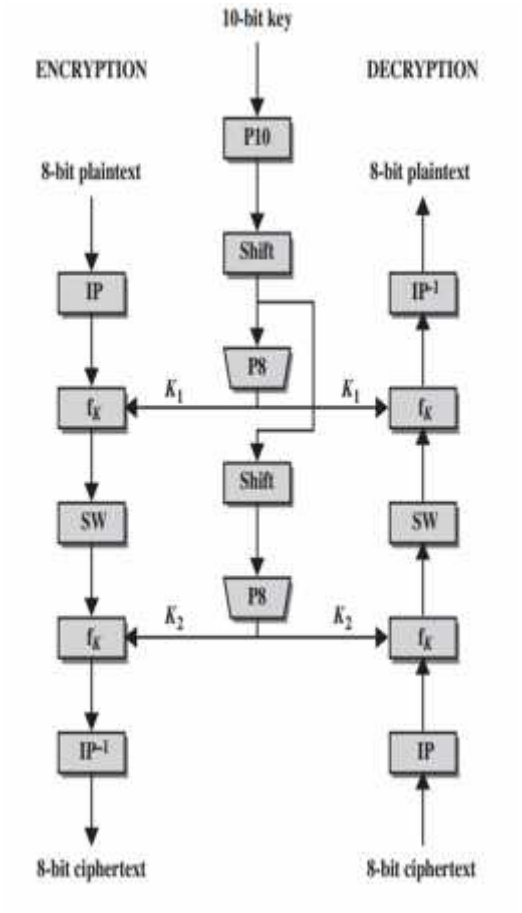

Fig.3: Simplified DES algorithm.

5. SYSTEM IMPLEMENTATION

Encryption: S-DES algorithm is applied to produce cipher text. This cipher text will be transmitted using FPGA interfaced RF module. Flow chart of the encryption is explained as fallows, initially plain text will be taken and it will be 8 bit, initial permutation includes mixing of all bits. Next step of the encryption process (fig.2) is function fK which consists of substitutions and permutation. Let L and R be the leftmost 4 bits and rightmost bits of input plain text. This plain text first four bits are fed into the s-box s0to produce a 2bit output, and remaining 4 bits are fed into s1 to produce another output. Switch function is the next step in which interchanging of left and right 4bits will occur so that second instance of fK will operates on another 4 bits, finally inverse of initial permutation will be done.

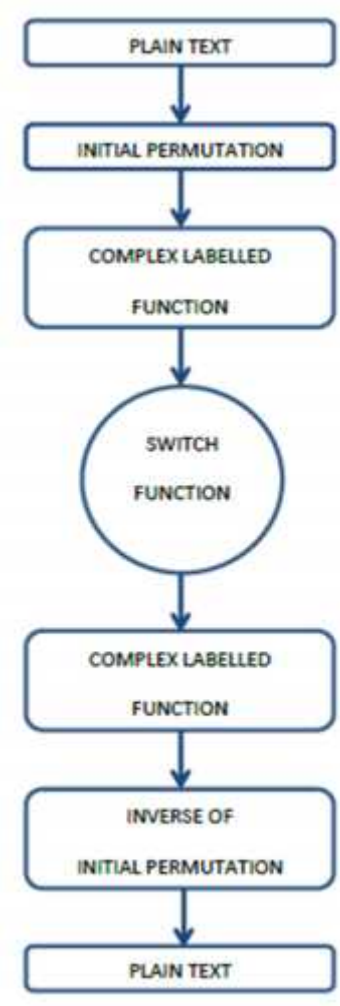

Fig.4: Encryption flowchart.

Decryption: Cipher text output which is out by encryption sample, which is an input for decryption process. We have to produce the plain

Journal of Theoretical and Applied Information Technology
20th July 2015. Vol.77. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

text after the completion of the decryption process. Main difference between the encryption and decryption process (fig.3), in the encryption XOR is first applied with key-1 and then with key-2, here in decryption the XOR will be the vice versa. The result will be the original data after the decryption.

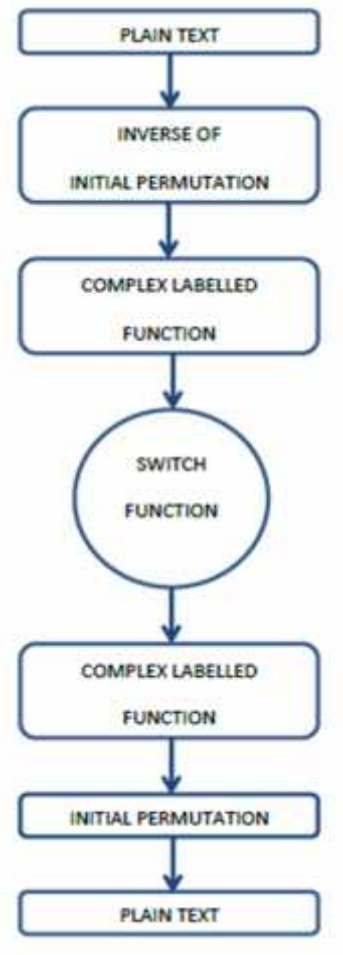

Fig.5: Decryption flowchart.

Block diagram:

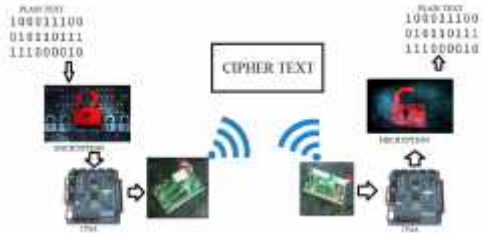

Fig.6: Block diagram

RF Module based wireless secured home Automation system [10] is developed using Spartan-3E FPGA for Encryption and Decryption. RF 8Bit Module is used for Wireless Communication between FPGA's for Transmission and Reception of Cipher Text. Two Different RF Transmitter Modules transmit cipher text data to the receiver as shown in above fig.4. Receiver RF Module receives Cipher Text data and transfers to FPGA [11]. The Decryption SDES Algorithm is configured to FPGA receives Cipher Text as input and decrypts the Plain Text. Home Appliances will on through Relays when cipher text is securely decrypted (fig.5).

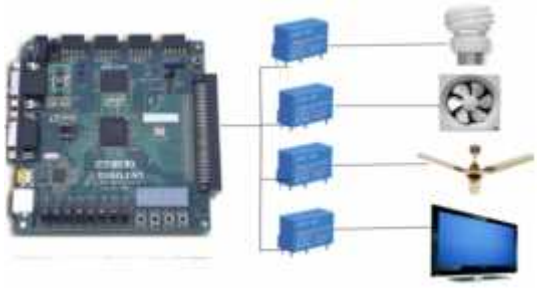

Fig.7: Controlling of appliances Through Relays

6. SIMULATION RESULTS

Encryption results:

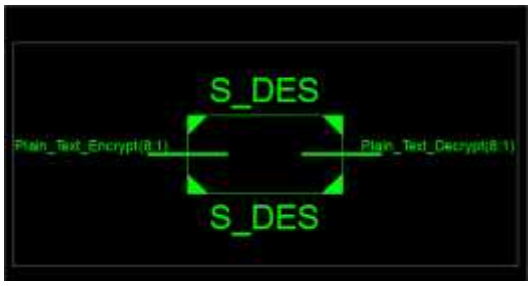

Fig.8: Encryption schematic view

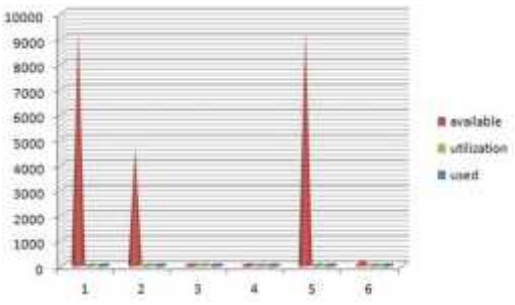

Fig.9: Device Utilization Summary

Journal of Theoretical and Applied Information Technology
20th July 2015. Vol.77. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

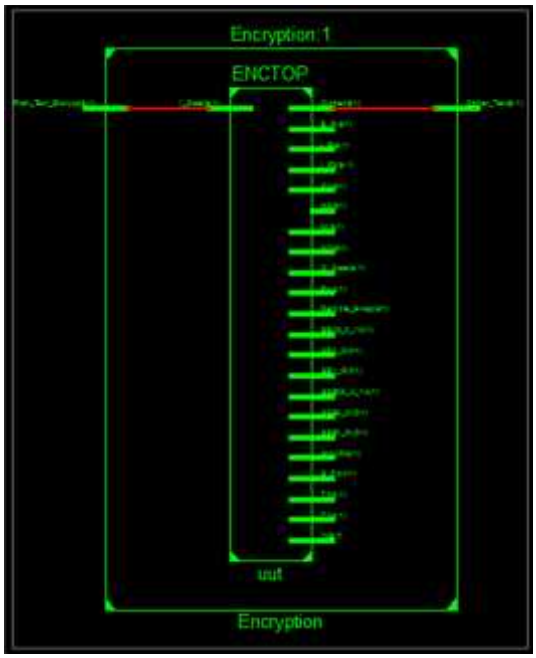

Fig.10: Encryption rtl schematic view

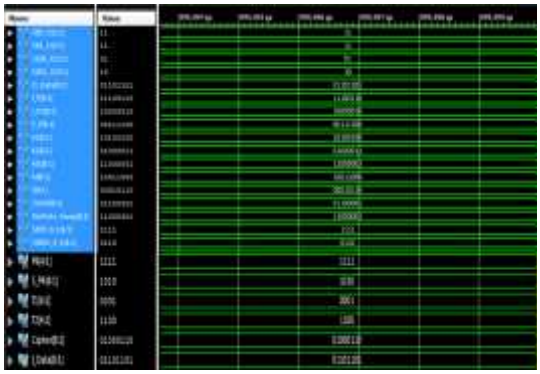

Fig.11: Encryption simulation

Decryption results:

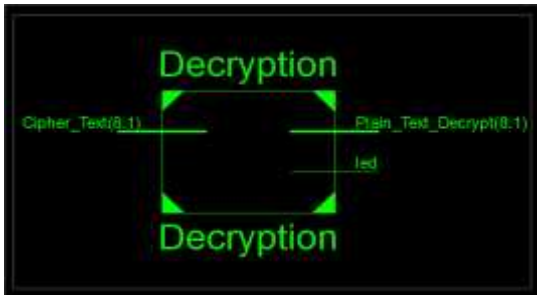

Fig.12: Decryption schematic view

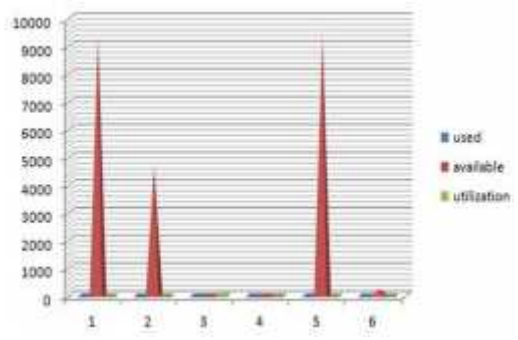

Fig.13: device utilization summary

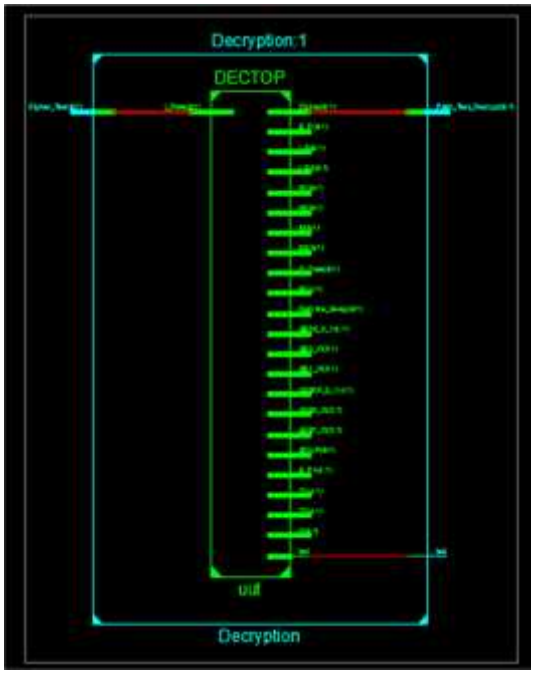

Fig.14: Decryption rtl schematic view

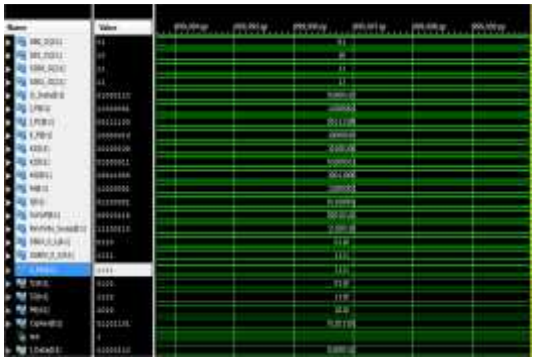

Fig.15: Decryption simulation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7. CONCLUSION

Comparison of existing wireless technologies for home automation and security we proposed based on low cost, low power consumption. RF Module based wireless secured home Automation system developed using Spartan-3E FPGA for Encryption and Decryption. RF 8Bit Module is used for Wireless Communication between FPGA's for 8-Bit Transmission and Reception of Cipher Text. Multiple Home Appliances will on through Relays when cipher text is securely decrypted. Depending on length of Input Data user can encrypt using 4, 8, 16, 32, 64, 256, 512 Bit with Serial RF and Zigbee Modules. Hence implemented the complete experimental work in real time and with the above proposed architecture. Thus combining all the above used techniques and components, obtained these features to the like flexibility, reliability, safety, limited delay, low power consumption, low cost and with high efficiency.

8. REFERENCES

[1].Alkar, Ali Ziya, and Umit Buhur. "An Internet based wireless home automation system for multifunctional devices." *Consumer Electronics, IEEE Transactions on* 51.4 (2005): 1169-1174.

[2].Wu, Jing-jie, and Rui Huang. "A FPGA-based wireless security system."*Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*. IEEE, 2011.

[3].Nichols, Randall K., and Panos C. Lekkas. *Wireless security*. New York: McGraw-Hill, 2002.

[4].Fallside, Hamish T., and Michael JS Smith. "FPGA-based communications access point and system for reconfiguration." U.S. Patent No. 6,326,806. 4 Dec. 2001.

[5].Hsu, George. "Modular RF communication module for automated home and vehicle systems." U.S. Patent No. 6,374,079. 16 Apr. 2002.

[6].Zamora-Izquierdo, Miguel A., José Santa, and Antonio F. Gómez-Skarmeta. "An integral and networked home automation solution for indoor ambient intelligence." *Pervasive Computing, IEEE* 9.4 (2010): 66-77.

[7].William, Stallings, and William Stallings. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.

[8].Van Oorschot, Paul C. "Public key cryptography based security system to facilitate secure roaming of users." U.S. Patent No. 6,317,829. 13 Nov. 2001.

[9].Redman, Scott, Dennis Mak, and Richard Terrill. "Access restriction to circuit designs." U.S. Patent No. 5,978,476. 2 Nov. 1999.

[10]. Hou, Jun, et al. "Research of intelligent home security surveillance system based on ZigBee." *Intelligent Information Technology Application Workshops, 2008. IITAW'08. International Symposium on*. IEEE, 2008.

[11].Ahmad, Arbab Waheed, et al. "Implementation of ZigBee-GSM based home security monitoring and remote control system." *Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on*. IEEE, 2011.