A WIFI-BASED SMART SECURITY SYSTEM

Peter Obinna Mbamaluikem & Joel Ogunyemi
Department of Electrical/Electronics Engineering, The Federal Polytechnic Ilaro
Peter.mbamaluikem@federalpolyilaro.edu.ng, joel.ogunyemi@federalpolyilaro.edu.ng

Abstract

Over the past few decades, smart security systems have become increasingly popular, enhancing poise and quality of life. A smart security system was created as a result of this investigation. The device makes use of a motion sensor that can identify fluctuations in warm-blooded moving objects within its detecting range. The infrared radiation changes produced voltages that were sent to the microcontroller. The microcontroller decodes the signal on when an intruder approaches the PIR sensor's detecting zone before using it to turn on the webcam and the relay-controlled lighting system. The webcam and light turn off as soon as the intruding party escapes the sensor's detection range. A secure digital Card was used to save images taken by the Microcontroller after they were programmed to do so. A smart phone can be used for monitoring without an internet connection because the devices are covered by the router network. The results of the testing demonstrate that the system works perfectly, with an average lag time between an invasion and its presentation on the monitoring equipment of less than 1 µs. The implemented smart security system's successful performance evaluation confirms and indicates the system's potential for quick commercial market adaptation.

Keywords: Smart security, webcam, microcontroller, PIR sensor, Wi-Fi

Introduction

One of the essential factors in protecting society from unfavorable events or accidents is security. Security is given such high priority since modern civilization is characterized by various forms of turmoil, including robbery attacks, political unrest, terrorism, armed infiltration, and the like. Due to all of this, security systems have developed quickly. Researchers have developed a wide range of security solutions that are used in homes, businesses, and remote locations to combat this dreadful threat. A smart security system is a combination of hardware and software that has been strategically set up to offer protection from infiltration in the location where it has been put. The proliferation of wireless technologies, which impacts the use of smartphones to remotely manage and monitor household appliances and the environment, has led to a variety of innovations in security systems.

A smart security system can be designed to monitor a number of locations and devices, including buildings, offices, shopping centers, and power lines (Felix & Raglend, 2011). From a variety of devices, including smartphones, tablets, desktops, and laptops, the smart security system may be simply controlled and managed (Ramlee, et al, 2013). This lowers the amount of manual work required to provide services (Ransing & Rajput, 2015; Jamil & Ahmad, 2015). Various wireless communication methods, including Bluetooth (Ullah & Celik, 2016), GSM (Chinchansure & Kulkarni, 2014), ZigBee (Han, et al., 2014), Wi-Fi (Vivek & Sunil, 2015) and EnOcean are used by a number of smart security systems to interact with microcontrollers (Courreges, et al., 2016).

In this study, a passive infrared (PIR) sensor that interfaces with a camera and microcontroller was used to develop a low-cost smart home security system. As soon as an intruder enters the range of the sensor, this system can recognize them and provide an output that activates the lighting system and webcam for real-time recording.

2 Literature Review

Wi-Fi Technology

The preferred communication protocol for multimedia applications in homes is Wi-Fi technology. It is used to allow access to the home automation system from Wi-Fi enabled devices. This decision was made since Wi-Fi networks and Wi-Fi compatible gadgets like smartphones, tablets, laptops, etc. are becoming more common in homes. Furthermore, Wi-Fi's high data rate characteristic provides for more freedom in interface design (Vivek & Sunil, 2015). Wi-Fi uses radio frequency to provide wireless networking and implements the IEEE 802.11 standard. There are several variations of this protocol, but IEEE 802.11g -which uses the unlicensed 2.4 GHz band and offers a top

raw data throughput of 54 Mbps is the most widely used one today. The Wi-Fi usage has a number of benefits over competing technologies including Bluetooth, ZigBee, and EnOcean. A typical Wireless (802.11b and 802.11g) ADSL Modem Router with a 4-port switch was used to construct the Wi-Fi network. Two main purposes are served by the modem. First, the modem establishes the link between the local Wi-Fi network and the internet, granting access to the Area network home gateway from any place with an internet connection. Second, the access point is instantly accessible by any nearby WiFi-enabled device that is inside the Wi-Fi network's coverage area (Muhammad & Ahsan, 2016). With Wi-Fi devices currently in use, this offers a low-cost communication option with the home network and lower infrastructure expenses. Additionally, homeowners can use well-known technologies and gadgets to monitor and manage the home automation network.

Related Literature

Home security systems have transitioned from conventional monitoring systems to high-tech devices like surveillance cameras, monitored and unmonitored intruder alarm systems, motion detectors, and automatic fire systems as the internet of things (IoT) develops (Zamshed, et al., 2011). A microcontroller-based automated home security system was created and deployed in the work of (Nikhil & Subramanya, 2013). The security system designed by (Kamoru, et al., 2018) uses motion sensors to detect intruders. Through the use of a single home gateway, a ZigBee-based home automation system and Wi-Fi integrated was designed by (Khusvinder, et al., 2009). The article discusses the causes behind the delayed uptake of home automation and assesses ZigBee's potential to solve these issues. Similar study was done by using the GSM cellular communication network to control a remote system by (Alheraish, 2004).
Similarly, (Deepali, et al., 2013) used Android ADK to create a home automation and security system. In the research of (Chandramohan, et al., 2017), a low-cost, adaptable, and internet protocol (IP)-connected house control and monitoring system was built and put into practice. The key parts of the paper's autonomous control and monitoring system are a temperature sensor (LM35) and a light dependent resistor (LDR).

3 Methodology

Proposed Work

The proposed Wi-Fi-based smart security system (WBSSS) aims to detect and display the presence of an intruder via the webcam in a location where it was installed. In this study an ESP32-CAM microcontroller is used to create a smart security controller system. The ESP32-CAM microcontroller's board is a low-cost, low-power system on chip microcontroller with built-in Wi-Fi and dual-mode Bluetooth. With the built-in antenna switches, RF baluns, power amplifiers, low-noise receiver amplifiers, filters, and power-management modules, the ESP32 series of microprocessors uses either a Tensilica Xtensa LX6 microprocessor in dual-core and single-core variations, an Xtensa LX7 microprocessor in dual-core or single-core variations, or a single-core RISC-V microprocessor. The ESP32-CAM microcontroller board, PIR sensors, battery, and LED make up the project's major parts. The sensor recognizes when a human pass and the signals generated are sent to the microcontroller, which activates the light and prompts the camera to record a movie and snap numerous pictures before saving them to the secure digital card (SD card). The planned WBSSS block diagram is shown in Figure 1.

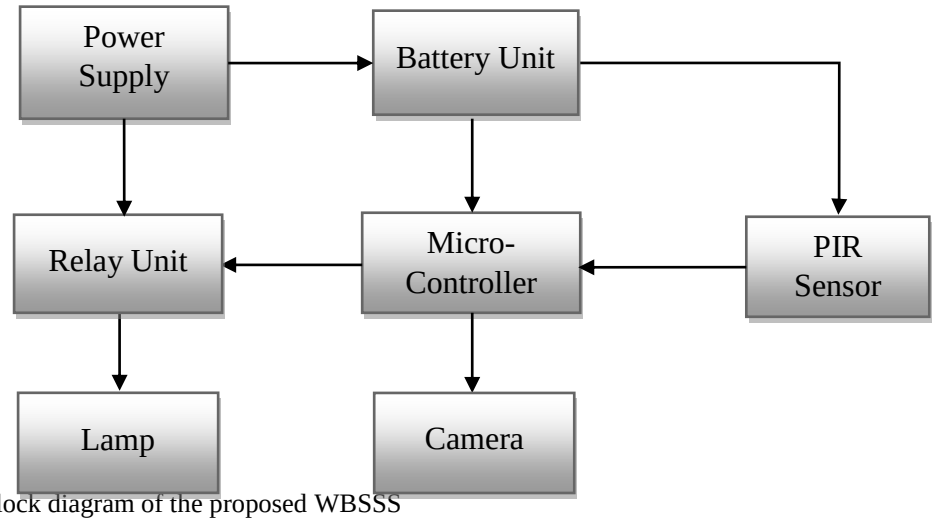

Figure 1: Block diagram of the proposed WBSSS

Design Analysis

For the purpose of monitoring an intruder in an environment, the WBSSS is designed and implemented. A PIR sensor, ESP32-CAM microcontroller board, Light Emitting Diode (LED), 5 V power supply, and Relay were utilized to show the viability and efficacy of the suggested system. A Wi-Fi network is set up to handle the high data rate requirements of such multimedia transmission. A typical Wireless (802.11b and 802.11g) ADSL Modem Router with a 4-port switch was used to construct the Wi-Fi network. Two main purposes are served by the modem. First, the modem establishes the link between the local Wi-Fi network and the Internet, granting access to the Wi-Fi-enabled home gateway from any place with an Internet connection. Secondly, locally WiFi-enabled device that is inside the home's Wi-Fi network's coverage area can instantly be accessible by any nearby WiFi-enabled device. To allow communication between various networks, a home gateway was created. Users can access home networks both locally and remotely via the home gateway's unified interface. With Wi-Fi devices currently in use, this offers a low-cost communication option with the home network and low infrastructure expenses.

For this system, two task apps were made. The first application made takes on the security camera's fundamental functions, which involve taking photos when motion is detected and saving those photos to an SD card placed into the ESP32-CAM. The second involves watching the video on a web browser by turning on the hotspot on the user's phone, entering the hotspot name and password, and the IP address that the hotspot has assigned to the device.

System Implementation

The WBSSS was primarily implemented using surface mounted components on the printed circuit boards that were used. A 30 W soldering iron was used to solder the components into the appropriate component slots. The emitter of the transistor is connected to the ground of the PIR motion sensor, and its base was connected to the output pin and 1 kΩ. The regulator IC is attached to the PIR sensor's positive pin. After the breadboard is wired to the power source, a delay of 2 to 5 seconds is allowed for the PIR sensor to stabilize. The structure was contained in a PVC box that measured 4 by 4 by 2 millimeters. Figure 2 and Figure 3 depict the system's pictorial diagram and the implemented system respectively.

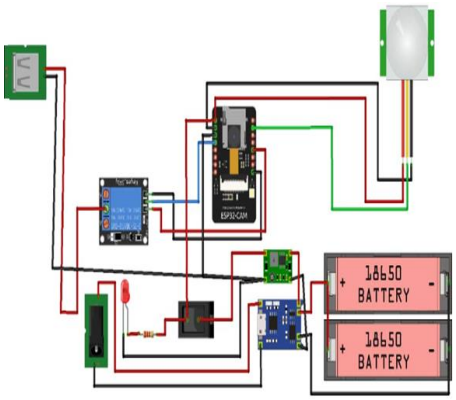

Figure 2: Pictorial diagram of WBSSS

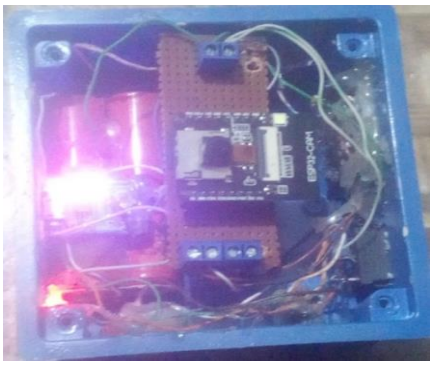

Figure 3: The constructed WBSSS

Result and Discussion

The viability of the implemented system was assessed on both a quantitative and qualitative level. Human subjects were made to severely cross the sensor's detection range to mimic a high degree of daily use in order to show the viability and efficacy of the proposed system. The results of the tests conducted are shown in Table 1 and Figure 4.

Table 1: Maximum sensitivity data of system

Detecting Distance (m)	Switch & Relay	LED indication	Lamp
2	ON	ON	ON
4	ON	ON	ON
6	ON	ON	ON
8	ON	ON	ON
10	ON	OFF	OFF

Figure 4: A real-time test conducted in an office

According to Table 1, the "ON" signifies that the device is still within Wi-Fi coverage while the "OFF" shows that it is outside of it. The result in Table 1 makes it clear that the Wi-Fi network's maximum wavelength of coverage is around 9 meters. Figure 4 also demonstrates a real-time capture carried out with the developed system when a human enters the sensor's detecting range. The graphic user interface used by the end user was used to create the interface in Figure 4. The developed system can be used to monitor an environment from a mobile phone using a Wi-Fi network as a tool without the need for a physical internet connection, as shown by the qualitative analysis of Figure 4. With an average lag of 1 µs between an invasion and its display on the monitoring device, the testing showed that the system works flawlessly.

Conclusion

This paper implemented a Wi-Fi based smart security system that uses an ESP32-CAM Microcontroller to monitor an area. Despite certain time lags when recording the video, it was found that the suggested approach can conserve recording system memory as it begins recording as soon as the camera is turned ON. Additionally, since the lighting system only turns on when the PIR sensor is triggered, the power consumption is highly reduced. The installed home gateway enables compatibility between the system's interface and all of the networks and devices that are used to access it. Through experimentation and user trials, the viability and suitability of the developed security system has been successfully assessed. The successful performance evaluation supports and demonstrates the potential of the proposed system to be easily adaptable for commercial purposes.

Reference s

Alheraish, A. (2004). Design and Implementation of Home Automation System. *IEEE Transactions on Consumer Electronics, 50* (4), 1087-1092.

Chandramohan, J., Nagarajan, R., Satheeshkumar, K., Ajithkumar, N., Gopinath, P. A., & Ranjithkumar, S. (2017). Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi. *International Journal of Engineering and Computer Science, 6* (3), 20694-20698.

Chinchansure, P. S., & Kulkarni, C. V. (2014). Home Automation System based on FPGA and GSM. *2014 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore.

Courreges, S., Oudji, S., Meghdadi, V., Brauers, C., & Kays, R. (2016). Performance and interoperability evaluation of radiofrequency home automation protocols and Bluetooth Low Energy for smart grid and smart home applications. *2016 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas.

Deepali, J., Mohd, M. S., & Mayur, S. (2013). Home Automation and Security System Using Android ADK. *International Journal of Electronics Communication and Computer Technology, 3*.

Felix, C., & Raglend, I. J. (2011). Home automation using GSM. *2011 IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies*, Thuckalay, India.

Han, J., Choi, C. S., Park, W. K., Lee, I., & Kim, S. H. (2014). Smart home energy management system including renewable energy based on ZigBee and PLC. *2014 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas.

Jamil, M. M., & Ahmad, M. S. (2015). A pilot study: Development of home automation system via raspberry Pi. *Biomedical Engineering (ICoBE), 2015 2nd International Conference on Penang*,

Kamoru, O., Olukayode, M., Shadrack, A., Akin, J., & Olatunji, T. (2018). Design and Implementation of Motion Detection Alarm and Security System. *International Journal of Scientific and Technology*, 26-38.

Khusvinder, G., Shuang-Hua, Y., Fang, Y., & Xin, L. (2009). A ZigBee-Based Home Automation System. *IEEE Transactions on Consumer Electronics, 55* (2), 422-430.

Muhammad, A., & Ahsan, R. (2016). An Overview of Home Automation Systems. *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 27-31.

Nikhil, A., & Subramanya, G. (2013). Microcontroller based Home Security System with Remote Monitoring. *IJCA Special Issue on International Conference on Electronic Design and Signal Processing (ICEDSP), 3*, 38-41.

Ramlee, R. A., Othman, M. A., Leong, M. H., Ismail, M. M., & Ranjit, S. S. (2013). Smart Home System using Android Application. *Information and Communication Technology (ICoICT), 2013 International Conference of, Bandung*, 277-280.

Ransing, R. S., & Rajput, M. (2015). Smart home for elderly care based on Wireless Sensor Network., *2015 International Conference on Nascent Technologies in the Engineering Field (ICNTE), Navi Mumbai*.

Ullah, M. A., & Celik, A. R. (2016). An Effective Approach to Build Smart Building Based on Internet of Things (IoT). *Journal of Basic and Applied Scientific Research* (6), 56-62.

Vivek, G. V., & Sunil, M. P. (2015). Enabling IOT Services using Wi-Fi - ZigBee Gateway for a Home Automation System. *2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Kolkata.

Zamshed, I., Haider, M., Moinul, M., Aktar, M., & Nafisa, S. (2011). Design and Implementation of Pyro-Electric Infrared Sensor Based Security Using Microcontroller.*Proceeding of the IEEE on Consumer Electronics*, 14-16.