International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 10 | Oct 2021 www.irjet.net p-ISSN: 2395-0072

IOT BASED ANTI THEFT SYSTEM FOR HOME

Siddalingesha G. R.[1] H. M. Shamita[2]

[1]M. Tech. Student, Dept. of Electronics and Communication Engineering, PDIT, Hospet, Karnataka, India
[2]Associate Professor, Dept. of Electronics and Communication Engineering, PDIT, Hospet, Karnataka, India

---

Abstract - *The project aims to design a framework for providing a house owner/member with the immediate notification of an ongoing theft or unauthorized access to their premises. For this purpose, a rigorous analysis of existing systems was undertaken to identify research gaps. The problems found with existing systems were that they can only identify the intruder after the theft, or cannot distinguish between human and non-human objects.*

Wireless Sensors Networks (WSNs) combined with the use of Internet of Things (IoT) are expanding smart home concepts and solutions, and their applications. This project proposes a novel IOT based smart home anti-theft system that can detect an intruder.

The fundamental idea is to design a cost-effective and efficient system for an individual to be able to detect any kind of theft in real-time and provide instant notification of the theft to the house owner. The system also promises to implement home security with large video data handling in real-time.

***Key Words*: WSN, IOT, Security, Anti-Theft, Smart home**

1. INTRODUCTION

IOT is generally considered as "Infrastructure of information Society", it enables us to obtain the data by each and every type of mediums like animals, kitchen appliances, humans, vehicles. Without human intervention IOT connects the physical objects that can exchange and communicate information between them.

In the modern era, security and surveillance are important issues. Recent acts of theft/terrorism have highlighted the urgent need for efficient video surveillance and on-the-spot notification of ongoing thefts to house owners and other household members.

A number of surveillance solutions are currently available on the market, such as CCTV cameras and digital video recorders (DVRs) that can record the unauthorized activities of a trespasser, but cannot distinguish between human and non-human objects. In recent times, the ratio of theft has increased tremendously due to a lack of awareness and low availability of smart-gadgets. The task of face detection and the recognition of an intruder become very difficult when the intruder hides their face partially or fully using some type of material, such as plastic, leather, or fabric.

Legacy systems cannot provide real-time theft notification to the house owner nor detect partially or fully obscured faces. It is also challenging for old systems to detect the intruder in the dark using a CCTV camera without night vision capability. The major flaw with this kind of arrangement is that it demands the 24/7 availability of a house owner or member, or manual video surveillance, which is almost impossible. In addition, it is a tedious task to go through all the recorded video clips after a possible theft has become known. It might be that the storage server contains a large amount of family member footage, which is of no use in identifying trespassers.

The proposed approach can be applied to an IoT-based smart home monitoring system in near real-time. A smart home designed and developed on an integrated framework of sensors, cameras, and customized hardware to analyze unauthorized access. The system operates at two different levels: through a hardware interface and through a software interface.

2. LITERATURE SURVEY

We have found different papers related to security system. Different security systems used for different purposes. Sushma .N. Nichal, Prof. J.K. Singh has done abstraction of Smart supervisor system using IOT based on embedded Linux O.S. with ARM11 architecture. In this Paper they have implemented real-time video monitoring system and acquired data. In this system they have also used PIR, temperature, Humidity sensors the system first requires authentication from user to activate the system if the system detect human it will send that data to the server or user smart phone.

Yogita Vijay Narkhede,S. G. Khadkehave presented smart security system with Raspberry Pi and IR sensor if IR sensor detects the person camera will capture image as well as video of the person, the data then encrypted first and then decoded. User will get notification on his mobile device. Authors discussed that user can also perform the live streaming and provide security. Authors have concluded that this system is important for commercial places; they have discussed few advantages of the system.

Harikrishnan G.R. et al have implemented home automation and security system in this system user can continuously monitor home from remote location if the intruder detected system will generate alarm and captures the image of the intruder and the captured image will be

send to owners mobile through SMS, WhatsApp, Call, E-mail. They have discussed few advantages of this system. Authors have concluded that this system is useful for securing commercial places.

R.Chandana et al have implemented monitoring and home security system using think and speak with the help of raspberry Pi, they have used Gyro sensor to detect the movements of person if the movements is detected camera will be captured image and the image will be send to the owners mail id with captured image. They have also stated some importance of this system. Authors have concluded that this system is important for security purpose.

K Saravana Kumar et al have developed the security system with proximity sensor, Raspberry Pi, and Camera, proximity sensor detect the person after detecting the person camera will be initiated and capture the image and image will be uploaded to drop box and user gets the notification about the intruder in the form of SMS. They have discussed few advantages like cost effective, portable. Authors concluded that this security system is useful for security of homes.

3. PROPOSED SYSTEM

The proposed system consists of two units. 1. Wi-Fi module 2. Microcontroller unit with sensors. Connection established between ADC and output of all the sensors. Sensed data from the sensors are spontaneously processed by the microcontroller and if something is sensed above the limit it sends an alert message to the owner of the house.

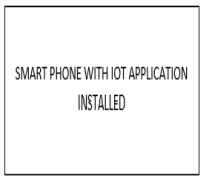

Fig.1: Mobile Unit

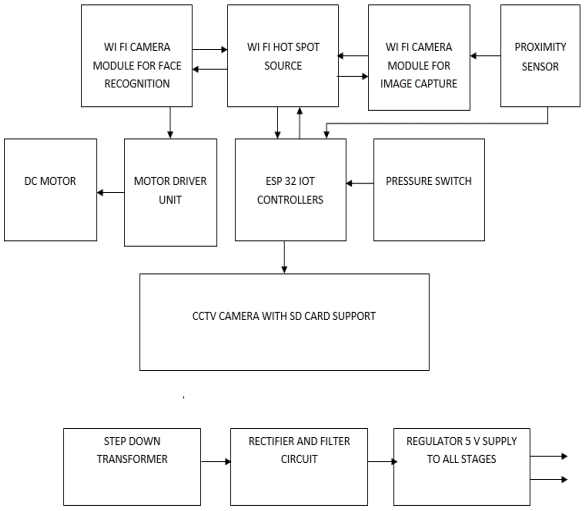

Fig.2: Microcontroller Unit

4. HARDWARE REQUIREMENTS

ESP 32: ESP 32 is the chip, which has high application potential in the future, for connection oriented projects we build. ESP 32 can be used for building connected things projects, alternative to microcontroller and add-on Wi-Fi, Bluetooth modules.

ESP32-CAM: The ESP32-CAM is referred as development board, which consist an OV2640 camera, a chip of ESP32-S chip and a slot of micro SD card and various GPIO's to connect peripherals.

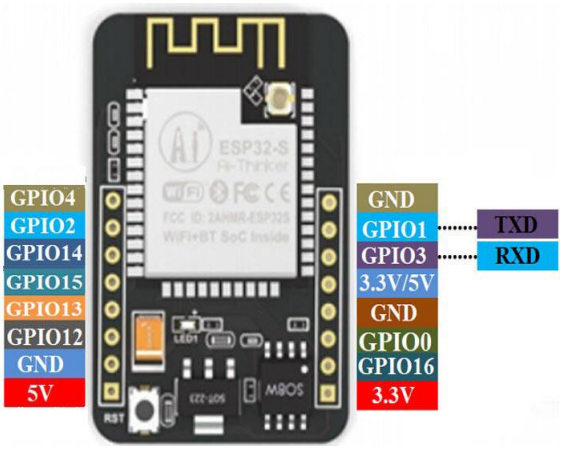

Fig 3:ESP 32 Cam Module

ELECTROMAGNETI RELAY AND INTERFACING CIRCUIT: Relay is utilized to control the external devices along with the isolation and it is defined as an electromagnetic switch.

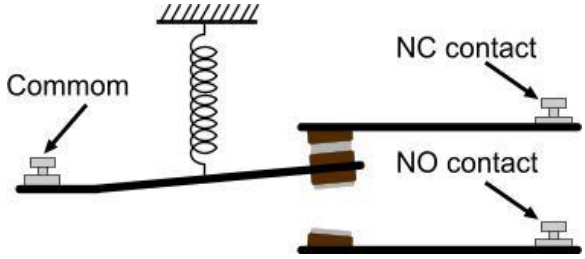

Fig 4: Internal contacts of the relay

Internal contacts of the relay is shown in the figure above. Off state of the relay is represented in the figure above. The relay shown in the figure is in off state. Common is in NC (Normally closed) contact When the relay is in off state and common is open for normally open contact.

IR Proximity Sensor: For various purposes technology of IR utilized in everyday life and industries. For instances, TVs, to understand the signals from the remote control it utilizes IR sensors. Convenient characteristics, easy design and minimum power usage these are the major advantages of the IR sensors. In electromagnetic spectrum in the region of visible and microwave IR signals are found. Generally, these waves wavelength are in range from 0.7 µm to 1000 µm. IR spectrum classified into 3 regions such as far-infrared, mid infrared and near infrared. The wavelength range of far infrared radiation is more than 6 µm,the wavelength range of mid infrared radiation ranges from 3 to 6 µm and the wavelength range of near infrared radiation ranges from 0.75 – 3 µm.

Fig 5: IR Proximity sensor

DC Motor: A Direct Current (DC) motor is a motor that diverts energy from an immediate current and transforms this into mechanical energy. The rotor is normally present within the motor, but stator is present outwardly. It has loop windings which are fuelled through DC current and the stator has lasting magnets or electro-magnetic windings. At the point when the motor is fuelled by DC current, an attractive field is made inside the stator, drawn in, repulsing magnets on it. Now rotor starts to turn. To keep the rotor pivoting, the motor has a commutator. It would quit turning, yet for this situation the commutator would switch the current through the stator and this way opposite the attractive field. This way the rotor can continue to turn. See the picture on the appropriate for a schematic showcase of how the dc motor functions.

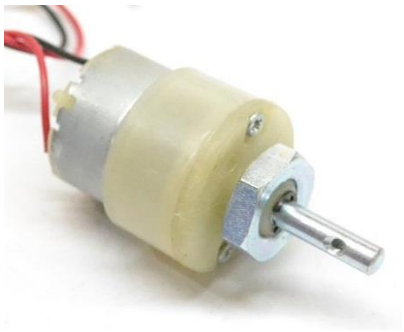

Fig 6: Dc Motor

Pressure Switch: A pressure switch is a form of switch that operates an electrical contact when a certain set fluid pressure has been reached on its input. The switch may be designed to make contact either on pressure rise or on pressure fall.

Fig 7: Pressure Switch

5. SOFTWARE REQUIREMENTS

BLYNK: Assume a prototyping board on your android which consists of sliders, displays, graphs, drag and drop buttons and other operational widgets. And it controls the arduino and collects the data from it. BLYNK operates over the internet. Hence it is necessary that your hardware can communicate with internet. You can select any kind of connection like Wi-Fi, Ethernet or ESP8266. Example sketches and BLYNK libraries will connect you to online and pair up with your android.

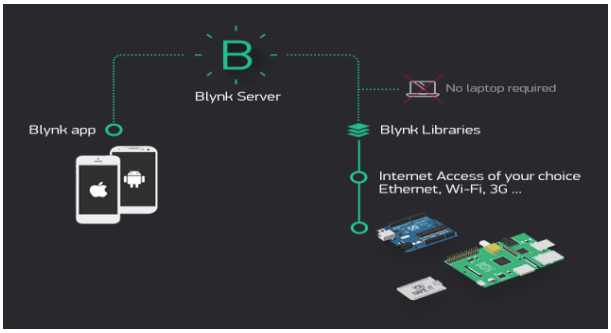

Fig 8:BLYNK connections

6. EXPERIMENTAL RESULTS

The following screenshots shows the results of the proposed system. Figure1 shows the blynk app with camera on, figure 2 shows the detection of intruder and figure 3 shows the image captured and sent to the owner,s computer through IOT.

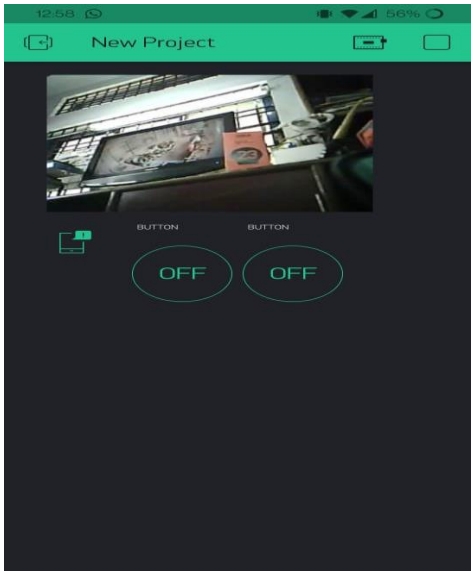

Fig 9: BLYNK App with Camera View

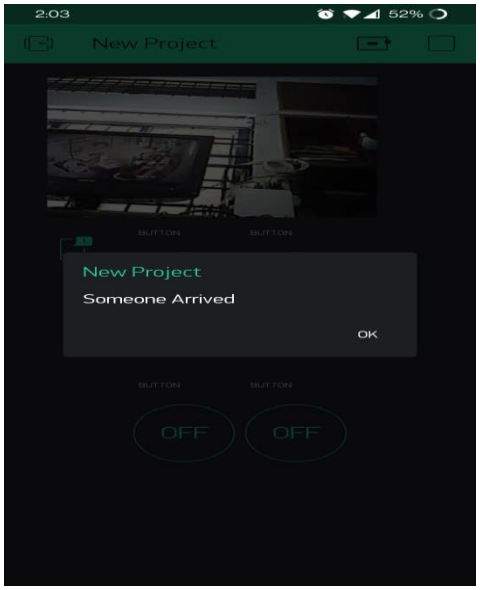

Fig 9: BLYNK App with Intruder Detection

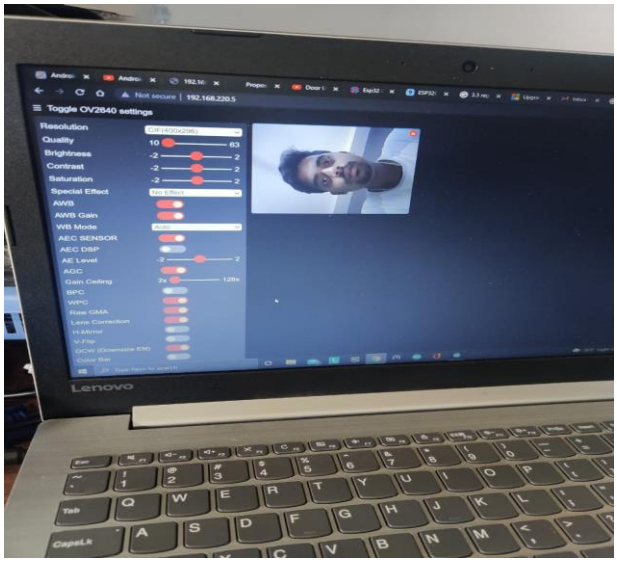

Fig 10: Owners Laptop with Intruder Picture

7. CONCLUSIONS

This project presents an innovative method to prevent smart home theft by providing spontaneous notification of ongoing intrusion. The research has provided a novel wireless sensing system for the surveillance and detection of a human intruder as well as instant notification of the intrusion to prevent theft.

It eliminates the use of DVR for recording as well as the use of large amounts of memory for storage. The system can effectively identify a human intruder and prevent false alarms when the intruder is a non-human, by distinguishing between human and non-human objects. All of these processes lead to the instant notification of intrusion by providing real-time notification about the potential theft.

The main advantage of the proposed system is that it is cheaper than the DVR and other surveillance-based solutions available on the market. If an intruder disables WiFi connection using DoS attack then the proposed system will not be able to notify the house members about the ongoing theft. However, the proposed system is equipped with Bluetooth network, which can still record the ongoing theft but cannot send the notification to the house owner due to the lack of WiFi/Internet connections.

New research challenges of security and privacy have arisen due to an increase in products that connect the cyber and physical worlds. It is expected that these research problems will be further resolved in the upcoming future.

REFERENCES

[1] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Regularized Transfer Boosting for Face Detection Across Spectrum," IEEE Signal Processing Letters, vol. 19, no. 3, pp. 131–134, 2012.

[2] W. H. Alobaidi, I. T. Aziz, T. Jawad, F. M. F. Flaih and A. T. Azeez, "Face detection based on probability of amplitude distribution of local binary patterns algorithm," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-5.

[3] Z. Jian, Z. Chao, Z. Shunli, L. Tingting, S. Weiwen and J. Jian, "Pre-detection and dual-dictionary sparse representation based face recognition algorithm in non-sufficient training samples," in Journal of Systems Engineering and Electronics, vol. 29, no. 1, pp. 196-202, Feb. 2018.

[4] T. Ahmed, S. Ahmed, S. Ahmed, and M. Motiwala, "Real-Time Intruder Detection in Surveillance Networks Using Adaptive Kernel Methods," 2010 IEEE International Conference on Communications, 2010.

[5] A. Sepas-Moghaddam, F. Pereira and P. L. Correia, "Light Field-Based Face Presentation Attack Detection: Reviewing, Benchmarking and One Step Further," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1696-1709, July 2018.

[6] H. Zhang, Q. Li, Z. Sun and Y. Liu, "Combining Data-Driven and Model-Driven Methods for Robust Facial Landmark Detection," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2409-2422, October 2018.

[7] "Identity Theft Research," Detection, Prevention, and Security Identity Theft Handbook, pp. 263–276, 2015.

[8] J. S. Kim, D. H. Yeom, Y. H. Joo, and J. B. Park, "Intelligent Unmanned anti-theft system using network camera," International Journal of Control, Automation and Systems Int. J. Control Autom. Syst., vol. 8, no. 5, pp. 967–974, 2010.

[9] V. V. Jog, D. Jain, R. Arora, and B. Bhat, "Theft prevention ATM model using dormant monitoring for transactions," 2013 IEEE Conference On Information And Communication Technologies, 2013.

[10] H. Li, "Design for home security video monitoring system based on SOPC," null JOURNAL OF ELECTRONIC MEASUREMENT AND INSTRUMENT, vol. 24, no. 3, pp. 294–300, Sep. 2010.