Realization of an IoT System to Ensure Doorway Security by Integrating ESP32-CAM with Cloud Server

Ms. Priyanka[1], Mr. Parveen Kantha[2]

[1]M.Tech. Scholar, Department of Computer Science Engineering, B.R.C.M.C.E.T., Bahal, Haryana, India
[2]Assistant Professor & Head, Department of Computer Science Engineering, B.R.C.M.C.E.T., Bahal, Haryana, India

---***---

Abstract - *The research work being reported here in and titled as "Design & Implementation of an IoT Networked Contactless Doorway Security System for Remote Monitoring and Control using ESP32-CAM and a Cloud Server". People want security in everyplace possible when they are into their homes or away from their homes. An anti-theft system is a device or method used to prevent or deter the unauthorized intrusion or trespassing activity in its coverage area. The implemented system was developed in combination of hardware and software. It's a unique security system made with low cost wireless camera and sensors which ensured remote monitoring and control of doorways. The system empowered the user to monitor the doorway by capturing images using a high performance wireless camera i.e. ESP32-CAM connecting other devices and sensors in an IoT network. For other tasks like to control electronic door lock remotely, to click more pictures as well as to get notifications a cloud server application 'Blynk' was used over the smart-phone. A major challenge was to develop this dynamic system with zero error, real-time response and smooth performance, viable, smart and feasible.*

Key Words: ESP32-CAM, Camera, IoT, Cloud, Blynk, Security, etc.

1. INTRODUCTION

The research work carried out here provided an insight into the development of IoT systems. The research area of the Internet of Things in recent years has experienced growth and development in an interdisciplinary manner. IoT is the inter-networking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The traditional fields of embedded system, wireless sensor networks, control system, automation systems are together interconnected to form the IoT. That means the internet of things builds over the revolutionary success of mobile and internet network.

2. OBJECTIVE

The aim of this work was to achieve a versatile, viable, low power doorway security solution with real-time response. The system developed should be integrated with IoT network and cloud computing. The objective was to develop a dynamic wireless doorway security system which empowers the user to acquire visitor's photo identity and take an informed decision for giving that person access into his/ her premises. Also the data collected by the cloud server could be retrieved if required for some investigation purpose. The developed system should be user friendly and feasible.

3. RESEARCH METHODOLOGY

This work had utilized the experimental set up based method of research as it was aimed to demonstrate the hardware interaction with a cloud server using a Wi-Fi local hotspot to remotely transfer the data specifically for monitoring and control based applications. The hardware used here comprised of a high performance low cost Wi-Fi enabled computational platform with integrated camera i.e. ESP32-CAM board. It has multiple GPIOs for interfacing with external input/ output devices. The other components used here to implement the proposed system were a solenoid lock, a buzzer, a two-channel relay module, an infrared proximity sensor module, a tactile push button, +5V and +12V DC power source, a USB TTL-UART Convertor to program ESP32-CAM board and finally a smart-phone with a 'Blynk' account. The experimental results obtained from this hardware experimental set-up should validate the work. The research will incorporate the gathering of data from the datasheets about various components used in developing the hardware. Data gathered from these research efforts were used to formulate the overall procedure to design, develop and implement the system. Appropriate tables, flowcharts and figures were included in the final report along with the snapshots of working prototype.

3.1 Hardware Connections

The developed system consists of multiple components hardwired as per the circuit design demonstrated below in figure 1. Here in this design the connections were made using multi-colored wires with appropriate signal flow directions so that it could be tracked easily that which wire belongs to which component. The signal flow demonstrated here segregates the input signal and output signal. All the components were interfaced to the GPIOs of ESP32-CAM as per the table given below.

Sr. No.	ESP32-CAM Pin	Interfaced with	Signal Nature	Action
1	GPIO 12	RELAY -2	Output	Turn ON/ OFF Door Lock
2	GPIO 13	RELAY-1	Output	Turn ON/ OFF Door Bell
3	GPIO 15	TACTILE PUSH BUTTON	Input	To Open the Door Lock from Inside
4	GPIO 2	IR PROXIMITY SENSOR	Input	To Ring the Door Bell & Click Photo
5	+5V	+5V DC Power Supply	Power	To drive the complete circuit
6	GND	DC Power Supply	Power	To drive the complete circuit

Table 1: ESP32 CAM Pin Connections

The Tactile Push button could be replaced by another infrared proximity sensor. Here one of the pins of tactile push button was connected to the GND signal (logic level 0) and another pin was connected to the GPIO-15 of ESP32-CAM board. A 10 Kilo Ohm resistor was also connected to pull-up (raise the logic level to high) this pin during high-impedance state. When the push button got pressed it gives a logic low (0) to the GPIO-15 otherwise it remains in its default logic high (1) state. Similarly, infrared proximity sensor at GPIO 2 gives logic high (1) for any detection otherwise it remains in its default logic low (0) state. Both the relays used here were driven by +5V DC power supply but they were used to control the switching of some higher voltage (+12V DC) devices like solenoid door lock and door bell buzzer. So, two separate DC power sources were used here to drive the system.
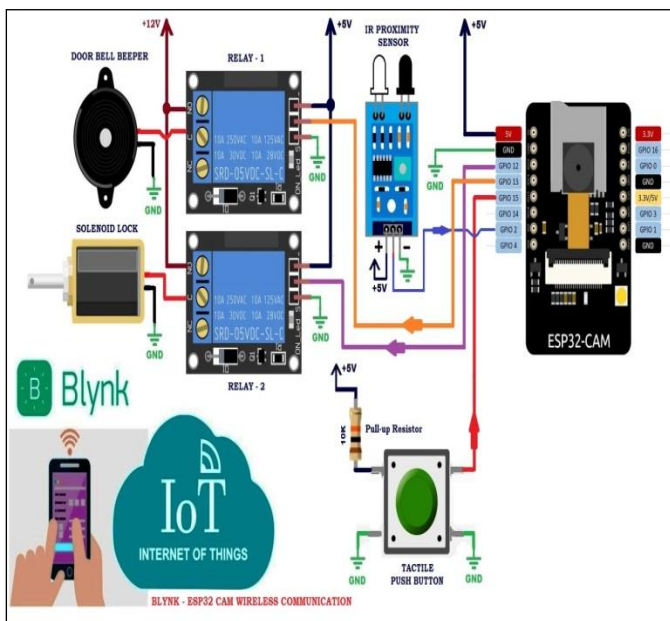

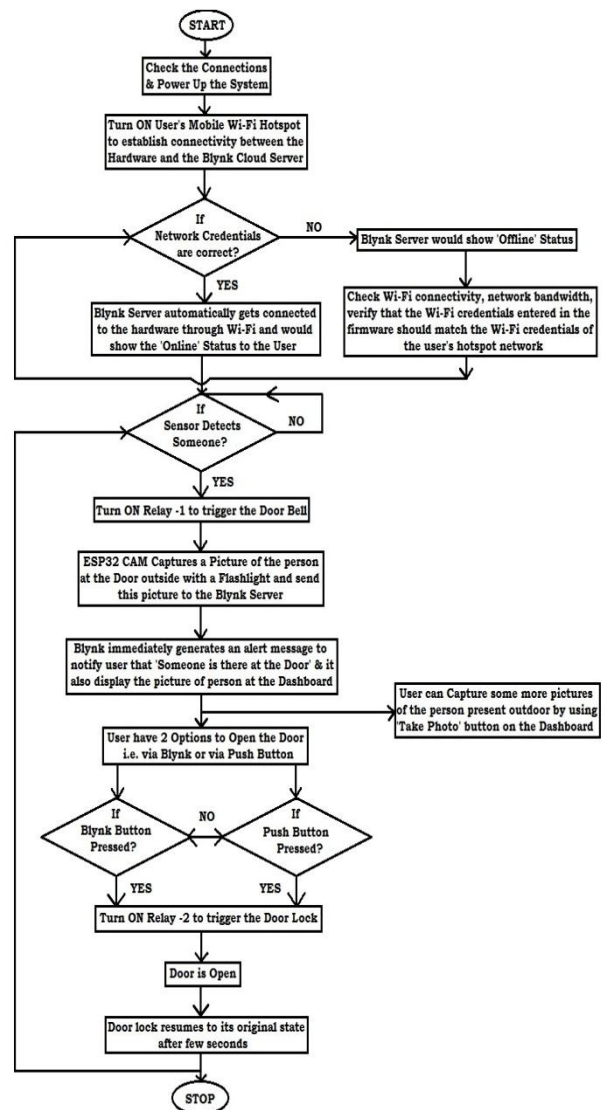FIG 1: Circuit Diagram

3.2 Flowchart

FIG 2: Flow Chart

4. EXPERIMENTAL RESULTS

4.1 Experimental Set-up

The experimental setup was developed as per the circuit design. The whole circuit was developed around ESP32-CAM board and all the input-output devices including IR Proximity sensor module, tactile push button, door bell, solenoid door lock and two LED indictors were connected to it via jumper wires. The circuit was powered by two DC power supply units. One was +12V DC to power up the door bell and the door lock and another one was +5V DC to power up rest of the circuit. To control the switching of these high power devices through 5V toggling signals, from ESP32-CAM, we used relays here. High power LEDs were also driven by these relays only. These LEDs were

used as indicators here in this design and the Red LED indicates the status of Door Bell and the Green LED indicates the status of Door Lock. The time of Door Lock and Door Bell operation can be extended or reduced by altering the delay values in the firmware. Initially the experimental set-up was developed as shown below in figure 3.
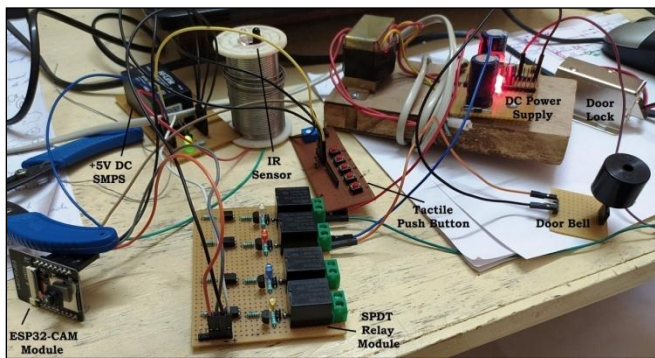

FIG 3: Experimental Set-up

4.2 Final Prototype Working

In the developed system the hardware prototype was deployed over a wooden board to demonstrate it as a real door. Here in this IoT system IR proximity sensor, ESP32-CAM and two LED indicators were deployed on the visitor side of door called the outdoor section. Similarly, Solenoid Door Lock, Door Bell, Tactile push button were deployed on the owner's side of the door called the indoor section.

1. Power up the system
2. Turn ON Wi-Fi Hotspot in the Smartphone whose credentials were entered in the firmware
3. Open up the Blynk Dashboard in the Smartphone and wait for the connection
4. A visitor at the door triggered the contactless door bell by raising hand
5. The bell rings for just two seconds turning the Red LED indicator on and instantly the camera clicks the picture with a flashlight. The door was still locked
6. The owner received a notification string 'Someone is there' on the Blynk dashboard followed by an image of visitor standing at the door outside
7. Thus the owner got the privilege to identify the visitor and respond back accordingly
8. The owner then could unlock the door by pressing a virtual button 'Lock' over the Blynk dashboard using smartphone or by pressing a physical push-button installed on the door
9. The owner could take some more photographs remotely by just pressing another virtual button 'Take Photo' deployed over the Blynk dashboard
10. The door unlocked for just 3 seconds only

Sr. No.	Input Signal Source	Signal Level	ESP32 CAM	Red LED	Green LED	Door Bell	Door Lock
1	IR Proximity Sensor	0	OFF	OFF	OFF	OFF	L
2	IR Proximity Sensor	1 → 0	ON → OFF	ON → OFF	OFF	ON → OFF	L
3	Virtual Button-1 'Lock'	1 → 0	OFF	OFF	ON → OFF	OFF	UL → L
4	Virtual Button-2 'Take Photo'	1 → 0	ON → OFF	OFF	OFF	OFF	L
5	Tactile Push Button	1 → 0	OFF	OFF	ON → OFF	OFF	UL → L

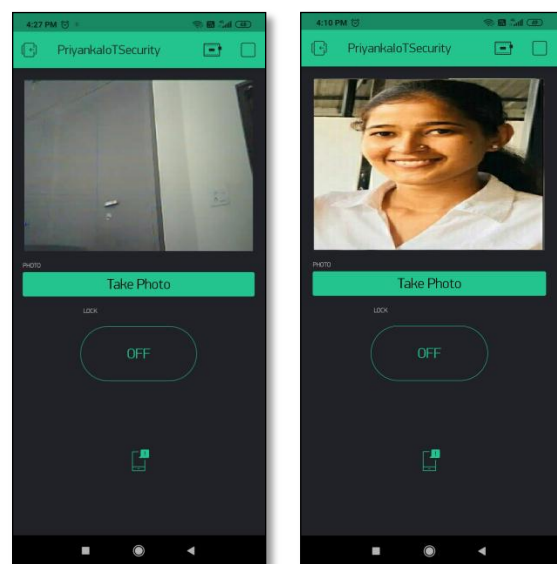Table 2: System Output Response for each Input

4.3 Results

FIG 4: CAM Images Received over Blynk Dashboard

The results obtained from the final prototype board could be clearly observed over the Blynk dashboard. For this the Blynk application was downloaded and installed into the user's smartphone and an account was created there by entering the required user credentials. The user was assigned an authorization token ID over the e-mail which was entered in the firmware itself before uploading it to the ESP32-CAM. A new project was created in the graphical-user-interface window of the Blynk App by selecting some widgets from its wide library and configured those widgets as per the system hardware and firmware. The ESP32-CAM based hardware and the Blynk over the smartphone got connected with the help of Wi-Fi hotspot network. Any interruption detected by the proximity sensor triggered the whole process and the

visitor could be monitored on the Blynk project dashboard screen along with an alert notification and that too in real-time. Also the relay to actuate the solenoid door lock could be triggered remotely by using this platform. One thing to note down here by the user was that the wireless communication network established here for the system was a local network only and thus the system operation was limited within the confines of the local Wi-Fi hotspot used by the user to establish system connectivity. To access this system from any place in the world some other protocols would be required at the firmware level and it was not under the scope of this work. Hence the overall response of developed hardware and the Blynk dashboard created for this purpose validated the work.
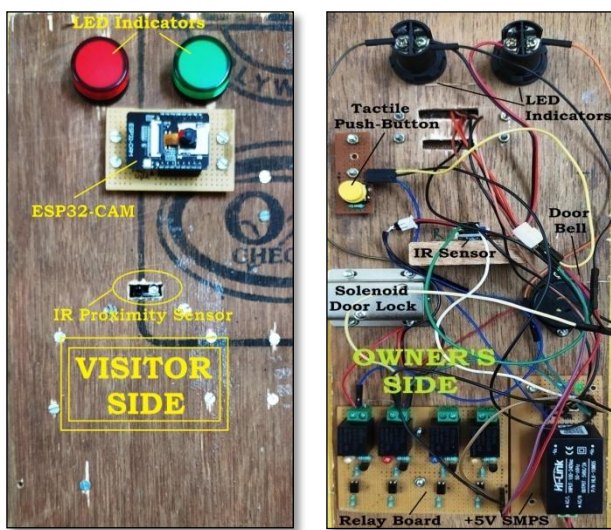

FIG 5: Final Prototype Implemented

5. CONCLUSION

By the end of successful completion of this work it was concluded that through IoT we can connect multiple input/ output devices, multiple sensors and actuators in a network so that they can talk to each other, data acquired from these things can be used to keep a log or monitor or control the other things without human intervention and much more. Thus IoT is like global networks which give the communication between things to things, human to things and human to human. IoT is the development of existing internet facility to manage everything which exists in the world or exists in the future. As per this work, surveillance is the procedure of close deliberate perception or supervision kept up over an individual, gathering, and so forth particularly one in care or under doubt. For the above mentioned purposes I developed here a system which was equipped with sensor, camera, processor, relays, buzzer, LED indicators and actuators as per the application requirements. The system worked well in the local environment and responded well as per the expectations. The Blynk cloud server was perfect for such

type of applications as it is the most popular IoT platform for connecting devices to the cloud, designing apps to remotely control and monitor them, and managing thousands of deployed products. Blynk software helps individuals and organizations to seamlessly progress from a prototype of a connected product to its commercial launch. The software is super easy to use. It's compatible with Arduino, Raspberry Pi, NodeMCU, and other microcontrollers. Very little coding is required and one can get a system up and running in no time.

REFERENCES

[1] Piyush Kumar Singh; Rahul Saxena; Utkarsh Dubey; Aakansha Raj; Biswa Mohan Sahoo; Vimal Bibhu, "Smart Security System Using IOT", International Conference on Intelligent Engineering and Management (ICIEM), 2020, Publisher: IEEE

[2] Tina; Sonam; Harshit; Muskan Singla, "Smart Lightning and Security System", 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, Publisher: IEEE

[3] Kushank Sehgal; Richa Singh, "Iot Based Smart Wireless Home Security Systems", 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), 2019, Publisher: IEEE

[4] Muhammad Zeeshan Saeed; Raja Raheel Ahmed; Omar Bin Samin; Nusrat Ali, "IoT based Smart Security System using PIR and Microwave Sensors", 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019, Publisher: IEEE

[5] Kabita Agarwal; Arun Agarwal; Gourav Misra, "Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT", Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, Publisher: IEEE

[6] Roshmi Sarmah; Manasjyoti Bhuyan; Monowar H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System", IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, Publisher: IEEE

[7] D. C. Dalwadi; B. C. Goradiya; K. Karthic; R. Rai, "GSM based security system", Journal of Computer Technology & Applications, 2019

[8] C. Davidson; T. Rezwana; M. A. Hoque, "Smart home security application enabled by IoT: in Smart Grid and Internet of Things", Cham: Springer International Publishing, 2019