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

Design & Development of an IoT System to Enable User to Remotely Monitor and Control Doorway Access

Mr. Ankit Sharma[1], Dr. Vivek Kumar[2], Mr. Vikrant Verma[3]

[1]*M.Tech. Scholar, Department of Electrical & Electronics Engineering, B.R.C.M.C.E.T., Bahal, Haryana, India*
[2]*Professor & Head, Department of Electrical & Electronics Engineering, B.R.C.M.C.E.T., Bahal, Haryana, India*
[3]*Assistant Professor, Department of Electronics & Communication Engineering, CGC Jhanjeri., Punjab, India*

Abstract - *The research project undertaken is termed and is being reported on here as "Design & Development of an IoT System to Enable User to Remotely Monitor and Control Doorway Access". When people are at home or away from home, they want to feel secure in every situation. An anti-theft system is a technology or mechanism that is used to prevent or deter unwanted access or trespassing activities in the region it covers. The prototype developed was basically a hardware and software interface. It's a one-of-a-kind security system that uses low-cost wireless cameras and sensors to provide remote entryway monitoring and control. The system was connected to an IoT network multiple actuators and sensors via an IoT network that enables the users to keep an eye remotely on the entryway by taking photos with a high-performance wireless camera, such as the ESP32-CAM. A cloud server application called Blynk was used over the smart-phone for various functions such as controlling an electronic door lock remotely, taking more images, and receiving notifications. The development of this dynamic system with zero error, real-time response, and smooth performance, as well as making it viable, clever, and feasible, was a huge task.*

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

1. INTRODUCTION

The IoT may be defined as an extended internet and network connections to diverse sensors and devices — or 'things' — offering a better degree of calculation and analytical capability even for basic products like light bulbs, locks and sales. The accessibility of the IoT is among the most significant features of its increasing popularity. Connected or 'smart' devices – as 'things' in the IoT are commonly termed – may collect data and exchange it with other wired and wireless networks from their surroundings. By analyzing and interpreting the data, machines may carry out their tasks with little or no human intervention. Components of their goods are introduced by suppliers to enable them to communicate data back on how things work. This can enable individuals to monitor if a failure happens and exchange before damage might occur. Companies may also make their systems and logistics providers more efficient using the information provided by these sensors, given that they have much more precise information on what actually happens. Production systems may become substantially more responsive also with inclusion of extensive, real-time data collecting and processing.

2. OBJECTIVE

The objective was an adaptable, practical, low-power door security technology with a reliable reaction in real time. IoT network and cloud computing should integrate the system that has been built. The aim was to build a dynamic wireless safety door system that enables the user to obtain the photo identity of the visitors and to make educated decisions to provide them with entry. If necessary for investigative purposes, including the data gathered by the cloud server can be accessed. The system created should be easy to use and viable.

3. LITERATURE REVIEW

The IoT allows things to be recognized and remotely controlled in the entire system framework, making doors open for more physical combinations of the world into PC-based frameworks and providing better accuracy, skills and financial benefits [1]. The concept for this article is essentially IOT and cloud-based services that here provides a cost-effective, secure, tolerant and easy to use monitoring and control system [2-4]. Although static systems built around multi-sensor networks are already flooded in the world market [5]. For dynamic systems the concept of Internet of Things (IoT) is becoming popular nowadays where millions of heterogeneous devices demand seamless communication [6]. IOT offers the possibility to use the Internet from anywhere else to operate the domestic automation system [7]. So, here is a system that uses IoT concept to demonstrate a dynamic doorway security system with least human intervention involved.

4. RESEARCH METHODOLOGY

The goal of this research was to show the hardware connection with a cloud server via a local Wi-Fi hotspot, which allows the remote transmission of data for monitoring and control-based applications. A computer

platform with an integrated camera, i.e., ESP32-CAM, with high-performance low-cost Wi-Fi is available for the hardware utilized here. It features many GPIOs to interface with external devices. The additional components for implementation were a power lock, a buzzer, a two-channel relay module, a proximity sensor infrared module, a +5V and +12V DC power supply, a USB TTL-UART to ESP32-CAM programming board and then, lastly, a smart phone with a 'Blynk' accounts. A smart phone was added. This hardware experimental setup should confirm the experimental results. The investigation will include data collection from data sheets on different components utilized in hardware development. The data collected from these research activities have been used to build, develop and execute the entire system process.

4.1 Hardware Connections

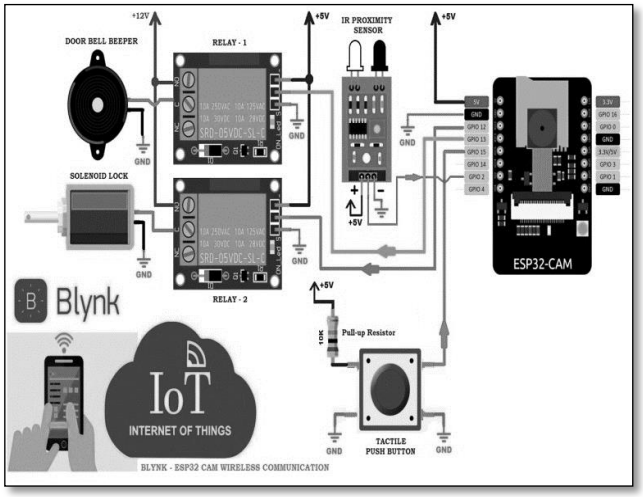

FIG 1: Schematic Diagram

The system has many hardwired components, as shown in Figure 1. In this design, the connections with proper direction of signal flow were created via multi-colored wires so that cables belonging to whatever component could readily be monitored. The signal flow separates the input and output signal. The GPIOs of ESP32-CAM were interfaced with all components in the following table.

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

Another infrared proximity sensor might replace the Tactile Push button. The GND signal was attached to one of the touch buttons pins (logical level 0), and the ESP32-CAM board's GPIO-15 pin was linked to another one. The pull up of this grip (up to high logic level) during the high-impedance stage is additionally supported by a 10-kilo Ohm resistor. The GPIO-15 is logically low (0) when the push button is pressed else it would stay high (1) in its default logic state. Infrared proximity sensor on GPIO 2 similarly delivers high (1) logic in its default low (0) state to detect any detection otherwise.

4.2 Flowchart

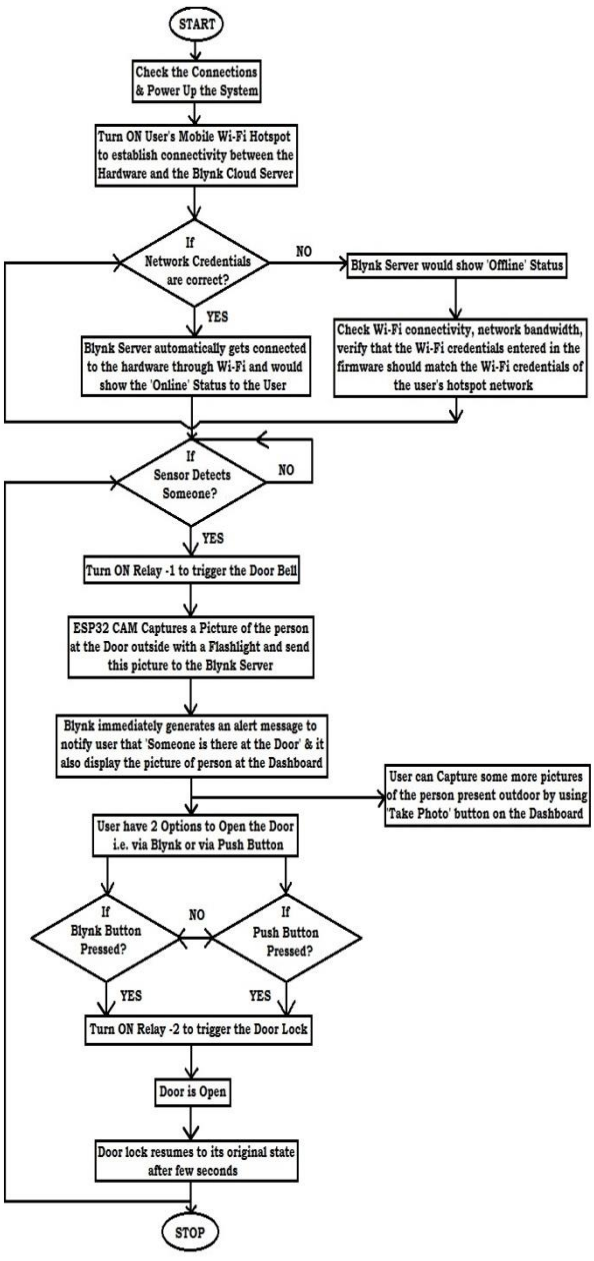

FIG 2: Implemented Flow Chart

4.3 System Operation

The system here created was totally user-friendly and environmentally friendly and provided an economical solution for a highly dependable safety system. In light of the Covid-19 scenario, the ESP32 CAM and infrared-reduced sensor unit was used on the external side of the door for the guest. By combining a cloud server platform with the proposed IoT system, the whole procedure to monitor and monitor the door was made totally contactless. There was also another provision for the actual opening of the door. The owner was allowed to access the guest using a smartphone or a physical button in the vicinity of the entrance via a virtual button.

5. EXPERIMENTAL RESULTS

5.1 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, doorbell, 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.

5.2 Final Prototype Working

The hardware-prototype was mounted on a wooden board to show it as a genuine door in the designed system. Here, on the guest side of the door, ESP32-CAM and two LED indicators, named the outside section have been implemented in this IoT system IR proximity sensor. Similarly, on the owner's side of the door termed the inside part, the Solenoid Door Lock, Door Bell, tactile push button was used.

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

1. Power up the system
2. Turn on Wi-Fi Hotspot on your smartphone using firmware credentials.
3. Open your smartphone Blynk Dashboard and expect connectivity.
4. The contactless door bell was activated by a door visitor by the hand.
5. The bell rings the Red LED indication for just two seconds The camera clicks with a spotlight immediately on the image. The gate remained closed.
6. The owner got a message string "Someone is there," followed by a visitor picture, which stands outside the door, on the Blynk dashboard.
7. The owner therefore had the liberty of identifying the visitor and answering accordingly.
8. The owner may then open the door with the use of an on-board virtual button "lock" or with a custom push-button on the door, through a smartphone.
9. By pushing a virtual button 'Capture Photo' installed over the Blynk dash board, the owner may take some additional photos remotely
10. The door unlocked for just 3 seconds only

5.3 Results

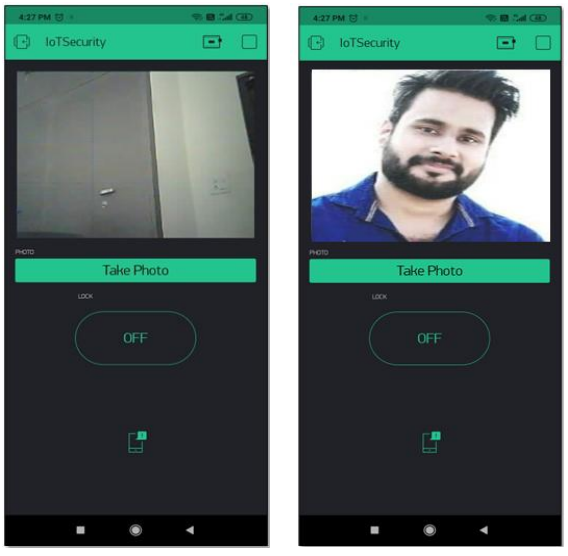

FIG 3: CAM Images Received over Blynk Dashboard

On the Blynk dashboard the findings from the final prototype board could be easily viewed. This was done by downloading and installing the Blynk program onto the user's smartphone and by entering the needed user identification, a user account was established. The email which was inserted in the firmware itself before it was uploaded to the ESP32-CAM was provided to the user with an Authorization ID. A new project was established via picking certain widgets from its large library in the graphical user interface window of the Blynk App, and configuring them using the hardware and firmware of the machine. Wireless connections have been made using the ESP32-CAM based hardware and the Blynk via smartphones. Any disruption identified by the local sensor started the entire process and could also be viewed in real time on the Blynk project dashboard page. This platform may also activate the relay to control the lock on the solenoid door remotely. One thing the user could see was that the wireless communication network set up here was simply a local network, so system operations were confined to the boundaries of the local wireless Internet hotspot that the user uses to build a system connection. Some more protocols at firmware level would be necessary from anywhere in the globe to access this system, and this was not part of our task. Therefore, the overall answer generated for this purpose by built hardware and the Blynk dashboard confirms the work.

6. CONCLUSION

When the study was successfully finished, we could link numerous input/output systems, multiple sensors and actuators to one another via IoT so that data gained from this may be used without human involvement, to maintain logs or monitor or to operate objects without human interaction. IoT is like worldwide networks that communicate between objects, between human and human and human. IoT is the development of current internet facilities to manage all that exists or exists worldwide. As per this work, monitoring is a method in which an individual is closely sensed or monitored, collected, and so forth, especially carefully or in question. I designed for these reasons a system which was furnished, in accordance with the application requirements, with sensor, camera, cellular, reel, buzzer, LED indications and drives. The technology functioned effectively in the local setting and met the requirements nicely. The Blynk cloud server was ideal for such applications as it is the most popular IoT platform for cloud-based devices, apps for remote monitoring and remote control and management of thousands of installed products. Blynk Software allows people and organizations, from a prototype of a connected product through its business launch, to develop effortlessly. The program may be used quite easily. The device is Arduino, Pi, NodeMCU and other microcontrollers compatible. It requires very little code and you can start a system 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