IoT based Smart Security and Surveillance System

Gurusha Lulla
Department of Computer Engineering
M.E.S. College of Engineering
Pune, India
gurushalulla@gmail.com

Abhinav Kumar
Department of Computer Engineering
M.E.S. College of Engineering
Pune, India
singhak97@gmail.com

Govind Pole
Department of Computer Engineering
M.E.S. College of Engineering
Pune, India
govind.pole@mescoepune.org

Gopal Deshmukh
Department of Computer Engineering
M.E.S. College of Engineering
Pune, India
gopal.deshmukh@mescoepune.org

2021 International Conference on Emerging Smart Computing and Informatics (ESCI) | 978-1-7281-8519-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ESCI50559.2021.9396843

***Abstract*—Internet of Things (IoT) is an escalating trend in today's world, and has proved to be a game changer in the field of technology. More and more sensors and devices are being connected together to develop new systems to solve real world problems. With the increase in technology and automation, security has become a major concern. The first line of defense for any property is always a security system, which alerts the owners regarding intrusion in real time. Currently, there exist multiple security systems, which make use of various motion sensors to detect any motion and notify the owner about the intrusion. However, most of these systems do not provide the features of zone barriers, facial recognition, remote camera surveillance and power failure detection, combined with ease of use, economic viability and power efficiency. The main objective of the proposed architecture is to overcome all these problems by developing a smart security and surveillance system which makes use of multiple ultrasonic sensors to detect intrusion attempts on the property of the owner, in order to notify them of the presence of an unauthorized person. Also, the system provides a warning to the person who has intentionally or unintentionally entered the property, so that they can step back in time, without triggering any alarm. With the help of a remote camera surveillance feature, the owner can monitor the surroundings of their property remotely. This system will issue an alert to the owner in case of a power failure as well. This system provides face recognition as an authentication procedure, in order to allow the valid entrants to enter into their property. All these features combined, create a flexible and reliable security system, which can be used in various properties, such as homes, offices, museums and so on.**

***Index Terms*—IoT, Perimeter Security, Camera Surveillance, Face Recognition, Arduino, Smart Security, Ultrasonic Sensor.**

I. Introduction

The technology in today's world is advancing at an unimaginable pace and the society is continuously exposed to new security concerns due to this rapid paced advancement. The utmost priority for anyone is to make sure that their commodities, such as homes, offices, money and collectibles are safe. As per a report, there are roughly 2.5 Million burglaries per year, out of which, 66% are home break-ins [1]. Also, according to the Federal Bureau of Investigation (FBI), 65% of burglaries happen between 6 a.m. and 6 p.m. and the average loss per burglary is $2,416 [1]. As per the same report, 65% of burglaries occur during the day to reduce the chance of someone being home [1]. Since the automation in the field of security is increasing day by day, there is a huge demand for security systems that can provide multiple security features within one system.

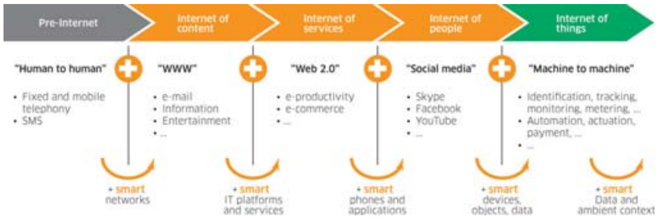

Fig. 1. Evolution of IoT [3]

The proposed system helps the users of the system to detect intrusions in time, thereby saving them from large amounts of financial losses. As cases of thefts and burglaries are becoming more common with each passing day, it is wise to have a security system in place. This system can detect and alert the owner about intrusions. The most widely used motion sensor is the Passive Infrared Sensor (PIR) [2]. In most of the systems, PIR sensors are being used to detect any kind of motion and the system notifies the user of the incident without being fully aware of the context.

The proposed system makes use of an Arduino Mega 2560, Ultrasonic sensors, Cameras and a combination of WiFi modules to deal with security issues faced by people. The system also consists of the feature of facial recognition as an authentication procedure in order to allow the users of the system to enter into their property. This module is connected to the entrance of the property and allows access to the valid entrants as soon as their faces have been authenticated. The system also locks the entrance automatically after a fixed time interval, in order to stop other people from entering the property after the users. This acts as an additional layer of security.

II. Literature Survey

The paper “Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform” extracts useful data from 63 research papers that examined smart home safety and security systems using the Arduino platform. This paper gives us a deep insight about the types of motion sensors and the frequency of their use in security systems and also talks about the various types of alert mediums used in these systems. Further, this paper also details the use of various Arduino boards in these systems, while also comparing their architectures. This data has then been analyzed in order to extract useful information regarding the advantages and disadvantages of these systems and how future research could enable better implementation and use of these systems [2].

The “Real-Time Monitoring Security System integrated with Raspberry Pi and e-mail communication link” uses a combination of a Raspberry Pi and a PIR sensor for detecting motion and alerting the owner on their e-mail in case of an intrusion. Also, it makes use of a webcam for the purpose of surveillance whenever motion is detected. However, there is no facility available for accessing the webcam on demand without an intrusion. Also, a major drawback of this system is that it provides only one alert medium which fails in case the user does not have access to their mail. This system makes use of a keypad lock as the authentication procedure, which is less secure as the unlock pattern needs to be shared among all the users and there is no way to recognize who is making use of the pattern to unlock the door at a particular point in time [4]. The “IOT Based Door Access Control Using Face Recognition” paper discusses the same problem which is faced by the traditional security systems because they make use of various authentication procedures such as keys, identification (ID) cards or passwords to access the properties which need to be secured. Such authentication procedures can easily be manipulated or compromised by anyone with the intention of damaging the property or stealing sensitive information. However, to tackle all these problems, this paper proposes a security system which makes use of face detection and recognition in order to provide an improved and advanced version of door security to sensitive locations [5].

“Sure-H: A Secure IoT Enabled Smart Home System” is a security system that made use of PIR sensors in order to detect any intrusion attempt and alert the owner of the property through the Blynk Mobile Application which is connected to the Blynk Cloud. This application is also used to control the system. The main aim of this system is to reduce the power consumption which is necessary to reduce the overall working cost of the system, making it not just affordable to install, but also to use for a long period of time. This system is remotely controlled, because of which it reduces the manual effort. It is also highly scalable and resists against man-in-the-middle and online dictionary attacks. This system provides all these features while requiring minimum infrastructure [6].

The “Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things” proposes a museum anti-theft security system which is based on the IoT technology and is used to identify whether the artifacts present in the museum are within a safe range by making use of a Passive Radio Frequency Identification (RFID) Reader/Writer. If any artifact leaves the effective RFID identification range, the system detects the same and immediately triggers an alarm to alert the authorities regarding the theft. The main drawback of this system is the fact that it cannot protect the artifacts from any intentional or unintentional damages caused by the general public visiting the museum. Also, it does not generate any kind of warning in order to alert the visitors if they come too close to the artifacts. This system only generates an alarm if an artifact is moved from its original position, but cannot detect any form of motion and provide an early warning regarding the theft attempt [7].

The “Study on Face Recognition Techniques” discusses various face recognition methods, in which a general procedure is followed including the application of a face recognition technique in order to obtain the image which will be used for the process of face detection, after which the face is aligned and all the features of the face are extracted and are matched with the database of enrolled users to find a match. If a match is found, the user is successfully authorized [8]. Similarly, the paper “Face Detection and Recognition System using Digital Image Processing” mentions 2 separate methods of face detection and recognition wherein the process of face detection reads the geometry of the face and converts it into a set of points which are plotted in a grid and are then transferred to a database as an algorithm of numbers, which is stored as a unique Face ID by the application. This Face ID is used in the process of mapping an individual’s details and their ID is created in the database. This Face ID is then made use of in the process of face recognition of a newly captured image in order to authenticate the user [9].

III. Comparative Study

A. Comparison between various Arduino Boards

TABLE I
Arduino Boards [2]

Sr. No.	Board Name	Processor Type	Clock Speed	Digital I/O	Analog Inputs	PWM
1.	Uno	ATmega328P	16 MHz	14	6	6
2.	Mega	ATmega2560	16 MHz	54	16	15
3.	Due	ATSAM3X8E	84 MHz	54	12	12
4.	Yun	ATmega32U4	16 MHz	20	12	7
		AR9331 Linux	400 MHz			
5.	Nano	ATmega168	16 MHz	14	8	6
		ATmega328P				
6.	Leonardo	ATmega32U4	16 MHz	20	12	7

B. Difference between Raspberry Pi and Arduino

TABLE II
RASPBERRY PI VS. ARDUINO [4]

Sr. No.	Parameter	Raspberry Pi 3 Model B	Arduino Mega 2560
1.	System	Microprocessor	Microcontroller
2.	Storage	Micro SD Card	Onboard Storage
3.	Power Consumption (Idle State)	1.4 Watt	0.27 Watt
4.	Real Time Operation	Slower	Faster
5.	GPIO Pins	26	54

C. Comparison between various Motion Sensors

TABLE III
VARIOUS MOTION SENSORS [2]

Sr. No.	Sensor Name	Sensitivity Range	Trigger Condition	Measurement Angle	Sensing Type	Ambient Temperature
1.	PIR	7 m	Temperature Change	100°	Projection Area	Dependent
2.	Ultrasonic	2-4 m	Movement	15°	Line Direction	Independent
3.	IR	2-30 cm	Movement	35°	Line Direction	Dependent
4.	Microwave	5-9 m	Movement	360°	Projection Area	Independent

D. Difference between Keypad Lock and Face Recognition Lock

TABLE IV
KEYPAD LOCK VS. FACE RECOGNITION LOCK [4], [5]

Sr. No.	Keypad Lock	Face Recognition Lock
1.	Key press access	Touch less access
2.	Need to remember pass code	No need to remember pass code
3.	Pass code needs to be shared with valid entrants	No need of sharing any pass code
4.	Less secure as anyone with the pass code can access the property	More secure as valid entrants are registered in the system and need to be physically present to access the property

IV. REQUIREMENTS

A. Hardware Tools

1) Arduino Mega 2560: The Arduino Mega 2560 is a microcontroller board which is based on the ATmega2560. This board has a total of 54 digital input/output pins, with 15 pins that can be used as Pulse Width Modulation (PWM) outputs, 16 analog inputs, 4 UARTs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. The Arduino Mega 2560 is programmed using the Arduino Software (IDE), an Integrated Development Environment common to all Arduino boards which runs both online and offline. In order to power it, it simply needs to be connected to a computer with a USB cable. It can also be powered up using an AC-to-DC adapter or battery [10].

2) Ultrasonic Sensor: An ultrasonic sensor is a device that is used in order to measure the distance of an object by the emission of ultrasonic sound waves. The sensor detects the reflection of these sound waves and converts them into electrical signals [11]. Ultrasonic sensors have two main components. The descriptions of those are as follows:

a) Emitter: The emitter is that part of the ultrasonic sensor which emits the ultrasonic waves. These waves are produced using piezoelectric crystals.

b) Detector: The detector is that part of the ultrasonic sensor which receives the reflected sound waves after they have travelled to and back from the target.

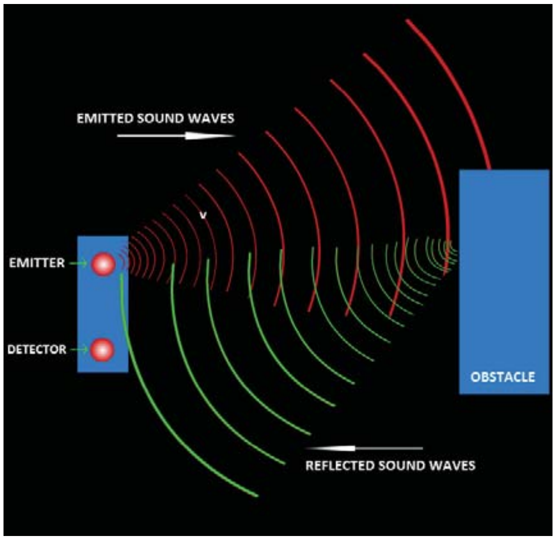

Fig. 2. Working of Ultrasonic Sensor [11]

3) NodeMCU ESP8266: The NodeMCU ESP8266 development board comes with an ESP-12E module containing an ESP8266 chip having Tensilica Xtensa 32-bit LX106 RISC microprocessor. This microprocessor supports Real Time Operating Systems (RTOS) and operates at 80 MHz to 160 MHz adjustable clock frequency. The NodeMCU has 128 KB of RAM and 4 MB of Flash memory in order to store data and programs. The high processing power of NodeMCU with in-built WiFi/Bluetooth and Deep Sleep Operating features makes it ideal for IoT projects. NodeMCU can be powered using a Micro USB jack and VIN pin (External Supply Pin). It supports I2C, SPI, and UART interfaces. The NodeMCU Development Board can be easily programmed and configured with Arduino IDE because it is easy to use [12].

4) Bolt WiFi Module: Bolt is an IoT platform that helps enterprises and makers to connect their devices to the Internet. Bolt comes with a WiFi/GSM Chip to connect various sensors to the Internet. It is an easy interface to quickly connect your hardware to cloud over GPIO, UART and ADC. Also, it connects to MODBUS, I2C and SPI with an additional converter. Bolt is equipped with industry standard protocols in order to ensure a secure and fast communication of your device data with the cloud. It also has built-in safeguards in order to secure all the user data from unwanted third-party intrusions. Bolt enables it's users to deploy machine learning algorithms with a few clicks. Bolt's alert system provides a feature of sending the information directly to a phone number or E-mail ID. These contact details can be configured and the alert conditions and thresholds can be set [13].

5) ESP32-CAM: The ESP32-CAM is a low cost development board with the ESP32-S chip consisting of a WiFi camera. It allows creating IP camera projects for video streaming with different resolutions. The ESP32-CAM has a built in PCB antenna. Besides the OV2640 camera, and several GPIOs to connect peripherals, it also features a microSD card slot that can be useful to store images taken with the camera or to store files to serve clients. However, the ESP32-CAM does not come with a USB connector, hence an FTDI programmer is required in order to upload code through the U0R and U0T pins (serial pins) [14].

B. Software Tools

1) Arduino IDE: The Arduino Integrated Development Environment (IDE) is a cross-platform application that is written in functions from C and C++. It is used to write and upload programs to not only Arduino compatible boards, but also, with the help of third-party cores, to other vendor development boards. The Arduino IDE is commonly used in various projects for IoT because of being flexible enough to program various development boards. Using special rules of code structuring, the Arduino IDE supports the languages C and C++. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures [15].

2) Blynk Mobile Application: Blynk is a platform which was designed for the Internet of Things. It can control hardware remotely, it can display and store data and can also visualize it. The Blynk platform consists of 3 major components, namely, the Blynk Mobile Application, the Blynk server and the Blynk libraries. Blynk works over the Internet, which implies that the hardware used should be able to connect to the internet. Some of the development boards, like Arduino Uno will need an Ethernet or WiFi Shield to connect to the internet, while some others are already Internet-enabled, like the NodeMCU ESP8266. The Blynk Application is mainly used in order to build the interface that will be used by the users of the system [6], [16].

3) Bolt Mobile Application: The Bolt mobile application has been specially designed in order to make use of in various IoT projects. This application acts as an interface between the Bolt WiFi module and the Bolt cloud. It establishes a connection between the Bolt WiFi module and the Bolt cloud by connecting it to the internet through a Home access point. It can be used to control various functionalities of the Bolt cloud and also to configure various Bolt devices.

4) Bolt Cloud: Bolt offers a cloud platform and a WiFi module. The Bolt cloud, directly and via Application Programming Interfaces (API), allows the storing of data, running analytics on it, and visualizing the data in the form of graphs. Alerts can be sent via E-Mail and SMS when the measured values of the data cross pre-decided thresholds. The Bolt cloud also supports a powerful dashboard for device management as well as online configuration and a code editor. This enables quick prototyping of IoT use cases which allows users to connect simple hardware and graph their data almost instantly. Bolt also allows users to quickly run Machine Learning Algorithms to make predictions on the data as well as detect anomalies. The Bolt Cloud API provides an interface for communication between the Bolt devices and any third party system e.g. mobile application, python programs, web server etc. This API contains an intuitive control and also has monitoring, communication and utility functions for the Bolt Devices connected to your account [17].

5) Twilio: Twilio is a third party SMS and call service provider. It is a cloud communication platform as a service company (PaaS). Twilio allows software developers to make and receive calls and send and receive messages using web application APIs. The Twilio Messaging API makes it easy to send and receive SMS and MMS messages as well as query meta-data about messages such as delivery status, compatible media, and help tools like Copilot to manage your messages globally. Twilio's Voice API makes it easy to make calls, retrieve, control and monitor calls. Using this REST API, it is possible to make outgoing calls, change ongoing calls, and query metadata about calls [18].

V. System Architecture

A. Block Diagram

Fig. 3 shows the block diagram consisting of all the components of the proposed system.

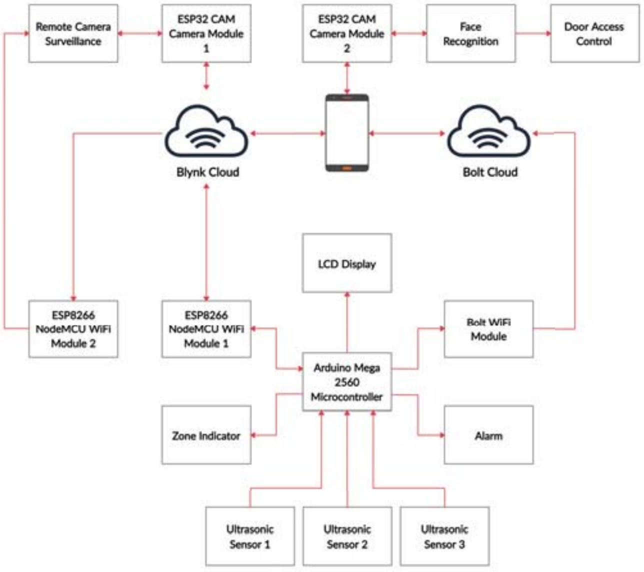
Remote Camera Surveillance
ESP32 CAM Camera Module 1
ESP32 CAM Camera Module 2
Face Recognition
Door Access Control
Blynk Cloud
Bolt Cloud
LCD Display
ESP8266 NodeMCU WiFi Module 2
ESP8266 NodeMCU WiFi Module 1
Bolt WiFi Module
Arduino Mega 2560 Microcontroller
Zone Indicator
Alarm
Ultrasonic Sensor 1
Ultrasonic Sensor 2
Ultrasonic Sensor 3

Fig. 3. Block Diagram

B. Process Model Specification

Fig. 4 shows the process model specification which defines the modes of operation of the proposed system.

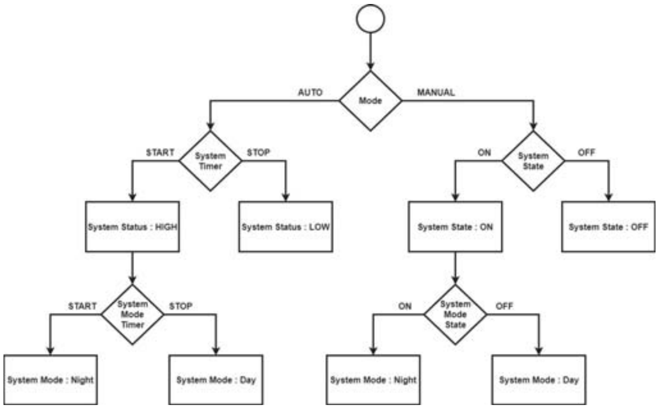

Fig. 4. Process Model Specification

VI. Proposed Work

The main objective of the proposed system is to offer various security features including day and night modes with different detection ranges, remote camera surveillance, power failure detection, alerts through various mediums such as call, SMS and E-mail, intrusion logging and face recognition technology for user authentication.

The system is mainly divided into two subsystems. Their functionalities and modules are as follows:

A. Perimeter Intrusion Detection System (PIDS)

A PIDS can be defined as a device that is used in order to detect the presence of an intruder attempting to break into the physical perimeter of a property, building, or other any other secured area. This system acts as an early warning system and alerts the alarm system which is installed on the site while the intruder is still at the perimeter and has not yet entered into the secured area or any other interior area. The modules of the PIDS are as follows:

1) Zone Barrier Module: The Zone Barrier Module provides 2 modes of detection. They are as follows:

a) Day Mode: In the day mode, the system will have 4 zone barriers - red, orange, yellow and green, in order to warn trespassers entering the surroundings of the secured property. The green zone indicates that there is no person in the vicinity of the property. If any person enters the yellow or orange zones by mistake, they will be alerted in advance, so that they can step back in time. However, if they do not step back and enter the red zone, the owner of the property will be alerted through SMS, call or E-mail and an on-site alarm will go off alerting the locals about the intrusion as well. For the purpose of motion detection, a combination of multiple ultrasonic sensors will be used. Also, the intrusion instance is logged into the Blynk mobile application, so that the data can be accessed by the owner anytime.

b) Night Mode: In the night mode, there exists only 1 zone - the red zone, with increased detection coverage, which is equivalent to the area of all the four zones provided in the day mode. This mode eliminates the early warning functionality and treats all instances of trespassing as intrusions which are considered as a threat to the secured property. The features remain the same as the features provided by the red zone in the day mode.

2) Remote Camera Surveillance Module: Another additional feature of the system is its surveillance capability, which allows the owner to start a live monitoring of the surrounding of the secured property, using an ESP32-CAM mounted on a pan and tilt camera mount. The angle of monitoring along the horizontal and vertical axes can also be controlled by the owner remotely so that the entire surroundings can be captured properly using minimum number of cameras.

3) Power Failure Detection Module: A unique feature provided by the proposed system is its capability to detect power failures by making use of the Bolt WiFi Module. If any person tries to power off the system in order to gain access to the secured property or the system loses power due to a power cut-off, the system will detect this power failure and send an alert, in the form of a call to the owner, made using the Twilio communication APIs, in order to make it known to the owner that the system is deactivated and will now not be able to detect any intrusion attempts. This enables the owner to take the appropriate actions concerning the security of the property in time. The system also has an additional capability to remember the status of the system when it last lost power. So when the power returns, the system reads the past status from the Blynk server through a NodeMCU ESP8266 Module, in order to resume functioning in the same mode.

Fig. 5 shows the Data Flow Diagram (DFD) of the PIDS.

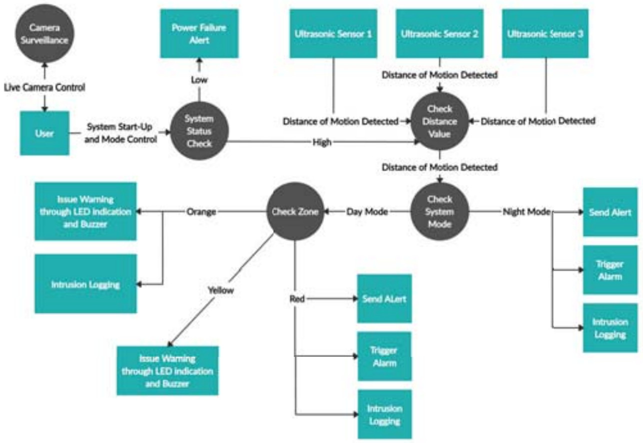

Fig. 5. DFD for PIDS

B. Face Recognition System

The proposed system also has the capability of face detection and recognition, which is provided through an ESP32-CAM Module. The system will first collect the images of the owner and all the other valid entrants who are allowed to enter the secured property or area, and as soon as a person approaches the entrance to enter the property, an image of the person will be captured and compared with the valid entrants to find if the person is a valid entrant or not. If the person is a valid entrant, the system will grant them an access to the property or area. However if the person is not a valid entrant, their access to the property will be restricted. In this process, the MTMN and FRMN models will be used for face detection and face recognition respectively.

Fig. 6 shows the DFD of the face recognition system.

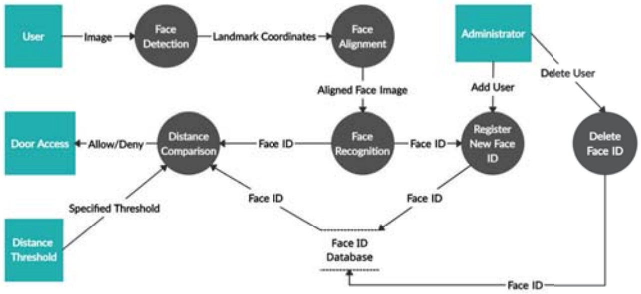

Fig. 6. DFD for Face Recognition System

VII. Applications

All the features of the proposed system when combined create a flexible and reliable security system which can be scaled up or down for use in various properties such as:

A. Homes

The proposed system can be made use of in order to protect homes from intruders, because it provides security to the perimeter of the house by customizing the installation of PIDS according to the boundaries of the house. At the same time, the face recognition system can be installed at the main entrance of the house, so that it can be used to unlock the door in order to allow access to the residents of the house.

B. Offices

The proposed system can also be used in offices in order to provide security to various sections of the office such as private cabins, electrical fuse boxes and server rooms from intruders, using the PIDS. The access to these secured areas can be controlled using the face recognition system, which will only allow the valid entrants to access their respective areas.

C. Museums

The proposed system can also be made use of in museums, by using it in place of traditional security measures such as physical barriers. This system serves many purposes, such as providing warnings to visitors if they are too close to artifacts and also alerting the security if a person does not pay attention to the warning and comes closer in order to cause damage to the artifacts. The remote camera surveillance feature can also be used in order to monitor the crowd in the museum, so as to avoid any mishaps. The face recognition system can be installed near the entrance of the areas which contain artifacts which are not to be accessed by the general public, so that such artifacts can be protected from any intruders.

VIII. Conclusion

Thus after an in-depth study of the previously available security systems, we have found out all of their important features along with their advantages and disadvantages and used this knowledge in order to propose an IoT based smart security and surveillance system, which is highly flexible and scalable and can be used to secure areas like homes, offices, museums or any other important commodities such as money, jewellery, artifacts and so on.

The proposed system provides various features such as zone barriers, facial recognition, remote camera surveillance and power failure detection all in one. It also provides the feature of intrusion logging so that the data about intrusions can be accessed by the owner of the secured property anytime and anywhere. All these features allow the owner to be worry free when it comes to the security of their property.

References

[1] [Online]. Available: https://safeatlast.co/blog/burglary-statistics/#gref

[2] Q. I. Sarhan, ”Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform,” in IEEE Access, vol. 8, pp. 128362-128384, 2020, doi: 10.1109/ACCESS.2020.3008610.

[3] [Online]. Available: https://codeforbillion.blogspot.com/2017/10/evolution-of-internet-of-thingsiot.html

[4] J. Kumar, S. Kumar, A. Kumar and B. Behera, ”Real-Time Monitoring Security System integrated with Raspberry Pi and e-mail communication link,” 2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence), Noida, India, 2019, pp. 79-84, doi: 10.1109/CONFLUENCE.2019.8776971.

[5] A. Nag, J. N. Nikhilendra and M. Kalmath, ”IOT Based Door Access Control Using Face Recognition,” 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, 2018, pp. 1-3, doi: 10.1109/I2CT.2018.8529749.

[6] R. Sarmah, M. Bhuyan and M. H. Bhuyan, ”SURE-H: A Secure IoT Enabled Smart Home System,” 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 59-63, doi: 10.1109/WF-IoT.2019.8767229.

[7] Z. Liu, M. Wang, S. Qi and C. Yang, ”Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things,” in IEEE Access, vol. 7, pp. 111387-111395, 2019, doi: 10.1109/ACCESS.2019.2933236.

[8] M. Sahu and R. Dash, ”Study on Face Recognition Techniques,” 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0613-0616, doi: 10.1109/ICCSP48568.2020.9182358.

[9] G. Singh and A. K. Goel, ”Face Detection and Recognition System using Digital Image Processing,” 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 348-352, doi: 10.1109/ICIMIA48430.2020.9074838.

[10] [Online]. Available: https://store.arduino.cc/usa/mega-2560-r3

[11] [Online]. Available: https://www.fierceelectronics.com/sensors/what-ultrasonic-sensor

[12] [Online]. Available: https://components101.com/development-boards/nodemcu-esp8266-pinout-features-and-datasheet

[13] [Online]. Available: https://www.boltiot.com/

[14] [Online]. Available: https://randomnerdtutorials.com/esp32-cam-video-streaming-face-recognition-arduino-ide/

[15] [Online]. Available: https://en.wikipedia.org/wiki/Arduino_IDE

[16] [Online]. Available: https://docs.blynk.cc/

[17] [Online]. Available: https://docs.boltiot.com/docs/introduction

[18] [Online]. Available: https://www.twilio.com/docs/api