IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

SMART INTRUDER DETECTION USING IOT AND REAL-TIME OBJECT DETECTION

#1SHAHJAHAN, #2P.PRABHAKAR, #3G LAVANYA
Assistant Professor, Department of ECE, Trinity College Of Engineering And Technology, Peddapalli, Telangana.

ABSTRACT: Smart security systems increasingly use video surveillance. Due of their ability to promptly alert authorities if someone breaks the law or enters sensitive areas without permission. Deep learning and IoT are presented for a new intrusion detection system. Our proposed approach tracks the object's center of mass to determine entrance after applying the "You Only Look Once" (YOLO) method to find things. Remote siren systems can detect intruders, alert authorities, and enable response. SORT is also constantly monitoring this person. The NVIDIA Jetson TX2 programming tool builds and tests the real-time video transmission system. The average frame rate is 30, and it works 97% of the time. The intrusion detection system (IDS) should be adaptive so the user can pick between the reference frame that specifies the region of interest's dimensions and form and the data-free area. The system's pre-trained object classes can also identify people, cars, and animals as threats. Thus, it protects farms, cars, guests, and smart homes from animals in smart cities.
Keywords: Deep learning, intrusion detection system, IoT, Cloud, transfer learning, smart city.

I. INTRODUCTION

Real-time Internet of Things (IoT) intrusion detection is the process of rapidly identifying security vulnerabilities by utilizing IoT sensors and devices. Traditional security systems are reliant on human touch and manual surveillance, which can result in a lengthy and ineffective process for identifying and preventing security hazards. Conversely, intrusion monitoring systems that are based on the Internet of Things (IoT) endeavor to promptly identify and prevent intrusions. Using a combination of sensors, algorithms, and machine learning, these systems are perpetually monitoring their surroundings for indications of an attack. Individuals have the ability to implement intrusion tracking devices that are IoT-based in public areas, as well as in their residences, offices, and enterprises. These systems are capable of identifying a wide range of attacks, including those that are permissible. A network assault is the term used to describe the act of obtaining tools or data without authorization. Finally, real-time intrusion tracking systems that are based on the Internet of Things (IoT) enhance the security and safety of both individuals and businesses by identifying security hazards more promptly and precisely.

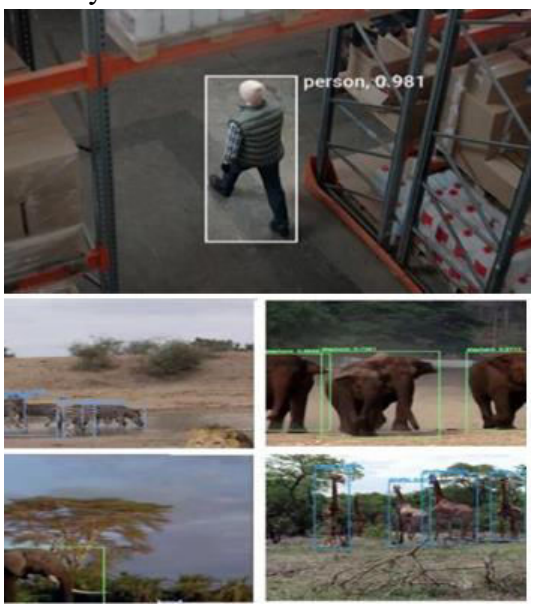

Fig 1, Qualitative results of object detection using YOLO

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

Because of its deep learning foundation, YOLO is capable of rapidly and accurately identifying objects in video and image streams. The system records video feeds from the area under observation using webcams and other Internet of Things (IoT) devices. Next, YOLO examines the camera images in order to identify potential attackers. Tracking and locating numerous perpetrators simultaneously is feasible due to the real-time object identification capabilities of YOLO. When it detects what it believes to be an intruder, YOLO notifies the user via email, phone, or another compatible device. This allows them to halt any security breaches before they occur and react accordingly. Visual aids, such as videos or photographs of the assailants, may be incorporated into the warnings to facilitate their identification and capture. Real-time intrusion monitoring systems that are based on the Internet of Things (IoT) and the YOLO principle are an effective method for identifying individuals who may be attempting to gain entry. These systems could identify potential security vulnerabilities in real time and promptly notify users of the necessary actions to prevent damage or loss by analyzing 178 video feeds with YOLO's object recognition capabilities.

II.IMPLEMENATION

Hardware setup: The system's essential components must be assembled prior to the commencement of activities. Select, install, and configure the appropriate Internet of Things sensors and devices prior to connecting them to the Internet of Things platform.

Data gathering: Data is then collected from the cameras and After that, data is collected using cameras and other devices. The devices are configured to transmit data to the Internet of Things application whenever they detect movement or any other significant event.

Data preprocessing: After the data has been collected, it must be processed to eliminate any unnecessary information or noise. Filtering, segmentation, and other methods are among the numerous methods available to sanitize and separate the data for this purpose.

Object detection: Before the data is transmitted to the YOLO object recognition algorithm, it undergoes preprocessing. This enables the identification and placement of multiple items simultaneously.

Intrusion detection: The items discovered are investigated to determine whether they are unlawful or obstructions. By conducting a comparison with a specific set of known objects, machine learning identifies unusual phenomena.

Alerting system: The user or security staff are notified by the system when an intruder is detected through email, text message, or another predetermined method.

Data storage and analysis: The sensors and cameras collect data, which is subsequently recorded in a database for future analysis and utilization. This entails identifying areas of vulnerability, enhancing the system as a whole, and identifying attempts to exploit the system in a suitable manner.

System upkeep: In order to guarantee that the system functions properly, it is necessary to conduct maintenance on a daily basis. All of the following are components of maintenance: updating software, replacing hardware and sensors,

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

and monitoring the system continuously to identify any issues.

BLOCK DIAGRAM

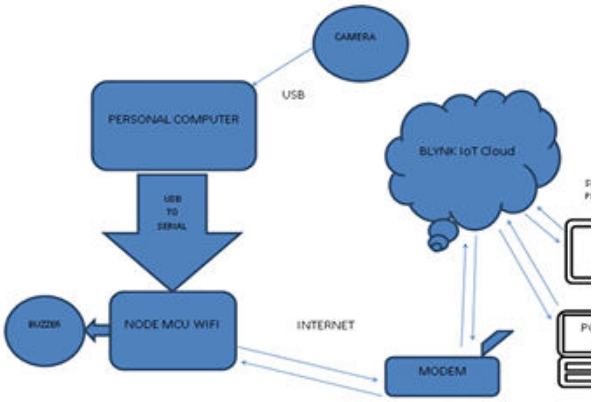

Fig 2 IoT Based intruder Detection using real time Object Detection

The block plan above illustrates the project's objective for our prototype system. As previously mentioned, this method is relatively inexpensive to implement. The standard components of a personal computer are being incorporated, as well as a camera interface. This will enable consistent monitoring to occur even when the system is not operational. This feature will also enable the system to emit a warning in the event that it detects unauthorized access, such as from individuals or animals. SMTP enables the transmission of images and the identification of objects in real time. Python, which enables the creation of program scripts, and YOLO, which I regard as a more potent CNN application, are responsible for the implementation of these features. Python IDLE is utilized to implement our instruments. This endeavor has enabled us to gain a deeper understanding of the inner workings of computers that are constrained by their capabilities. The system will detect individuals who are not authorized to be present in the subsequent phase of the research, and cloud communications will be integrated. The Node MCU is a hardware component that simplifies this task. This WiFi module, which is based on the esp8266 chip, establishes a rapid connection to the cloud and informs users of any modifications via email and other communication channels. It also enables users to activate the warning from a distance, thereby ensuring the safety of the area and deterring unknown intruders and animals. In conclusion, the development of an Internet of Things (IoT) system that can detect and notify of real-time intrusions through YOLO necessitates the use of dependable hardware, software, and data processing methods, as well as the assurance that all components can communicate and coordinate without any issues.

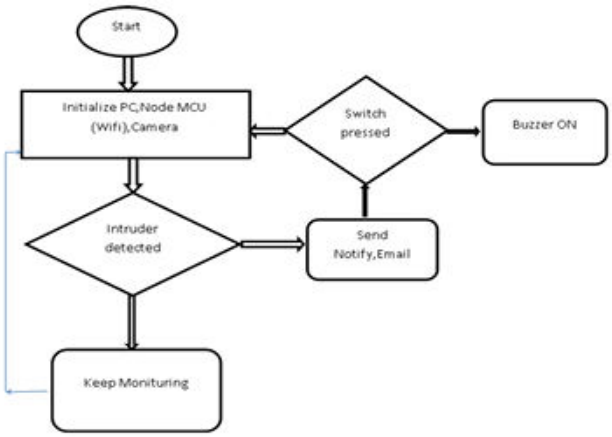

Fig 3 Detailed work Flow chart

III. HARDWARE REQUIREMENTS

ESP8266 D1 TINY NODE MCU:

Fig-4 Node Mcu D1 Mini

The ESP8266 D1 Mini NodeMCUWifi Development Board is a diminutive WiFi device. It is compatible with Arduino. It

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

contains the ESP8266EX chip and 4MB of Flash memory. Except for D0, the eleven digital input/output ports on the board are capable of controlling interrupts, PWM, I2C, and one-wire Micro USB connections. Additionally, there is a single analog connection that can handle a maximum voltage of 3.3V.

This is all the information you require regarding the Esp8266 D1 Tiny Node MCU WiFi Development Board...

- ESP-8266EX microcontroller
- Digital I/O Pins: 11 Analog Input Pins: 1 Operating Voltage: 3.3 V (Max input: 3.
- Clock Frequency 80/160 MHz
- 4M bytes of flash
- 34.2mm long by 25.6mm wide.

BUZZER

- Buzzer Features and Specifications
- Rated Voltage: 6V DC
- Operating Voltage: 4-8V DC
- Rated current: <30mA
- Sound Type: Continuous Beep
- Resonant Frequency: ~2300 Hz

IV. SOFTWARE REQUIREMENTS

PYTHON

In 2008, Python 3 replaces Python 2 as a high-level computer interpreter. It is capable of performing a variety of tasks, including the development of websites, data analysis, artificial intelligence, and scientific computing.

YOLO

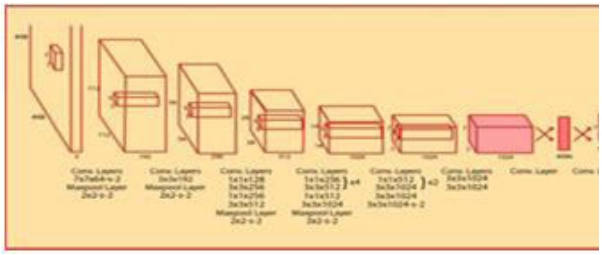

Fig 5 Network Layers

- Yolo is compatible with Windows, Linux, and macOS.
- A Python interpreter is required due to the fact that YOLO is typically written in Python.
- YOLO frequently employs Python utilities such as NumPy, Pillow, and matplotlib. These tools enable individuals to modify data, alter images, and gain a more comprehensive understanding of information.

BLYNK

Blynk provides a cloud-based environment for the development and administration of Internet of Things (IoT) applications. The objective is to eliminate the necessity for extensive hardware and software expertise in order to facilitate the development and administration of Internet of Things (IoT) applications by non-technical users and writers. Blynk users can establish connections to sensors and devices that are part of the Internet of Things (IoT) through a web-based control interface and a mobile app.

ARDUINO IDE

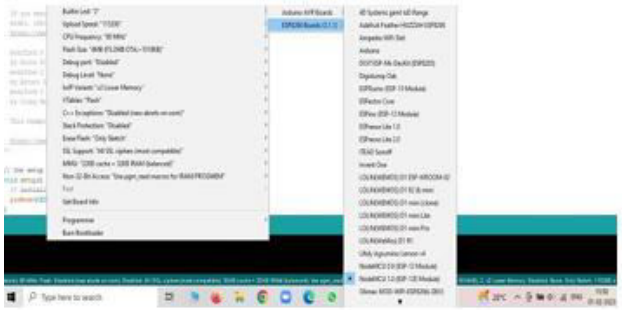

Fig-6 Arduino Ide Configuration for ESP8266 node mcuProgrammimg

1. Download the most recent version of the Arduino IDE from the official website and install it.
2. Assembling the containers for the ESP8266 board: If the Arduino Integrated Development Environment (IDE) is already open, navigate to the File menu and select Preferences. Enter

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

the following URL in the Other Boards Manager URLs field:

3. "https://arduino.esp8266.com/stable/package_esp8266com_index.json". The index.json file for the Arduino package is loaded at esp8266.com/stable, which is the URL that this URL points to. Navigate to Tools > Board > Boards Manager in order to locate and install the "esp8266" package. What is the best method for determining the type of ESP8266 device to purchase? Select the appropriate ESP8266 board, such as NodeMCU or Wemos D1 Mini2, from the Tools menu.
4. The Arduino IDE, which is built on the ESP8266 board, is a valuable resource for initiating Internet of Things (IoT) initiatives due to its extensive collection of code examples. Additionally, there are numerous free tutorials and instructions available to assist novices in programming the ESP8266 using the Arduino IDE.

V. RESULTS

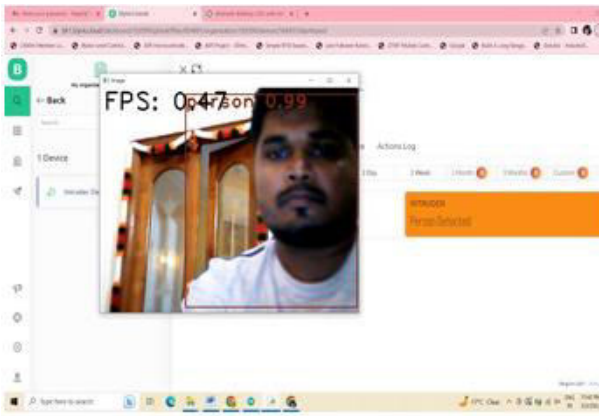

Fig-7 Intruder Detection and updating status to Cloud

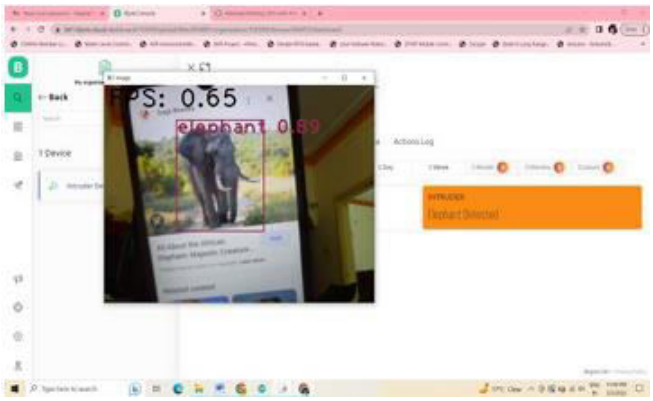

Fig 8 Other animal Intruder Detection using YOLO and updating status to Cloud

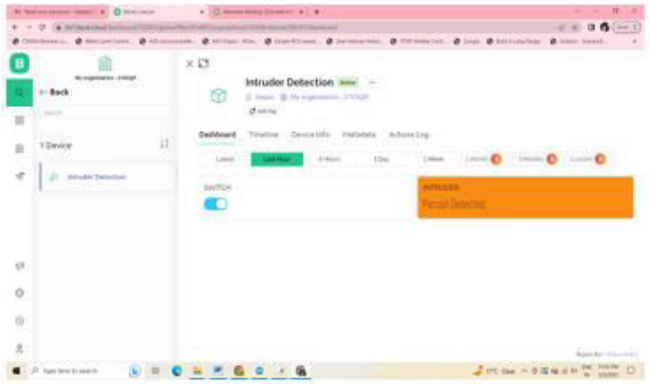

Fig 9 Alerting Buzzer to protect Area From intruder using Remote Switch from web or apk

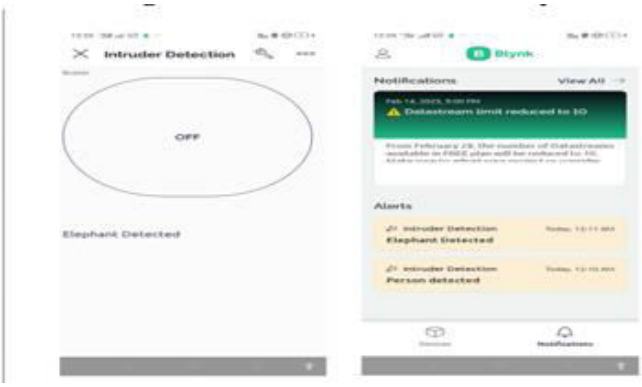

Fig 10 same application can be monitored using Smart phone with notification alerts

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 09, 2022

Fig 11 Hardware Setup for IoT integration using Node MCU and PC

VI CONCLUSION

Instantaneous intrusion tracking systems that are connected to the internet are becoming increasingly critical for the protection of residences, public spaces, and common areas. In these systems, a network of sensors, cameras, and other high-tech tools rapidly identify security violations and notify the authorities. Other advantages of these architectures include improved standard security, reduced false alarms, and speedier reaction times.

Nevertheless, the establishment, management, and operation of intrusion monitoring systems that utilize the Internet of Things (IoT) necessitate robust connections to other security systems. It is probable that intrusion tracking systems for the Internet of Things (IoT) will become more robust in the years ahead. In order to enhance their accuracy and utility, these systems will implement artificial intelligence and machine learning. In conclusion, these structures represent a significant advancement in security and will be critically essential in the future to ensure the safety of individuals. This configuration could be simplified by employing command boards that resemble Raspberry Pis and feature a Pi Camera interface.

REFERENCES

1. Adriano, Davin Bagas, and Wahyu ApsariCiptoning Budi. “IoT-based Integrated Home Security and Monitoring System.” In Journal of Physics: Conference Series, vol. 1140, no. 1, p. 012006. IOP Publishing, 2018.
2. Nico Surantha and Wingky R. Wicaksono. “An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients”. Journal of Computer Science 2019, 15 (8): 1108.1122
3. Radke, R.J.; Andra, S.; Al-Kofahi, O.; Roysam, B., "Image change detection algorithms: a systematic survey," Image Processing, IEEE Transactions on, vol.14, no.3, pp.294,307, March 2005.
4. Sampson, R, "False Burglar ". Retrieved April, 2014Available:http://www.cops.usdoj. gov/pdf/e 05021556.pdf.