IoT Based Intruder Detection Using Real Time Object Detection

Thejas A. V.[1], Dr.Kusumadhara S.[2], Dr.Bhagya H. K.[3]
[1]*M.tech, Digital Electronics and Communication, KVGCE, Sullia D.K, Karnataka, India*
[2]*M.tech, Ph.D, MISTE, MIEEE, E&C. Dept, Professor & Head KVGCE, Sullia D.K, Karnataka, India*
[3]*M.tech, Ph.D, MISTE ,E&C. Dept, Professor KVGCE, Sullia D.K, Karnataka, India*

***Abstract*-- There is a huge demand of video surveillance-based intelligent security systems which can automatically detect the unauthorized entry or mal-intentional intrusion into the unattended sensitive areas and notify to the concerned authorities in real time. A novel video-based Intrusion Detection System (IDS) using deep learning is proposed with IoT technologies. Here, the You Only Look Once (YOLO) algorithm is used for object detection and intrusion is decided using our proposed algorithm based on the shifted center of mass of the detected object and after detection of intrusion we can categorize the object and send a notification to IoT cloud and notify the concerned user and he can take actions using remote siren systems . Further, Simple Online and Real time Tracking (SORT) algorithm is used for the tracking of the intruder in real-time. The developed system is also implemented and tested for live video stream using NVIDIA Jetson TX2 development platform with an accuracy of 97% and average fps of 30. Here, the proposed IDS is a generic one where the user can select the region of interest (the area to be intrusion free) of any size and shape from the reference (starting) frame and potential intruders such as a person, wild animals, vehicle, etc. from the list of trained object classes. Hence, it can have a wide range of smart city applications such as person intrusion free zone, no vehicle entry zone, no parking zone, smart home security, protect agriculture land From wild Animals etc.**

Index Terms—Deep learning, intrusion detection system, IoT, Cloud, transfer learning, smart city, SORT algorithm, YOLO algorithm.

I. INTRODUCTION

IoT-based real-time intrusion detection is the process of detecting security breaches in real-time using Internet of Things (IoT) devices and sensors. Detecting and reacting to security threats can be sluggish and ineffectual with traditional security systems' reliance on manual monitoring and human interaction. Contrarily, IoT-based intrusion detection systems are built to instantly identify and address threats. These systems continually monitor the environment and look for any irregularities that could point to an intrusion using a mix of sensors, algorithms, and machine learning approaches. Systems for detecting intrusions that are IoT-based can be deployed in a range of locations, including residences, workplaces, industries, and public places. These systems may be modified to recognise many incursion types, including physical break-ins, Network attacks involve illegal access to data or devices. All things considered, IoT-based real-time intrusion detection systems offer a more effective and efficient approach to defend against security threats, helping to increase safety and security for people and businesses.

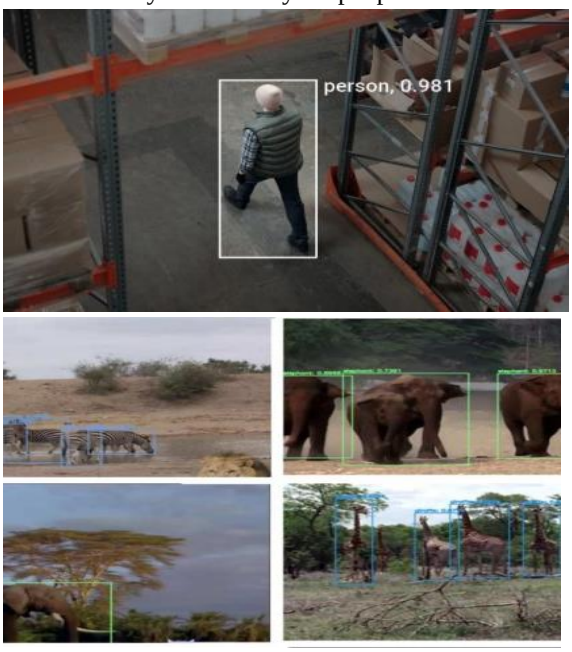

Fig 1, Qualitative results of object detection using YOLO

A deep learning algorithm called YOLO is able to quickly and accurately identify objects in picture and video streams. The system functions by capturing video feeds of the area being watched using cameras and other IoT devices. Next, YOLO examines the video streams to find any prospective invaders. Real-time object detection capabilities of YOLO allow for the simultaneous detection and tracking of several intruders. A warning is sent to the user's smartphone, email, or any other notification device when YOLO discovers a suspected intruder, allowing them to take rapid action to stop any security breaches. The warnings may also To help with identification and capture, attach pictures or video of the invaders.. In conclusion, YOLO-based IoT-based real-time intrusion detection systems provide an efficient technique to quickly identify possible attackers. These systems may identify possible security breaches in real-time by 178 ecognizi video feeds utilising YOLO's object identification capabilities, giving users must act quickly in order to stop any harm or loss..

PROBLEM STATEMENT

- Use the YOLO (You Only Look Once) object detection technique to implement an IoT-based system that can instantly identify and notify for intrusions.
- The system should employ sensors to detect any movement or breach in the monitored area (e.g., motion sensors, door sensors, etc.), and should then use the YOLO algorithm to pinpoint the object or objects that caused the incursion.
- The system ought to be able to 178ecognizi many items and distinguish between legitimate objects (such people, animals, etc.) and invaders (e.g., burglars, animals, etc.). When an intrusion is discovered, the system should also be able to instantly send an alarm or notice (such as an email, SMS, etc.) to the user or security employees.
- The system must be scalable and capable of alerting and monitoring. For simultaneous incursions in several places.
- Last but not least, the system should be created to be effective and economical, utilizing low-power IoT devices and reducing false alerts.

OBJECTIVES

- Real-time detection: The system must be able to identify any intrusion in real-time and notify the user or security staff right away.
- Accurate detection: The system must be able to 178ecognizi intruders and distinguish them from everyday items like people, pets, and other living things.
- Multiple object detection: The system must be able to identify and follow the motion of many objects at once.
- System for sending warnings: The system should be able to deliver notifications by email, SMS, and other channels.
- Scalability: The system must be built such that it may be expanded to simultaneously monitor several locations.
- Efficiency: To cut expenses, the system should be built to employ low-power Internet of Things devices and prevent false alerts.
- Flexibility: The system must be sufficiently adaptable to support many IoT platforms, sensor and camera kinds, and sensor types.
- User-friendly: The system should have an intuitive user interface and be simple to use and adjust.
- Cost-effectiveness: The system should be created in such a way that it can be implemented within the user's or organization's budget.
- Security: The system should employ encrypted communication channels and secure data storage to maintain user privacy and ensure system security.

II.IMPLEMENATION

- Hardware setup: The system's necessary hardware must first be configured. The right IoT sensors and devices must be chosen, installed, and configured before being connected to the IoT platform.
- Data gathering: Gathering data from the sensors and cameras is the next stage. In this case, the sensors are set up to detect motion or any other pertinent events, and the data is then sent to the IoT platform.
- Data preprocessing: When data has been gathered, it must be processed to eliminate noise and unimportant data. This entails cleaning and

segmenting the data using filters, segmentation, and other methods.

- Object detection: When the data has been preprocessed, it is run through the YOLO object detection algorithm, which Real-time detection and localization of several objects.
- Intrusion detection: The items that have been found are evaluated to see if they are legitimate objects or intrusive ones. Machine learning techniques are used to discover abnormal 179ecogniz by comparing the items to a database of known things.
- Alerting system: The system notifies the user or security staff through email, SMS, or any other configured channel if an intrusion is discovered.
- Data storage and analysis: For later analysis and usage, the data gathered by the sensors and cameras is saved in a database. This entails 179 ecognizing infiltration trends, pinpointing weak points, and enhancing the system as a whole.
- System upkeep: To make sure the system is functioning properly, it must be maintained on a regular basis operating properly. Maintenance include changing broken sensors and hardware, upgrading the software, and keeping an eye out for any irregularities in the system.

BLOCK DIAGRAM

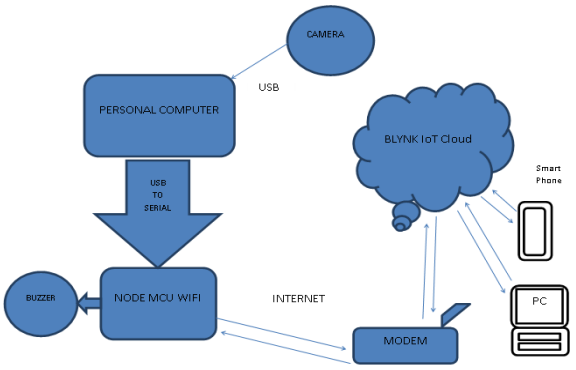

Fig 2 IoT Based intruder Detection using real time Object Detection

The above figure shows the working of our prototype system project objective block diagram as discussed at beginning of the introduction this system is achieved with low-cost implementation more over we are implanting a camera interface to a generic system so-called personal computer so that normal monitoring can be done in offline mode and system sound alerts can be created during intruders like person or animals detections this real-time object detection is achieved along with image capturing and sending to mail using SMTP these functionalities are archived with the combination of python for program scripting and yolo which I so-called advance module of CNN this YOLO are trained module weight file which is used as main classification module for our test frames which are inputted from the camera. the python IDLE is used for the deployment of our project and all this work explained what takes place inside the functionality boundary of the PC. The next part of the system is Integrating notifications during intruder detection to the cloud to achieve this we are using a hardware called Node MCU which is esp8266 based WIFI module that is used to integrate to cloud and achieve notifications, and emails to the user and also provide a buzzer activation control to users from the cloud and make the area safe from unknown intruders and animals. In conclusion, good hardware, software, and data processing approaches, as well as appropriate integration and communication between the various components, are all necessary for the construction of an IoT-based real-time intrusion detection and alerting system employing YOLO.

FLOW CHART

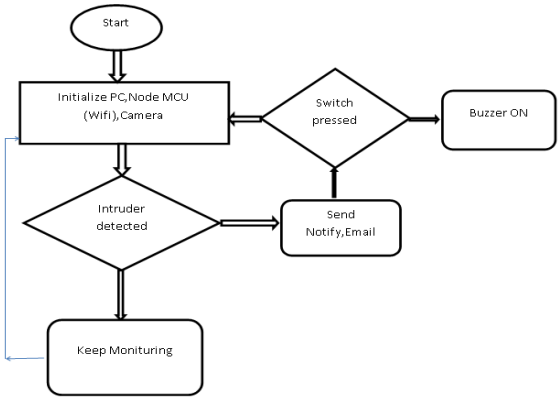

Fig 3 Detailed work Flow chart

III. HARDWARE REQUIREMENTS

ESP8266 D1 TINY NODE MCU:

Fig-4 Node Mcu D1 Mini

An Arduino Compatible Small WiFi Board with 4MB Flash, the ESP8266 D1 Mini NodeMCU Wifi Development Board is based on the ESP8266EX. The board has 11 digital input/output pins, all of which support interrupt, PWM, I2C, and one-wire (except D0) Micro USB connectivity and one analogue input (3.3V maximum input).

Esp8266 D1 Tiny Node MCU Wifi Development Board specifications:

- ESP-8266EX microcontroller
- Digital I/O Pins: 11 Analog Input Pins: 1 Operating Voltage: 3.3 V (Max input: 3.2V)
- 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

Test Python 3, a high-level, interpreted programming language that replaced Python 2, was made available in 2008. It is frequently used for creating websites, analysing data, using AI, scientific computing, and many other things.

YOLO

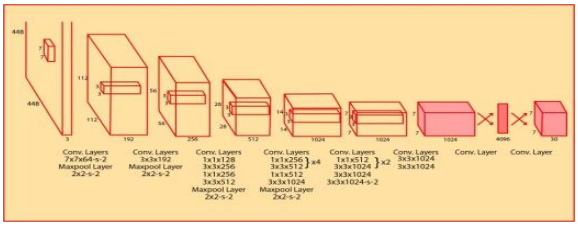

Fig 5 Network Layers

1. YOLO is compatible with Windows, Linux, and macOS.

2. Python: Python is generally used to implement YOLO; hence a Python interpreter is necessary.

7. Python libraries: Many Python libraries, including as NumPy, Pillow, and matplotlib, are frequently used with YOLO. Further capability for data processing, picture editing, and visualisation is offered by these packages.

BLYNK

An Internet of Things (IoT) platform called Blynk offers a cloud-based architecture for creating and overseeing IoT applications. It is intended to make the creation and deployment of IoT applications simple for developers and amateurs without having a deep understanding of hardware or software development.To communicate with IoT devices and sensors, Blynk offers a mobile app and a web dashboard.

ARDUINO IDE

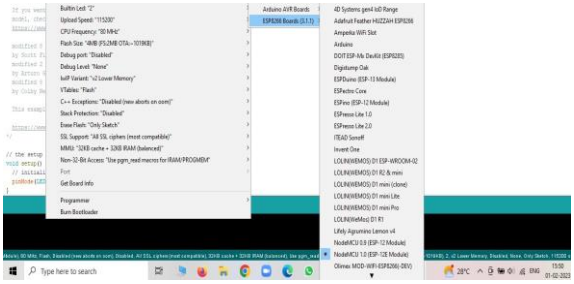

Fig-6 Arduino Ide Configuration for ESP8266 node mcu Programmimg

- Installing the Arduino IDE requires downloading and installing the most recent version from the Arduino website.
- Putting together the ESP8266 board package: Go to File -> Preferences in the open Arduino IDE. Provide the following URL in the Other Boards Manager URLs field: https://arduino.esp8266.com/stable/package esp8266com index.json. After that, install the package by searching for "esp8266" in Tools -> Board -> Boards Manager.
- ESP8266 board should be chosen: Choose the proper ESP8266 board, such as NodeMCU or Wemos D1 Mini, under Tools -> Board.
- It is simple to get started with IoT projects that use the ESP8266 chip since the Arduino IDE offers a variety of libraries and examples that can be used to programme the ESP8266 board. Other from that, there are a tonne of online guides and tutorials that may teach novices how to utilise the Arduino IDE to programme the ESP8266.

V RESULTS AND DISCUSSIONS

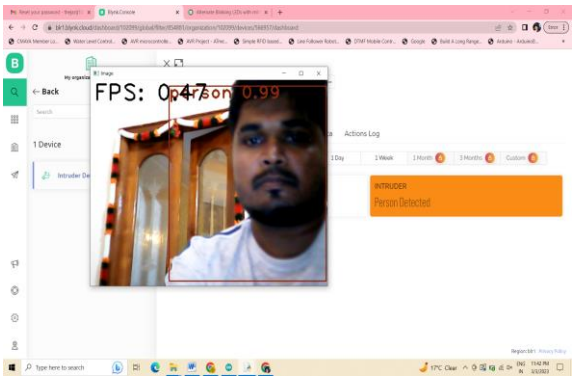

Fig-7 Intruder Detection and updating status to Cloud

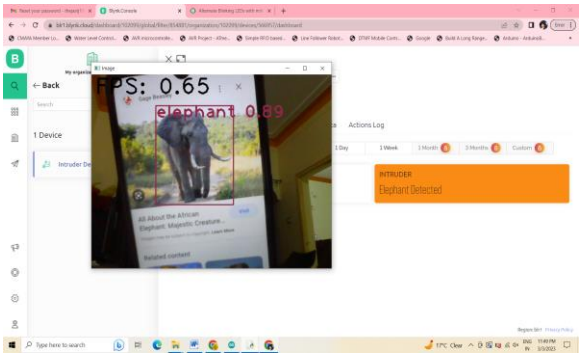

Fig 8 Other animal Intruder Detection using YOLO and updating status to Cloud

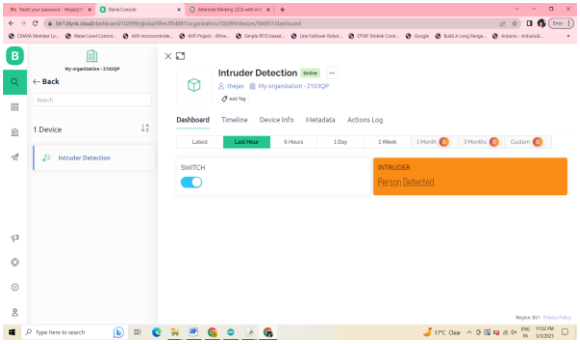

Fig 9 Alerting Buzzer to protect Area From intruder using Remote Switch from web or apk

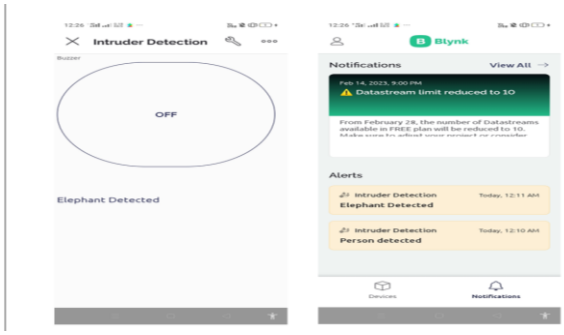

Fig 10 same application can be monitored using Smart phone with notification alerts

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

VI CONCLUSION

IoT-based totally actual-time intruder detection structures have emerge as an increasing number of important in making sure the safety of homes, groups, and public areas. By leveraging a network of sensors, cameras, and different smart gadgets, those structures can discover and alert government to ability protection breaches in real-time. The benefits of those structures are, together with progressed reaction instances, decreased fake alarms, and expanded standard protection.

However, the achievement of IoT-primarily based intruder detection systems relies upon on right set up, renovation, and management, as well as powerful integration with other safety systems. As the era keeps to advance, we can anticipate to look even more sophisticated IoT-based totally intruder detection structures that include gadget getting to know algorithms and synthetic intelligence to enhance their accuracy and effectiveness. Overall, these structures constitute an vital breakthrough in the field of security and are poised to play a vital role in ensuring public protection within the years to come also this system can be more compacted by using Raspberry pi like controller boards with pi cam interface.

REFERENCE

[1] Adriano, Davin Bagas, and Wahyu Apsari Ciptoning 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/e05021556.pdf.