ADAM Project D2 for CS370

Nathan Kopacz
Electrical Engineering, Colorado State University
Fort Collins, United States
ndkopacz+ADAM@gmail.com

Nikki Bauer
Computer Science, Colorado State University
Durango, United States
nbauer@colostate.edu

I. Status of Project

At this stage of our project, all hardware components have been assembled and are ready for use. The website interface, designed to connect with the camera and audio feeds, has also been created. We utilized the Adam Project logo, shown in Fig.1 and the theme is based on that. Our current focus is establishing communication between the camera feed and the website. We're working through challenges connecting a second remote computer via SSH to the Pi camera, troubleshooting is ongoing and has been our top priority. Both partners are now successfully connected to the OpenVPN, and we will continue working to SSH both computers into the device.

Below this section we left in the objective and expense report, underneath that you will find the hardware in addition to the attribute evaluations.

Fig. 1. ADAM Logo

II. Objective

The objective of ADAM is to develop an intelligent doorbell camera system with advanced threat detection capabilities. Leveraging real-time video processing and machine learning, ADAM will autonomously identify potential security threats and deploy a deterrent response to proactively protect homes and deter intruders. The project is designed around the concept of monitoring and detecting threats. It comes in the form of a raspberry pi enclosed in a 3D printed case with a servo that is able to actuate some form of deterrent.

III. Expenses

Table I below shows expenses already purchased and received for the project.

Future expenses may include: A GPU accelerator ($70.00), Google Coral ($60.00), and Hailo Pi AI Kit ($85.00).

TABLE I
Project Expenses

Component	Cost
Raspberry pi 5	$91.00
SD Card	$10.00
Pi Active Cooler	$8.00
Pi Power Supply	$13.00
Servo	$2.00
Pi Cam	$12.00
Ribbon Cable	$4.00
Mini Speaker	$3.00
Mini Microphone	$13.00
Standoff Kit	$13.00
PLA	$20.00
FOX Teargas Grenade	3 x $31.00
M2.5 Bolts Kit	$11.00
90 Degree USB C	$11.00
Total	$304.00

Images shown in Fig. 2 and Fig. 3 are of the finished physical project, both inside the box with the Raspberry Pi and shown on the wall mount where the camera feed will be captured.

IV. Selected Board

The board we will be using is the Raspberry Pi 5. This is a low cost board but has the ability to attach a PiHat AI Accelerator if we need a little bit more compute to run the NN. This board has been ordered from Amazon and already has been received (see Fig. 3). This was a relatively easy decision to make, but it still deserves some consideration. The Pi is able to Ubuntu, which will be flashed as the primary OS. Not only that, but there is a enormous community that exists already doing similar projects such as vision processing on this edge

device. We will be able to leverage this community to push past most roadblocks we may face.

V. Software and Documentation

Our project consists of a few core computational components: the scripts for peripheral control and the neural network (NN). The peripheral control scripts will be developed from scratch, while the NN will likely be implemented through transfer learning using a model like YOLO, sourced from Ultralytics. YOLO, which stands for "You Only Look Once", is a model for object detection in computer vision. The distinguishing feature of YOLO is that, unlike other models that carry out object detection in two steps (first identifying regions of interest, then classifying these regions), YOLO accomplishes both tasks in a single pass, hence the name "You Only Look Once". Thus, YOLO is one of the fastest methods for object detection, making it ideal for real-time applications. [1] The CNN works impressive on visual input for features' extraction as low-level features are efficiently propagated from the initial convolutional layers to later convolutional layers in a deep CNN. Herein, the challenge lies in the accurate identification of multiple objects along with their exact positioning present in a single visual input. [2]

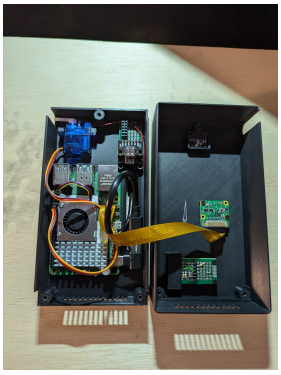

Fig. 2. Inside the box

Fig. 3. Box on wall mount

VI. Limitations

The first attribute of this project we will evaluate are limitations.

There are a few limitations to consider with an intelligent home security device. One of these being resolution. The resolution of the pi cam likely will be lower because it has to be accepted by YOLO. With lower resolution, this can impact the accuracy of detection. Accuracy will also be measured as the accuracy of the model tested on our test dataset that we create. The integration of AI and machine learning technologies is gradually enhancing capabilities of surveillance systems, [3] however a lower-resolution image could impact these capabilities.

Response time is also a limitation and relies on YOLO capacity for the time it takes for a forward pass and how long it takes the data to be loaded into the model. It will take between 3-5 cycles of YOLO since we are doing 3-5 hits on our tracker to activate the device. The performance of YOLO could also be a limitation. In this research, two models of YOLO were tested against eachother on the same datasets. Each model was trained for 20 epochs, with an input size of 320×320 pixels. YOLOv8 achieved a mean average precision (mAP) of 84.9%, demonstrating a considerable increase in its object detection capabilities compared to YOLOv5, which only managed to obtain a 64.2% mAP. [1] We will have to take into account the trade-off between speed, accuracy, and capability between the YOLO we work with and the resolution of our images from the pi camera. In another research of YOLOv3, the accuracy was found to be better on small objects in comparison to other YOLO versions. The model's average accuracy value came out to be 85.6%. Accuracy refers to how precisely the model can categories items. In terms of recall, the model achieved an average value of 86.6%, which also points to its consistency in classification [4].

These limitations could cause false positives and risk flagging a normal activity as suspicious, or vice versa.Finding a balance between reducing false positives and false negatives is one of the main issues faced by intrusion detection systems. [5] Various methods to determine abnormal behavior for intelligent video surveillance systems that focus on recognizing abnormal behavior have been widely discussed [3]. Enhancing the accuracy of these systems is crucial for improving security and trust in automated monitoring technologies. With the Adam project, we hope to train an accurate model and find a YOLO implementation that works concurrently with our image quality and speed requirements.

VII. Security Holes

The second attribute of our project we are discussing are the potential security holes and how they can be mitigated. As with any surveillance device, there are concerns about what the camera captures and who has access to this footage. For this device specifically, the goal is to provide a deterrent that users can activate in response to an intruder or suspicious activity. This can be especially dangerous if malicious activity were to occur, making security measures essential. A recent study showed that 40.3% of smart homes worldwide had five or more devices connected to the internet, and that 40.8% of homes had at least one vulnerable device that puts the entire home at risk [6]. This is an alarming percentage and needs to be considered when looking at security measures.

Internet of Things (IoT) devices use different types of media and protocols to communicate to Internet. Unfortunately, security can be compromised if devices do not implement encryption, authentication, and data integrity measures [7]. Using OpenVPN in conjunction with the Raspberry Pi can help prevent against malicious activity. In order to access the Pi remotely, a user has to be connected to the VPN with the given client configuration file. The VPNoT device is an IoT solution that uses an encrypted tunnel to enable secure access to the IoT Server from devices equipped with sensors [7].

If an unauthorized individual were to access our device, they could potentially activate the deterrent and monitor the

surrounding area, creating a significant privacy risk, especially if the camera is located indoors. To mitigate this, in addition to the OpenVPN, we would use additional user authentication mechanisms to make sure only specified users can activate the deterrent.

Lounis and Zulkernine [8] developed a taxonomy of attacks targeting Wi-Fi, Bluetooth, ZigBee, and Radio Frequency Identification (RFID) infrastructures, along with a comprehensive survey of specific assaults on each network technology. Their findings show that many attacks exploited vulnerabilities in authentication protocols. For example, some motion sensor and home-surveillance cameras transmit unencrypted information, making it relatively easy for hackers to know when users are home based on the motion sensors' state. Further results indicated that 26% of Hypertext Transfer Protocol Secure (HTTPS) servers were susceptible to Man-in-the-Middle (MITM) attacks, with weak SSL configurations compromising the integrity of the Transmission Layer Security (TLS) ecosystem [6].

In order to mitigate these security risks, our solution will require OpenVPN for any connected devices to ensure a secure connection. Additionally, we will implement user authentication to access the camera feed, with an added layer of authorization for users with permission to activate the deterrent. This layered security approach is aimed to protect both the device and user privacy to the fullest extent.

REFERENCES

[1] J. Da Silva, T. Flores, S. Júnior, and I. Silva, "Tinyml-based pothole detection: A comparative analysis of yolo and fomo model performance," in *2023 IEEE Latin American Conference on Computational Intelligence (LA-CCI)*, 2023, pp. 1–6.

[2] T. Diwan, G. Anirudh, and J. V. Tembhurne, "Object detection using yolo: challenges, architectural successors, datasets and applications," *Multimedia Tools and Applications*, vol. 82, no. 6, pp. 9243–9275, 2023. [Online]. Available: https://doi.org/10.1007/s11042-022-13644-y

[3] M. F. Nuryasin, C. Machbub, and L. Yulianti, "Abnormal event behavior detection for home surveillance cameras system," in *2023 IEEE 13th International Conference on System Engineering and Technology (ICSET)*, 2023, pp. 7–11.

[4] H. Hashmi, R. Dwivedi, and A. Kumar, "Yolo-rs: An efficient yolo-based approach for remote sensing object detection," in *2023 12th International Conference on System Modeling Advancement in Research Trends (SMART)*, 2023, pp. 50–56.

[5] A. Darbar, A. S. Krishna Reddy, P. V. Sai Neela Lohith, P. S. Kumar, and R. Kumar Tata, "A study on automating sos alerts for unauthorized access detection and home security," in *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, 2024, pp. 524–527.

[6] N. M. Allifah and I. A. Zualkernan, "Ranking security of iot-based smart home consumer devices," *IEEE Access*, vol. 10, pp. 18 352–18 369, 2022.

[7] C. A. Romero Goyzueta, J. E. Cruz De La Cruz, and C. D. Cahuana, "Vpnot: End to end encrypted tunnel based on openvpn and raspberry pi for iot security," in *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2021, pp. 1–5.

[8] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for iot," *IEEE Access*, vol. 8, pp. 88 892–88 932, 2020.