Weapons Detection System Based on Edge Computing and Computer Vision

Zufar R. Burnayev[1], Daulet O. Toibazarov[2], Sabyrzhan K. Atanov[3], Hüseyin Canbolat[4], Zhexen Y. Seitbattalov[5], Dauren D. Kassenov[6]

Department of Social Disciplines and Pedagogy, The National Defence University named after the First President of the Republic of Kazakhstan - Elbasi, Astana, Kazakhstan[1]

Department of Arms and Military Equipment Research, The National Defence University named after the First President of the Republic of Kazakhstan - Elbasi, Astana, Kazakhstan[2]

Department of Computer and Software Engineering, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan[3, 5]

Department of Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Ankara, Turkey[4]

Department of Education and Science, Ministry of Defense of the Republic of Kazakhstan, Astana, Kazakhstan[6]

***Abstract*—Early detection of armed threats is crucial in reducing accidents and deaths resulting from armed conflicts and terrorist attacks. The most significant application of weapon detection systems would be found in public areas such as airports, stadiums, central squares, and on the battlefield in urban or rural conditions. Modern surveillance and control systems of closed-circuit television cameras apply deep learning and machine learning algorithms for weapons detection on the base of cloud architecture. However, cloud computing is inefficient for network bandwidth, data privacy and slow decision-making. To address these issues, edge computing can be applied, using Raspberry Pi as an edge device with the EfficientDet model for developing the weapons detection system. The image processing results are transmitted as a text report to the cloud platform for further analysis by the operator. Soldiers can equip themselves with the suggested edge node and headphones for armed threat notifications, plugged into augmented reality glasses for visual data output. As a result, the application of edge computing makes it possible to ensure data safety, increase the network bandwidth and provide the device operation without the internet. Thus, an independent weapon detection system was developed that identifies weapons in 1.48 seconds without the Internet.**

***Keywords*—Internet of Things; gun recognition; edge device; Raspberry pi; military systems control; network analytic**

I. Introduction

Recent world events show that the number of terrorist attacks per year and armed conflicts continues to grow. According to the report of Global Terrorism Index 2022 [1], even developed countries such as the United States of America ranked 30th in the overall terrorism index score, while France and Germany were in 34th and 35th places and the United Kingdom was in 42nd place among 195 countries. More than 20 countries are involved in armed conflicts and civil wars in 2023 [2]. Most of these acts of violence involve armed people whose goal is to seize territories and destroy stability in a region or state. Often enemy strikes and terrorist attacks occur at strategic targets and in public areas. Defence forces and intelligence agencies should monitor the situation to prevent and minimize the consequences of those violent acts. One of that approaches is early weapons detection.

The conventional surveillance and control system of Closed-Circuit Television (CCTV) cameras involve human as operator and requires manual control of a large number of cameras [3]. Thus, it is requiring a significantly large number of personnel to monitor cameras in vast areas. Modern Weapons Detection Systems (WDS) mainly apply an Artificial Intelligence (AI). The initial task of the first AI recognition and detection systems was to recognize a person and a face [4]. Since the process of face recognition is one of the most important task in the field of Computer Vision (CV) with various promising applications from academic research to intelligence services [5]. Moreover, a human pose [6] can give some information about the probability that a person is going to use a weapon.

This paper describes the process of creating a weapons detection system for military and civil purposes. To avoid the disadvantages of cloud architecture, such as low network bandwidth, threats to data safety and lack of computing resources of a data center, the edge computing architecture has been applied in the development of the weapons detection system. A single-board computer, Raspberry Pi, has been selected as an edge computing device, or it is briefly called an edge device [7, 8]. Our previous studies have shown the excellent results in the application of computer vision and edge computing to number plate recognition system on the Raspberry Pi [9], as well as in the development of an intelligent task offload system [10]. Thus, the Raspberry Pi would be able to complete the task of weapon recognition based on the EfficientDet model and significantly reduce the cost of the technical solution. In order to minimize the possibility of bias or overfitting with subsequent performance degradation [11], some method optimization parameters can be applied.

This study aimed to develop a weapons detection system based on Raspberry Pi with a camera module using the EfficientDet model and edge computing algorithms, as well as notification about armed threats through headphones and the capability of visualization output on the interface of soldiers' augmented reality (AR) glasses and send results to the Internet

This research is sponsored by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Program No. BR1090140221).

of Things (IoT) cloud platform for further report analyses by an operator.

As a hypothesis, it is assumed that the application of edge computing significantly decreased the volume of transcended data to the cloud, offloading the computing resources of the data center and affording the edge device functioning without an Internet connection.

The paper is organised as follows: Section II reviews the related works in the area of weapon detection and Internet of Things application. Section III presents the EfficientDet and edge computing architectures, the process of building a model for weapons detection and its algorithms. Section IV provides a detailed description of the results for each various experimental case of weapons detection. Section V compares the obtained experimental results with the existing related works. Finally, Section VI summarises all text and indicates a direction for future work.

II. Related Works

During the last years, object detectors have been greatly improved technologically and allow security forces to identify weapons with fast speed and high accuracy. Nevertheless, there is an issue in practice when it comes to recognising small objects or the reflective surface of the knife [12, 13]. One study has focused on training a model for tilling approach using Single Shot Detector MobileNet V2 and Armed CCTV Footage dataset to detect small weapons [14]. The mean average precision (mAP) of that research was about 0.758 for pistol and knife evaluation. Also, a rather significant problem is the detection of a weapon in the attacker's hand [15] or whether it is hidden from an observer in the other part of the body.

As previously noted, there are many related works describing Deep and Machine Learning methods that are currently used to detect weapons. One of the most widely used classic real-time weapons detection approaches is the Convolutional Neural Networks (CNN). The accuracy and speed of weapon detection by the CNN approach through the transfer learning method using the Visual Geometry Group and fine tuning [16] show a moderate result. This is true that CNN had quite impressive image classification performance, but without enormous data and multiview cameras, it has a problem with overfitting [17]-[19]. Since the architecture of CNN can be transformed in Faster Region CNN due to a feature extractor Inception-ResNetV2 [20], that model type can demonstrate a high per cent of mAP. However, You Only Look Once V2 (YOLO) is faster in testing and training time compared to Faster Region CNN. The other study showed that Region CNN (R-CNN) and Region Fully Convolutional Networks (R-FCN) approaches have increased the speed of weapon detection, according to the experiment conducted by Arif [3]. However, in their experimental part of the study, there were false positive results for the detection of weapons. The next paper has considered CNN approach with applying Transfer Learning and two techniques such as AlexNet and GoogLeNet [21]. Nonetheless, they have the same issue connected with false positive results as previously considered work. To overcome false positive results, Debnath and Bhowmik [12] have developed an Iterative Model Generation Framework (IMGF), which detects only moving persons with a gun and decreases the consumption of computing resources. Goenka and Sitara [23] have applied Gaussian deblur technique for Mask RCNN to detect guns better in case of a blurred image. Comparing Deep Learning (DL) and Machine Learning (ML) approaches for weapons detection [24] in terms of speed and accuracy, the former is better.

The newest and most accurate model for object detection is YOLO, and it has a lot of versions. The paper described difference between YOLOv3 and YOLOv4 in terms of sensitivity and processing time [25]. The experimental part of following studies confirms the superiority of YOLOv4 over previous YOLOv3 [26]-[28]. Also, this model can be implemented for custom object detection on Jetson Nano GPU from Nvidia with a TensorRT network optimizer [29]. The newer YOLOv5 allows to significantly increase the accuracy of weapons detection [30, 31]. The processing time per frame is 0.010 seconds compared to the 0.17 seconds of the Faster R-CNN [32]. There is also an implementation of the YOLOv5 model on high-cost device Nvidia's Jetson AGX Xavier with an impressive accuracy of 98.56 percent [33]. The applying complex hardware and DL algorithms allow for achieving effective results, but they are expensive and difficult to deploy [34]. Besides YOLO, there is a promising method based on the use of semantic embeddings and a pre-trained Contrastive Language-Image Pre-Training (CLIP) model. The highest accuracy rate of this method was 99.8 percent [35], which is quite competitive with FireNet and YOLO algorithms.

The majority of modern WDS solutions are based on the IoT. The IoT applications automate routine processes and work without human interactions [36]. The IoT technology has a wide range of applications [37], ensuring people’s safety in smart homes, industry, transportation and cities [38, 39]. Most IoT solutions use cloud services as a data treatment center, for instance, data collected from sensors of smart farm are sent to the server [40], as well as the video stream data are transmitted to the cloud for further processing [41, 42]. However, some studies point to insufficient network bandwidth [43], massive generated data [44], high power consumption [45, 46], weak network security [47] and data privacy issues [48] because of using the cloud paradigm in the IoT. Those issues of IoT applications are strongly critical for military purposes. Mainly the latest researches are focused on the security of the IoT [49] since the consequences of disabling the network are not measurable. The application of military IoT could be found in the field of battlefield perception, improving the early warning, weapons and equipment management, intelligence sharing ability and support efficiency of the military, logistics support, military training and so on [50, 51]. To be more specific, military IoT studies also consider WDS, such as rope roaming robots for 360 degrees of monitoring a specific area [52], a semi-autonomous robot with WDS and stair climbing functions [53], drones or Unmanned Aerial Vehicles (UAV) for WDS [54] and explosive weapons detector [55]. To partially solve the issue associated with high power consumption, it was advised [56] to use Field Programmable Gate Array (FPGA). However, in order to finally resolve all the above list of issues, it is highly recommended to replace the cloud paradigm with edge computing [57]. FPGA provides high energy-efficient,

accelerating and high performance for complex AI tasks [58]-[60]. Thus, the edge device implements pre-processing data and sends the result to the data server [61] with much lower network bandwidth.

III. Materials and Methods

As previously mentioned in the first section, it was decided to apply Raspberry Pi 4 Model B (4 GB) with a camera, which are shown below as edge device in Fig. 1.

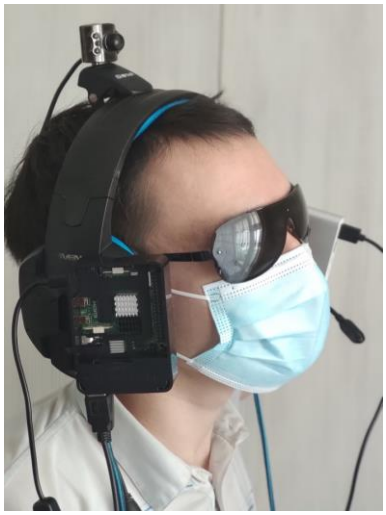

Fig. 1. Raspberry Pi with a camera as an edge node.

Headphones and a power bank have been used for audio notifications about armed threats and for the power supply of the Raspberry Pi. Raspberry Pi OS (Raspbian) has been picked as the operating system. 'Thingspeak' has been chosen as the IoT cloud platform for report and analytics formation due to visual infographic capabilities. However, the Message Queue Telemetry Transport (MQTT) without graphical support could be applied for more private message exchanges between publisher and subscribers.

A. Edge Node

The high-level programming language Python has been selected for supporting a computer vision by progressive libraries and frameworks: TensorFlow Lite, Numpy, OpenCV, Python Imaging Library (PIL) and Picamera. Since Raspberry Pi (RPi) have limited CPU and GPU resources to train a model, it was decided to use the computing server of Google Colaboratory, the framework TensorFlow Lite and 1588 images from the Kaggle dataset of various types of weapons [62, 63]. Some samples of weapons for the model training and the flow scheme are illustrated in Fig. 2.

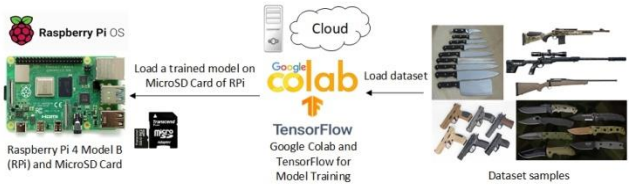

Fig. 2. The scheme of model training using Google Colab and TensorFlow Lite.

The EfficientDet has been selected as the model for weapons detection because it creates a smaller output model file, consumes less computing resources, and implements algorithms faster [64]. Moreover, EfficientDet offers a list of mobile-size lite models, which are suitable for IoT and edge devices. The EfficientDet architecture is illustrated below in Fig. 3.

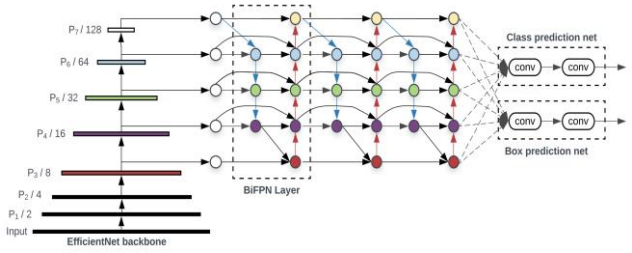

Fig. 3. The EfficientDet architecture.

EfficientDet can be considered as the one-stage detector paradigm that applies EfficientNet as the backbone network. Bi-directional feature pyramid network (BiFPN) acts as the feature network and utilizes level 3-7 features {P3, P4, P5, P6, P7} from the backbone network. It repeatedly applies bidirectional feature fusion, both top-down and bottom-up, resulting in fused features that are then fed to the class and box network for object class and bounding box predictions.

There are a few EfficientDet-Lite variants, and their checkpoints and results are shown in Table I.

TABLE I. EfficientDet-Lite Checkpoints and Results

Model	Mean average precision (float)	Quantized mean average precision (int8)	Parameters, millions	Mobile latency, milliseconds
EfficientDet-lite0	26.41	26.10	3.2	36
EfficientDet-lite1	31.50	31.12	4.2	49
EfficientDet-lite2	35.06	34.69	5.3	69
EfficientDet-lite3	38.77	38.42	8.4	116
EfficientDet-lite4	43.18	42.83	15.1	260

Since it is necessary to prioritize safety and provide the highest speed of object detection, the EfficientDet-Lite0 has been chosen.

The general equitation for compound scaling of the EfficientDet model would be the following:

$$f = \alpha + \beta^{\varphi} + \gamma^{\varphi} \quad (1)$$

Where α is a depth scaling factor, β is a width scaling factor, γ is a resolution scaling factor, φ is a number of network variation, and f is a network scaling factor.

The BiFPN network width and depth would use scaling equitations:

$$W_{bifpn} = 64 \times (1.35^{\varphi}) \quad (2)$$

$$D_{bifpn} = 3 + \varphi \tag{3}$$

Box/class prediction network would be scaled with the following equitation:

$$D_{box} = D_{class} = 3 + \lfloor \varphi / 3 \rfloor \tag{4}$$

Input image resolution uses the next scaling equitation:

$$R_{input} = 512 + \varphi \times 128 \tag{5}$$

Thus, the EfficientDet allows us to decrease the size of the model file by 4x–9x and use 13x–42x fewer Floating-point operations per seconds (FLOPs) than most previously reviewed detectors.

The flowchart of weapons detection is presented below in Fig. 4.

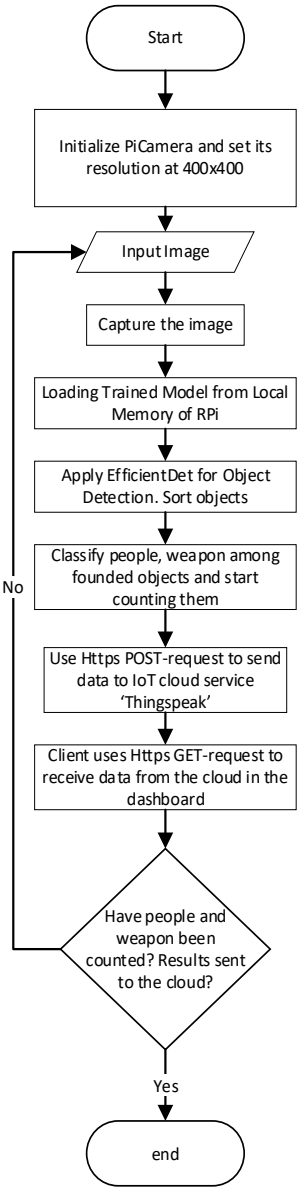

Fig. 4. The flowchart of weapons detection process.

Firstly the Pi's camera has been initialized, and its resolution has been configured at 400x400. Then algorithm started capturing an image and loading a trained model by Google Colab and TensorFlow Lite. An applying that model and EfficientDet architecture allowed to detect objects from captured image. The sorted objects were counted and classified by a model as person, rifle, pistol (handgun) and knife. Finally, the results were transcended to IoT cloud platform 'Thingspeak' through HTTP-request. After that a subscriber can send Http GET-request to collect results. If an armed threat was detected, the user of the system would receive a voice notification via headphones.

The common scheme processing of captured image is demonstrated in Fig. 5.

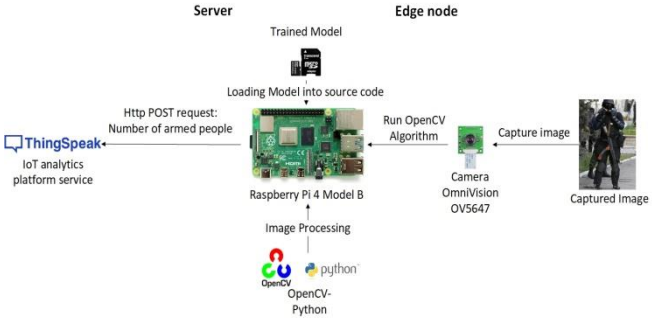

Fig. 5. The scheme of image processing.

B. Server Side

The IoT cloud platform 'Thingspeak' has been used to monitor the results of weapons detection on the server side, as mentioned before. 'Thingspeak' supports Representational State Transfer of the Application Programming Interface (RESTful API) and due to this users can easily exchange messages between edge device, client and server. The client-server model is illustrated in Fig. 6.

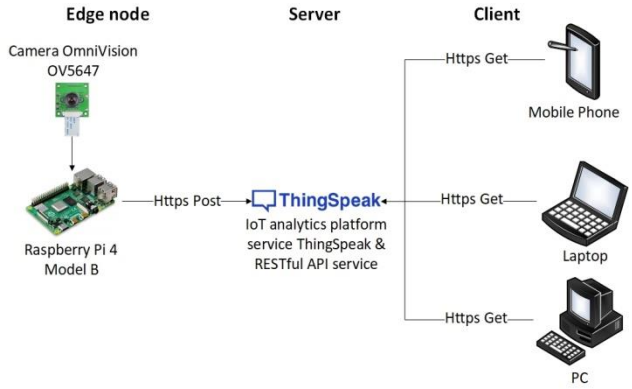

Fig. 6. The client-server model for the weapons detections system.

To observe the processed data securely from any type of device, an admin has logged in to the 'Thingspeak' account and created a private channel. Then he has gotten an API and started the configuration process of private channel. The configuration of channel and widgets are shown in Fig. 7.

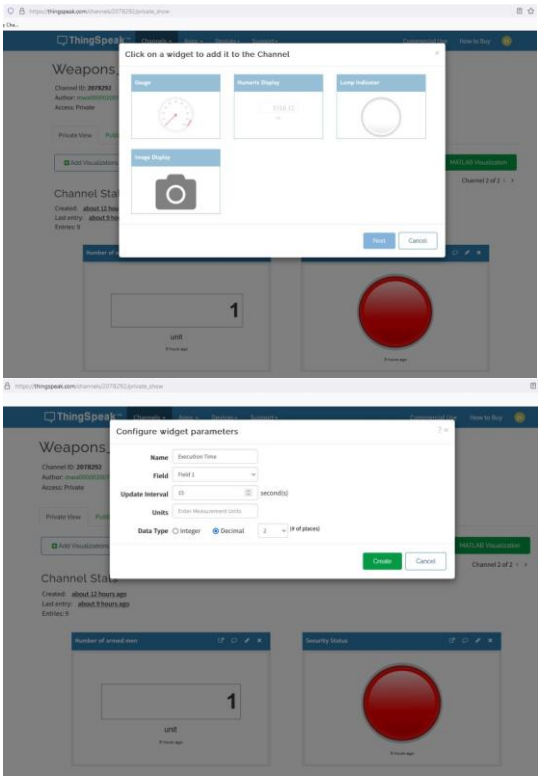

Fig. 7. The procedure of configuration the channel and adding widgets in Thingspeak.

C. Client Side

An operator browsing a private channel from any accessible type of device (table, smartphone, personal computer) and collect all data for report and analysis. The processes data are presented in the widgets of the web application 'Thingspeak', which could be found in Fig. 8.

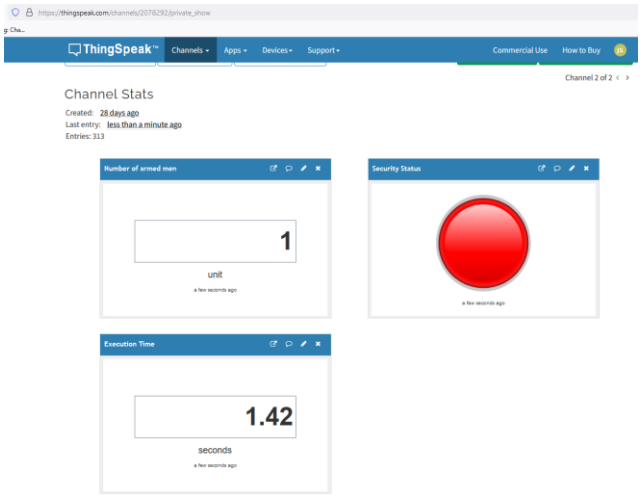

Fig. 8. Results in the web application 'Thingspeak' for the case with rifle detection.

The operator has a capability to apply the MQTT protocol as an option to keep data privacy and output received results in a terminal window, which is shown in Fig. 9.

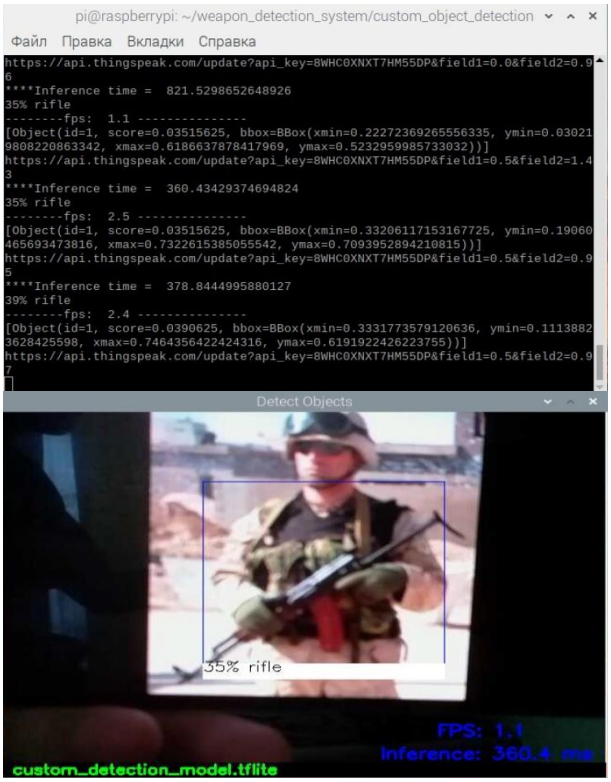

Fig. 9. Results in a terminal window.

D. The Application of Weapons Detection System for Augmentation Reality Glasses

To improve the user experience of armed threats detection in addition to voice notification, it has been proposed to plug in Raspberry Pi to AR glasses for better visualization. The result of marking an armed threat will be displayed on the interface of the soldier's glasses, providing him with the necessary information to make a quick decision. The scheme of AR glasses interaction with Raspberry Pi is shown in Fig. 10.

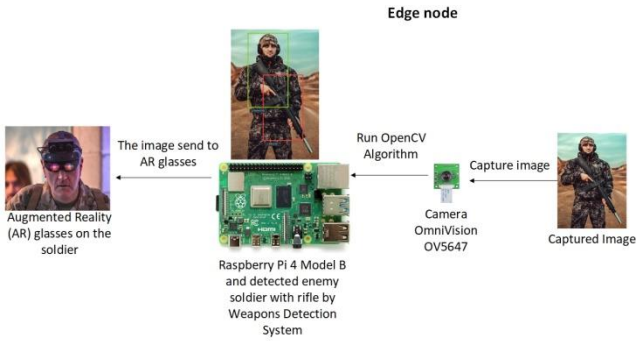

Fig. 10. The scheme of AR glasses interaction with Raspberry Pi.

IV. Experimental Results

Three cases of weapons detection have been considered such as rifle, pistol (handgun) and knife. The first case with the rifle detection from smartphone display has been presented in the previous section in Fig. 9. The terminal window describes the following information: weapon type with accuracy recognition in per cent, inference time in milliseconds, and

frame per second. For this case, an operator can find such information in the web application: number of armed persons and time for algorithm execution, which are presented in Fig. 8.

The results of the next case with handgun are shown in Fig. 11.

Fig. 11. The case with pistol (handgun) detection.

The handgun has been marked by rectangle and labeled. The terminal window also outputs the type of detected weapon, inference time and Http POST-request. The results of that case in web application are shown in Fig. 12.

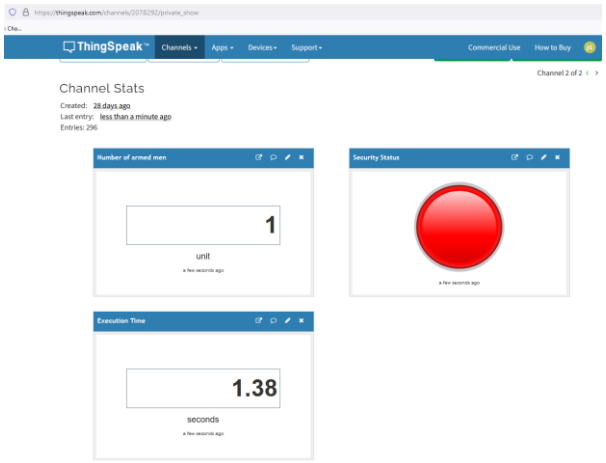

Fig. 12. The view of the web application for the case with pistol (handgun) detection.

The first widget from the left presents the number of armed persons. The lamp of the next widget has become active and red since the armed threat has been detected. The last widget shows the execution time of the algorithm.

Finally, the last case of cold steel weapon (knife) detection from the real scenario is shown in Fig. 13.

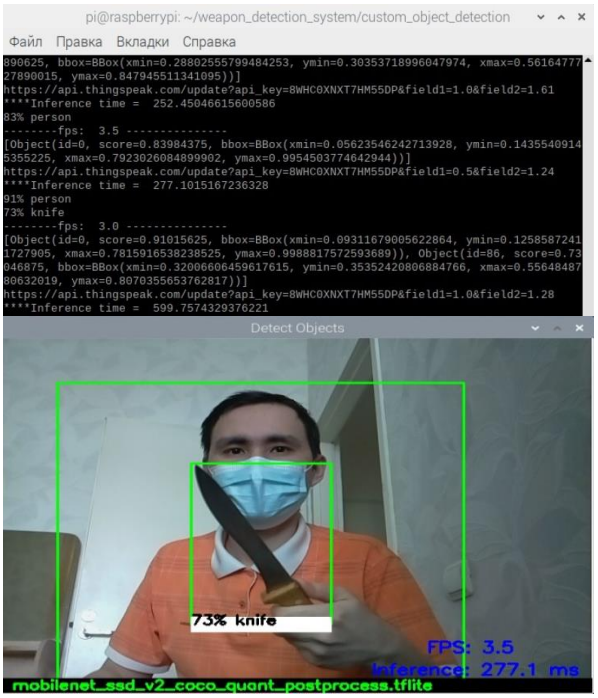

Fig. 13. The case with knife detection.

The common view of the knife detection case for the web application is shown in Fig. 14.

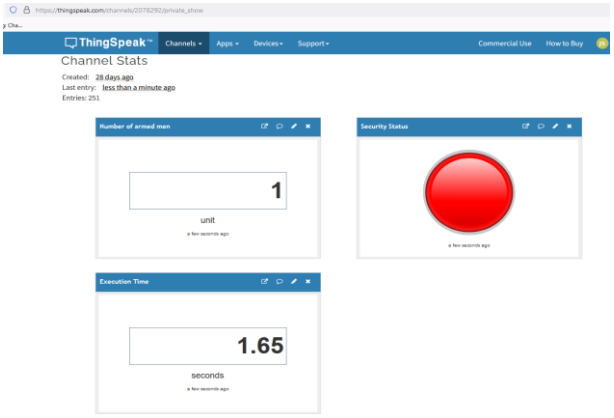

Fig. 14. The view of the web application for the case with knife detection.

To collect information about network traffic and bandwidth, the web application 'Monitorix' was deployed on the Raspberry Pi for the local host. Fig. 15 demonstrates that the maximum transmitted data to the IoT cloud platform have reached about 53 kilobytes per second or 40 packets per second without any network error during transcending data

.

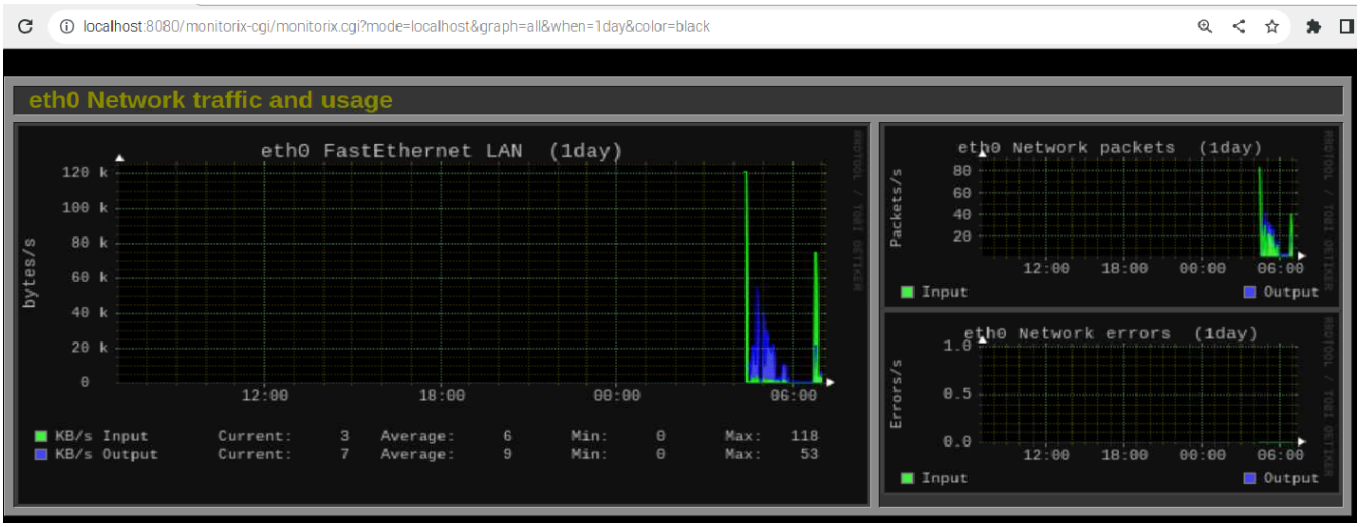

Fig. 15. The web application 'Monitorix' for monitoring network traffic.

V. Discussion of Results

To compare with the transmission of the video stream with an average required throughput of over 1.8 megabytes per second [43], the proposed approach requests less network bandwidth and significantly reduces the amount of transmitted data. As a consequence, it also reduced the load on the network and server resources. The average time for algorithm execution is approximately 1.48 seconds. It is quite a medium time of algorithm execution compared to 1.76 seconds for the Inception-ResNetV2 model and 1.1 seconds for the ResNet50 CNN model [20]. That is true that YOLO and MobileNetV2 [15, 20] are almost twice as fast in terms of object recognition and detection as EfficientDet-Lite0, but it should be noted that the productivity of the proposed algorithm execution time can be improved with Coral USB Accelerator. However, YOLO and ResNet require over 10 million parameters for object classification [41, 64]. Consequently, those models consume more disk space and computing resources. The highest accuracy of the knife detection case for EfficientDet-Lite0 model is an average result compared to 71.44 per cent for Faster R-CNN [17] and 77.78 per cent for YOLOv4 [26].

VI. Conclusion

In this paper, the weapons detection system has been developed based on the Raspberry Pi using computer vision and edge computing. The suggested approach has successfully overcome the resource limitation of Raspberry Pi to train a model through Google Colaboratory and TensorFlow Lite. Also, the hypothesis has been confirmed and obtained results indicating a significant decrease in the amount of data transmitted over the Internet, and as a result, it allows optimizing the server resources to accomplish other tasks. The presented data in the web application allows the operator to create a report. Moreover, it has been considered the capability to plug in Raspberry Pi with a camera module to AR glasses of soldiers for visually marking humans with weapons in real-time. The application of edge computing made it possible for the device to work without the Internet connection and thus ensure data safety. In addition to that, edge computing has reduced the cost of the technical solution and provides an option to operate the device on a local area network using MQTT protocol for message exchange. As a result, an autonomous weapon recognition system has been proposed that can operate without an Internet connection and detect weapons within 1.48 seconds.

In the future, it is considered expanding our research to detect explosive devices, heavy tanks and unmanned aerial vehicles. Though there may be some issues related to the detection of fast-moving objects, poor lighting conditions and quality of images, which should be solved with an FPGA and high megapixels infrared camera.

Acknowledgment

The authors thank the editor and anonymous reviewers for their comments that helped to improve the quality of this work.

References

[1] Vision of Humanity, Global Terrorism Index. [Online]. Available: https://www.visionofhumanity.org/maps/global-terrorism-index/#/

[2] World Population Review, Countries Currently at War 2023. [Online]. Available: https://worldpopulationreview.com/country-rankings/countries-currently-at-war

[3] E. Arif, S. K. Shahzad, R. Mustafa, M. A. Jaffar, and M. W. Iqbal, "Deep neural networks for gun detection in public surveillance," Intelligent Automation and Soft Computing, vol. 32, no. 2, pp. 909-922, 2022. https://doi.org/10.32604/iasc.2022.021061.

[4] W. Rahmaniar and A. Hernawan, "Real-time human detection using deep learning on embedded platforms: a review," Journal of Robotics and Control (JRC), Review vol. 2, no. 6, pp. 462-468, 2021. https://doi.org/10.18196/jrc.26123.

[5] T. V. Dang, "Smart home management system with face recognition based on ArcFace model in deep convolutional neural network," Journal of Robotics and Control (JRC), vol. 3, no. 6, pp. 754-761, 2022. https://doi.org/10.18196/jrc.v3i6.15978.

[6] A. Lamas, S. Tabik, A. C. Montes, F. Pérez-Hernández, J. García, R. Olmos, and F. Herrera, "Human pose estimation for mitigating false negatives in weapon detection in video-surveillance," Neurocomputing, vol. 489, pp. 488-503, 2022. https://doi.org/10.1016/j.neucom.2021.12.059.

[7] M. G. Ismail, F. H. Tarabay, R. El-Masry, M. A. El Ghany, and M. A. M. Salem, "Smart cloud-edge video surveillance system," in 11th International Conference on Modern Circuits and Systems Technologies,

MOCAST 2022, 2022. https://doi.org/10.1109/MOCAST54814.2022.9837646.

[8] S. S. Brimzhanova, S. K. Atanov, M. Khuralay, K. S. Kobelekov, and L. G. Gagarina, "Cross-platform compilation of programming language golang for raspberry pi," in 5th International Conference on Engineering and MIS, ICEMIS 2019, 2019. https://doi.org/10.1145/3330431.3330441.

[9] Z. Y. Seitbattalov, H. Canbolat, Z. S. Moldabayeva, and A. E. Kyzyrkanov, "An intelligent automatic number plate recognition system based on computer vision and edge computing," in 2022 International Conference on Smart Information Systems and Technologies, SIST 2022, 2022. https://doi.org/10.1109/SIST54437.2022.9945787.

[10] S. K. Atanov, Z. Y. Seitbattalov, and Z. S. Moldabayeva, "Development an intelligent task offloading system for edge-cloud computing paradigm," in 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021. https://doi.org/10.1109/ICECCO53203.2021.9663797.

[11] Y. Arslan and H. Canbolat, "Performance of deep neural networks in audio surveillance," in 6th International Conference on Control Engineering and Information Technology, CEIT 2018, 2018. https://doi.org/10.1109/CEIT.2018.8751822.

[12] J. L. Salazar González, C. Zaccaro, J. A. Álvarez-García, L. M. Soria Morillo, and F. Sancho Caparrini, "Real-time gun detection in CCTV: an open problem," Neural Networks, vol. 132, pp. 297-308, 2020. https://doi.org/10.1016/j.neunet.2020.09.013.

[13] A. Castillo, S. Tabik, F. Pérez, R. Olmos, and F. Herrera, "Brightness guided preprocessing for automatic cold steel weapon detection in surveillance videos with deep learning," Neurocomputing, vol. 330, pp. 151-161, 2019. https://doi.org/10.1016/j.neucom.2018.10.076.

[14] N. Hnoohom, P. Chotivatunyu, and A. Jitpattanakul, "ACF: an armed CCTV footage dataset for enhancing weapon detection," Sensors, vol. 22, no. 19, 2022. https://doi.org/10.3390/s22197158.

[15] R. Debnath and M. K. Bhowmik, "A comprehensive survey on computer vision based concepts, methodologies, analysis and applications for automatic gun/knife detection," Journal of Visual Communication and Image Representation, vol. 78, 2021. https://doi.org/10.1016/j.jvcir.2021.103165.

[16] O. Veranyurt and C. O. Sakar, "Hand-gun detection in images with transfer learning-based convolutional neural networks," in 28th Signal Processing and Communications Applications Conference, 2020. https://doi.org/10.1109/SIU49456.2020.9302394.

[17] P. Y. Ingle and Y. G. Kim, "Real-time abnormal object detection for video surveillance in smart cities," Sensors, vol. 22, no. 10, 2022. https://doi.org/10.3390/s22103862.

[18] J. Li, C. Ablan, R. Wu, S. Guan, and J. Yao, "Preprocessing techniques' effect on overfitting for VGG16 fast-RCNN pistol detection," International Journal of Computers and their Applications, vol. 28, no. 1, pp. 45-54, 2021. https://doi.org/10.29007/ml35.

[19] N. U. Haq, M. M. Fraz, T. S. Hashmi, and M. Shahzad, "Orientation aware weapons detection in visual data: a benchmark dataset," Computing, vol. 104, no. 12, pp. 2581-2604, 2022. https://doi.org/10.1007/s00607-022-01095-0.

[20] R. M. Alaqil, J. A. Alsuhaibani, B. A. Alhumaidi, R. A. Alnasser, R. D. Alotaibi, and H. Benhidour, "Automatic gun detection from images using faster R-CNN," in 1st International Conference of Smart Systems and Emerging Technologies, SMART-TECH 2020, pp. 149-154, 2020. https://doi.org/10.1109/SMART-TECH49988.2020.00045.

[21] M. K. El Den Mohamed, A. Taha, and H. H. Zayed, "Automatic gun detection approach for video surveillance," International Journal of Sociotechnology and Knowledge Development, vol. 12 no. 1, pp. 49-66, 2020. https://doi.org/10.4018/IJSKD.2020010103.

[22] R. Debnath and M. K. Bhowmik, "Novel framework for automatic localisation of gun carrying by moving person using various indoor and outdoor mimic and real-time views/scenes," IET Image Processing, vol. 14 no. 17, pp. 4663-4675, 2020. https://doi.org/10.1049/iet-ipr.2020.0706.

[23] A. Goenka and K. Sitara, "Weapon detection from surveillance images using deep learning," in 3rd International Conference for Emerging Technology, 2022. https://doi.org/10.1109/INCET54531.2022.9824281.

[24] P. Yadav, N. Gupta, and P. K. Sharma, "A comprehensive study towards high-level approaches for weapon detection using classical machine learning and deep learning methods," Expert Systems with Applications, vol. 212, 2023. https://doi.org/10.1016/j.eswa.2022.118698.

[25] T. S. S. Hashmi, N. U. Haq, M. M. Fraz, and M. Shahzad, "Application of deep learning for weapons detection in surveillance videos," in 2021 International Conference on Digital Futures and Transformative Technologies, 2021. https://doi.org/10.1109/ICoDT252288.2021.9441523.

[26] W. E. I. B. W. N. Afandi and N. M. Isa, "Object detection: harmful weapons detection using YOLOv4," in 2021 IEEE Symposium on Wireless Technology and Applications, pp. 63-70, 2021. https://doi.org/10.1109/ISWTA52208.2021.9587423.

[27] M. Gali, S. Dhavale, and S. Kumar, "Real-time image based weapon detection using YOLO algorithms," 6th International Conference on Advances in Computing and Data Sciences, vol. 1614 CCIS, pp. 173-185, 2022. https://doi.org/10.1007/978-3-031-12641-3_15.

[28] A. Jaleel, S. K. Khurshid, R. Mustafa, K. Mehmood Aamir, M. Tahir, and A. Ziar, "Towards proactive surveillance through CCTV cameras under edge-computing and deep learning," Mathematical Problems in Engineering, vol. 2022, 2022. https://doi.org/10.1155/2022/7001388.

[29] S. Ahmed, M. T. Bhatti, M. G. Khan, B. Lövström, and M. Shahid, "Development and optimization of deep learning models for weapon detection in surveillance videos," Applied Sciences, vol. 12, no. 12, 2022. https://doi.org/10.3390/app12125772.

[30] N. Yeddula and B. E. Reddy, "Effective deep learning technique for weapon detection in CCTV Footage," in 2nd IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2022, 2022. https://doi.org/10.1109/ICMNWC56175.2022.10031724.

[31] L. Sumi and S. Dey, "YOLOv5-based weapon detection systems with data augmentation," International Journal of Computers and Applications, 2023. https://doi.org/10.1080/1206212X.2023.2182966.

[32] A. H. Ashraf, M. Imran, A. M. Qahtani, A. Alsufyani, O. Almutiry, A. Mahmood, M. Attique, M. Habib, "Weapons detection for security and video surveillance using CNN and YOLO-V5s," Computers, Materials and Continua, vol. 70, no. 2, pp. 2761-2775, 2022. https://doi.org/10.32604/cmc.2022.018785.

[33] M. Dextre, O. Rosas, J. Lazo, and J. C. Gutiérrez, "Gun detection in real-time, using YOLOv5 on Jetson AGX Xavier," in 47th Latin American Computing Conference, CLEI 2021, 2021. https://doi.org/10.1109/CLEI53233.2021.9640100.

[34] D. Berardini, A. Galdelli, A. Mancini, and P. Zingaretti, "Benchmarking of dual-step neural networks for detection of dangerous weapons on edge devices," in 18th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications, MESA 2022, 2022. https://doi.org/10.1109/MESA55290.2022.10004469.

[35] Y. Deng, R. Campbell, and P. Kumar, "Fire and gun detection based on sematic embeddings," in 2022 IEEE International Conference on Multimedia and Expo Workshops, ICMEW 2022, 2022. https://doi.org/10.1109/ICMEW56448.2022.9859303.

[36] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, "Survey on IoT: security threats and applications," Journal of Robotics and Control (JRC), vol. 2, no. 1, pp. 42-46, 2021. https://doi.org/10.18196/jrc.2150.

[37] Y. He, "Research and application of the key technology of cloud platform in various fields of computer internet of things technology," in 5th International Conference on Mechanical, Control and Computer Engineering, ICMCCE 2020, pp. 1357-1360, 2020. https://doi.org/10.1109/ICMCCE51767.2020.00297.

[38] X. Xia, "Internet of things research and application of information technology," in 5th International Conference on Mechanical, Control and Computer Engineering, ICMCCE 2020, pp. 1818-1821, 2020. https://doi.org/10.1109/ICMCCE51767.2020.00399.

[39] K. L. M. Ang and J. K. P. Seng, "Application specific internet of things (ASIoTs): taxonomy, applications, use case and future directions," IEEE Access, vol. 7, pp. 56577-56590, 2019. https://doi.org/10.1109/ACCESS.2019.2907793.

[40] A. P. Atmaja, A. E. Hakim, A. P. A. Wibowo, and L. A. Pratama, "Communication systems of smart agriculture based on wireless sensor

networks in IoT," Journal of Robotics and Control (JRC), vol. 2, no. 4, pp. 297-301, 2021. https://doi.org/10.18196/jrc.2495.

[41] Q. Yao, W. Tan, J. Liu, and D. Qi, "Edge to cloud end to end solution of visual based gun detection," in 2020 3rd International Conference on Computer Information Science and Application Technology, CISAT 2020, vol. 1634, 1 ed., 2020. https://doi.org/10.1088/1742-6596/1634/1/012033.

[42] A. Singh, T. Anand, S. Sharma, and P. Singh, "IoT based weapons detection system for surveillance and security using YOLOV4," in 6th IEEE International Conference on Communication and Electronics Systems, ICCES 2021, pp. 488-493, 2021. https://doi.org/10.1109/ICCES51350.2021.9489224.

[43] C. Fathy and S. N. Saleh, "Integrating deep learning-based IoT and fog computing with software-defined networking for detecting weapons in video surveillance systems," Sensors, vol. 22, no. 14, 2022. https://doi.org/10.3390/s22145075.

[44] R. Wang, W. T. Tsai, J. He, C. Liu, Q. Li, and E. Deng, "A video surveillance system based on permissioned blockchains and edge computing, in 2019 IEEE International Conference on Big Data and Smart Computing," BigComp 2019, 2019. https://doi.org/10.1109/BIGCOMP.2019.8679354.

[45] M. Perea-Trigo, E. J. López-Ortiz, J. L. Salazar-González, J. A. Álvarez-García, and J. J. Vegas Olmos, "Data processing unit for energy saving in computer vision: weapon detection use case," Electronics, vol. 12, no. 1, 2023. https://doi.org/10.3390/electronics12010146.

[46] M. U. Harun Al Rasyid, F. Astika Saputra, and A. Kurniawan, "Surveillance monitoring system based on internet of things," in 2020 International Electronics Symposium, IES 2020, pp. 588-593, 2020. https://doi.org/10.1109/IES50839.2020.9231634.

[47] P. Gao, R. Yang, C. Shi, and X. Zhang, "Research on security protection technology system of power internet of things," in 8th IEEE Joint International Information Technology and Artificial Intelligence Conference, ITAIC 2019, pp. 1772-1776, 2019. https://doi.org/10.1109/ITAIC.2019.8785603.

[48] A. Kaknjo, M. Rao, E. Omerdic, T. Newe, and D. Toal, "Real-time secure/unsecure video latency measurement/analysis with FPGA-based bump-in-the-wire security," Sensors, vol. 19, no. 13, 2019. https://doi.org/10.3390/s19132984.

[49] X. Li, W. Pan, J. Zhang, G. Liu, and P. Wan, "Research on security issues of military internet of things," in 17th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 399-403, 2020. https://doi.org/10.1109/ICCWAMTIP51612.2020.9317401.

[50] X. Li, W. Pan, J. An, and P. Wan, "The application research on military internet of things," in 17th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2020, pp. 187-191, 2020. https://doi.org/10.1109/ICCWAMTIP51612.2020.9317321.

[51] C. Donghao, Z. Bohua, O. Chaomin, and C. Zhiyu, "Research on military internet of things technology application in the context of national security," in 2nd International Conference on Electronics, Communications and Information Technology, CECIT 2021, pp. 992-998, 2021. https://doi.org/10.1109/CECIT53797.2021.00177.

[52] P. K. Maduri, P. Sharma, H. Saini, P. M. Tripathi, and S. Singh. "Weapon detection rope roaming human safety robot," 2nd International Conference on Mechanical and Energy Technologies, ICMET 2021, pp. 43-51, 2023. https://doi.org/10.1007/978-981-19-1618-2_5.

[53] M. Z. Islam, A. Ahsan, and R. Acharjee, "A semi-autonomous tracked robot detection of gun and human movement using Haar cascade classifier for military application," in 2019 International Conference on Nascent Technologies in Engineering, ICNTE 2019, 2019. https://doi.org/10.1109/ICNTE44896.2019.8945848.

[54] D. R. Hawale and P. S. Game, "Real-time weapon detection using drone," in 6th International Conference on Computing, Communication, Control and Automation, ICCUBEA 2022, 2022. https://doi.org/10.1109/ICCUBEA54992.2022.10010921.

[55] A. Bhatt and A. Ganatra, "Explosive weapons and arms detection with singular classification (WARDIC) on novel weapon dataset using deep learning: enhanced OODA (observe, orient, decide, and act) loop," Engineered Science, vol. 20, 2022. https://doi.org/10.30919/es8e718.

[56] X. Liu, J. Yang, C. Zou, Q. Chen, X. Yan, Y. Chen, and C. Cai, "Collaborative edge computing with FPGA-based CNN accelerators for energy-efficient and time-aware face tracking system," IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 252-266, 2022. https://doi.org/10.1109/TCSS.2021.3059318.

[57] C. Yang, "FPGA in IoT edge computing and intelligence transportation applications," in 2021 IEEE International Conference on Robotics, Automation and Artificial Intelligence, RAAI 2021, pp. 78-82, 2021. https://doi.org/10.1109/RAAI52226.2021.9507835.

[58] C. Xu, S. Jiang, G. Luo, G. Sun, N. An, G. Huang, and X. Liu, "The case for FPGA-based edge computing," IEEE Transactions on Mobile Computing, vol. 21, no. 7, pp. 2610-2619, 2022. https://doi.org/10.1109/TMC.2020.3041781.

[59] C. Xiao and C. Zhao, "FPGA-based edge computing: task modeling for cloud-edge collaboration," International Journal of Modeling, Simulation, and Scientific Computing, vol. 13, no. 2, 2022. https://doi.org/10.1142/S1793962322410094.

[60] Z. Zhu J. Zhang, J. Zhao, J. Cao, D. Zhao, G. Jia, and Q. Meng, "A hardware and software task-scheduling framework based on CPU+FPGA heterogeneous architecture in edge computing," IEEE Access, vol. 7, pp. 148975-148988, 2019. https://doi.org/10.1109/ACCESS.2019.2943179.

[61] R. Ferdian, R. Aisuwarya, and T. Erlina, "edge computing for internet of things based on FPGA," in 6th International Conference on Information Technology Systems and Innovation, ICITSI 2020, pp. 20-23, 2020. https://doi.org/10.1109/ICITSI50517.2020.9264937.

[62] Weapons datasets. Annotated rifle and handgun images. [Online]. Available: https://www.kaggle.com/datasets/ar5p1edy/weapons-datasets

[63] Ankan Sharma, Weapon detection dataset. Weapon detection including knife, gun, pistol etc. [Online]. Available: https://www.kaggle.com/datasets/ankan1998/weapon-detection-dataset

[64] M. Tan, R. Pang and Q. V. Le, "EfficientDet: scalable and efficient object detection," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 10778-10787, Seattle, WA, USA, 2020. https://doi.org/10.1109/CVPR42600.2020.01079.