engineering proceedings

MDPI

Proceeding Paper

An Intelligent and Efficient Approach for Weapon Detection System Using Computer Vision and Edge Computing †

Imdad Ali Shah [1,*], NZ Jhanjhi [2] and Raja Majid Ali Ujjan [3]

[1] Faculty of Engineering Science & Technology, Iqra University (main), Karachi, Pakistan
[2] School of Computer Science, SCS Taylor's University, Malaysia; noorzaman.jhanjhi@taylors.edu.my
[3] School of Computing, Engineering & Physical Sciences University of the West of Scotland, raja_majidali@hotmail.com
* Correspondence: shshsyedimdadali@gmail.com
† Presented at The 11th International Electronic Conference on Sensors and Applications (ECSA-11), 26–28 November 2024; Available online: https://sciforum.net/event/ecsa-11.

Abstract: Pattern recognition algorithms have been used to make it possible for computer vision to self-train and comprehend visual input. Advanced measurements have been required every time for the early detection of armed threats because of decreasing accidents and terrorist attacks. Weapon detection systems have mostly been used in public spaces such as stadiums, airports, key squares, and battlefields, whether they are in urban or rural settings for better security objectives. Based on cloud architecture, DL, and ML algorithms have been used by contemporary closed-circuit television surveillance and control systems to detect weapons. Using the Raspberry Pi as an edge device and an Efficient model to construct a weapons detection system, edge computing is used to address these problems. The text report includes the image processing results. Soldiers can outfit themselves with the recommended edge node and headphones, and visual data output to receive alerts about armed threats. Furthermore, we can improve our method's performance by adding more training data and changing the network architecture. The primary object of this paper is to build a model for detecting weapons such as pistols and rifles. This research detects weapons such as pistols and rifles with an average time of 1.30 s.

Keywords: gun recognition; military systems control; raspberry Pi; computer vision; edge computing and IoT

Citation: Shah, I.A.; Jhanjhi, N.Z.; Ujjan, R.M.A. An Intelligent and Efficient Approach for Weapon Detection System Using Computer Vision and Edge Computing. *Eng. Proc.* **2024**, *6*, x. https://doi.org/10.3390/xxxxx

Academic Editor(s):

Published: 26 November 2024

1. Introduction

Weapon detection systems use various parts and devices, from cameras and sensors to analytics software, to identify threats. An overview of these advanced security measures that protect us provided here. Armed individuals capture territory and upend stability in a state or region are typically involved in these violent crimes. Terrorist and adversary strikes frequently take place in public spaces and at strategic locations. The early detection of weapons is one of those strategies. A human operator needed for the traditional closed-circuit television (CCTV) monitoring and control system, which necessitates the manual operation of numerous cameras [1,2]. A notably large staff needed to watch cameras over wide areas, Artificial intelligence (AI) is the primary technology used by modern weapons detection systems. The original artificial intelligence (AI) detection and identification systems' primary duty was to identify a person by their face. Given that face recognition is one of the most significant tasks in the field of computer vision, it has a wide range of potential applications, ranging from intelligence services to scholarly studies. Furthermore, a person's posture can reveal information about the likelihood that will brandish a weapon [3,4]. Figure 1. Overview of the human vision system.

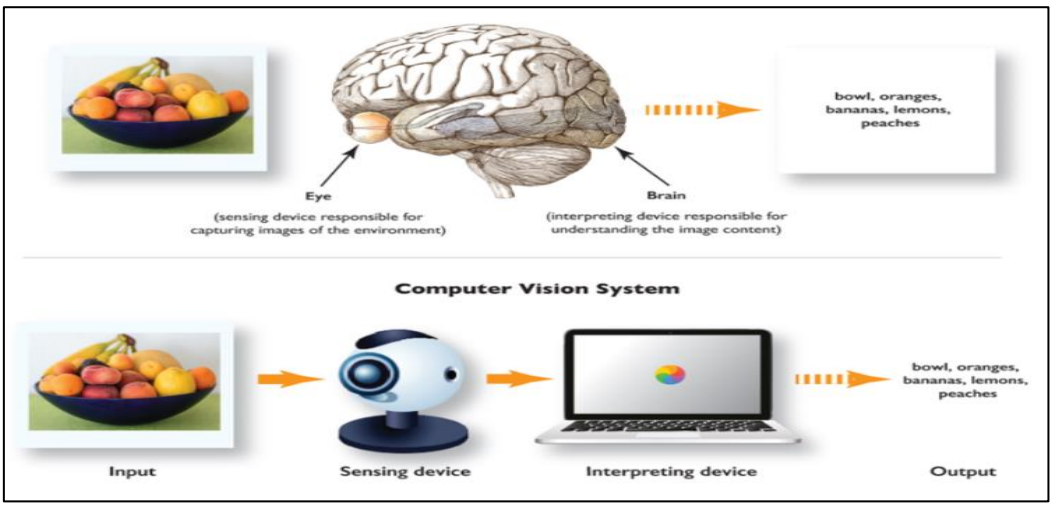

Figure 2. Overview of the human vision system adapted from v7labs.com.

[5,6] The Raspberry Pi will be able to finish the EfficientDet model-based weapon detection work and lower the cost of the technical solution.

Research Contribution

- This research detects weapons such as pistols and rifles with an average time of 1.30 s.
- This research decreases the amount of transmitted data and less network bandwidth.
- This research takes an average time for the execution of algorithm 1.30 and compared to 1.76 s for the InceptionNetV2 model.
- This research compares transmission video streams of 1.8 megabytes per second.

2. Literature Review

In one study, a model for the tilling technique trained to detect tiny weapons using the Armed CCTV Footage dataset and the Single Shot Detector MobileNet V2. Related studies on weapon detection include the work by [9], which evaluated the sliding window approach using Faster-RCNN and VGG-16 on various datasets and videos from YouTube [10]. Affected the rate of weapon detection, specifically for cold-steal knives and blades. While this proved successful for indoor applications, the accuracy reduced for outdoor use due to various lighting conditions and reflections. To train the model to stop mistaking similarly shaped objects for weapons, [11,12]. This method involved training multiple CNN models to identify distinct components of the weapon, like the trigger or the muzzle, and then averaging the models to predict the presence of pistols in the images. [13] This approach produced higher detection rates, but also longer detection times. To identify concealed weapons, the research conducted by [14,15] relied on specialized images captured by passive millimetre wave cameras and employed a CNN model to identify similar-shaped grey items as firearms. Figure 2 presents the taxonomy of the literature review.

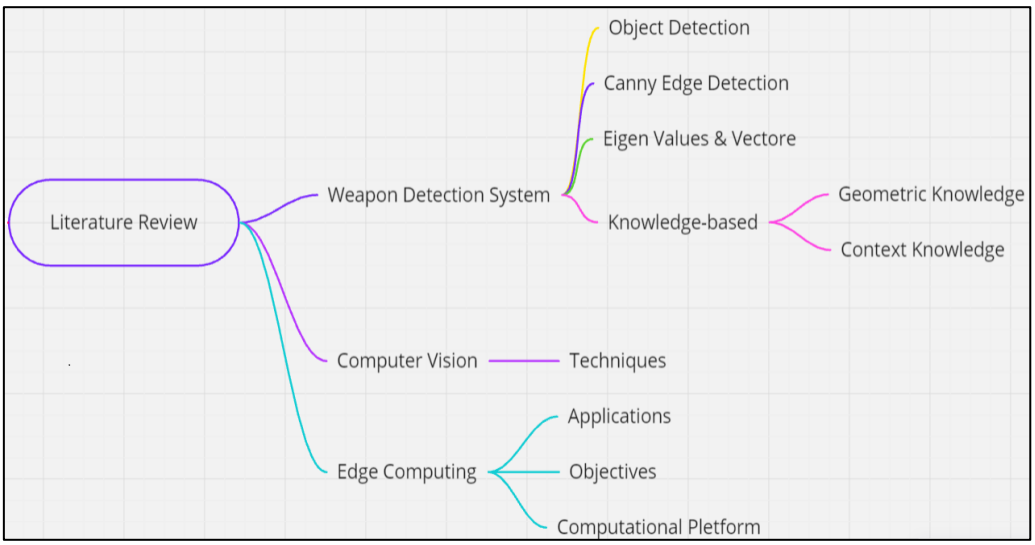

Figure 2. presents the taxonomy of the literature review.

Although these systems yield good outcomes, households cannot afford the high cost of this technology. To detect firearms, the research by [16] uses an ensemble of semantic neural networks. Multiple neural networks are given distinct tasks, and the average of the outputs indicates whether a handgun was present. [17] has conducted additional research on the Faster-RCNN model for item and pedestrian detection. [19] employed support vector machines (SVM) for real-time apparel recognition from security footage. A survey titled Advances in Deep Learning using X-ray Security Imaging, [18] analysed the performance of various CNN versions and other algorithms around security and the identification of potentially dangerous objects in luggage at airports. Although this model functioned effectively, regular settings, households without sufficient money, and regions with exceptionally high or low temperatures cannot use the system due to the requirement of passive millimetre-wave pictures. Using the previously mentioned literature review, the optimal model attempted to identify to maximize the outcomes through pre-processing approaches and detect objects quickly and accurately in real-time. As mentioned before, there are relevant publications that explain how deep machine-learning techniques now applied to weapon detection. Convolutional neural networks are one of the most used traditional real-time weapons detection techniques [19]. While CNN did do remarkably well in image classification, it suffered from overfitting in the absence of large datasets and Multiview cameras. This allows the CNN architecture to turn into Faster Region CNN. There are several uses for IoT technology, including protecting people's safety in smart cities, smart homes, businesses, and transit [20]. Studies indicate that the usage of the cloud paradigm on the Internet of Things has resulted in inadequate network capacity, massively generated data, excessive power consumption, weak network security, and data privacy issues [21,22]. For military objectives, those Internet of Things application concerns are quite important. Since the effects of turning off the network are immeasurable, the current research concentrated on IoT security.

3. Overview Weapon Detection System

TensorFlow already provides state-of-the-art object identification models, which is crucial because the goal of this study is to deploy a weapon detection system on Android rather than design the model. TensorFlow, an open-source machine learning platform with a large, flexible ecosystem of tools and libraries, enables the utilization of state-of-the-art resources for machine learning and for creating and testing deep learning architectures [23]. The TensorFlow Object Detection API is an additional open-source software library built on top of TensorFlow that facilitates the creation, training, and implementation of detection models. TensorFlow's pre-trained models saved architectures that have

previously undergone intensive training on a large dataset, usually consisting of image classification tasks. This allows the model to extract useful features, which is an important first step in learning new jobs. The discovery of irregular, unexpected, unpredictable, or unusual events or items that are present in a dataset and, as a result, diverge from preexisting patterns—that as regularly recurring events or regular items in a pattern—is known as weapon or anomaly detection [24]. Accurate gun detection and categorization are the main goals of the proposed implementation. Systems for detecting weapons are a crucial component of both private and public security infrastructure. These solutions safeguard digital assets, stop terrorist attacks, and much more. In the modern world, these methods are necessary to guarantee safety without compromising an individual's civil liberties. Therefore, it is crucial to comprehend the necessity of weapon detection systems before delving into the technology they use.

4. Security Weapon Detector Types

This is critical to discuss the kinds of firearm detection systems in use today. For instance, airport security uses handheld metal detectors. Furthermore, contemporary technology is being used more and more for comparable functions, like thermal imaging cameras and security X-ray equipment (Al-Dulaimy et al., 2020). When analyzing potentially harmful products, this allows security officers to examine them with greater accuracy and precision. Sophisticated analysis and signal processing algorithms are the foundation of advanced weapon detection systems' ability to precisely recognize and identify possible threats. For this reason, for the system to accurately assess whether an object is a real weapon, it needs a data-rich model of an object, like a gun. Tests are conducted on the object's physical attributes to develop this model. Radar-based systems are another kind of weapon-detecting system employed in security today. These systems use electromagnetic waves to identify the location, velocity, and existence of objects. These systems have several drawbacks despite their propensity for great accuracy. Digital network technology is another option for weapon detection in addition to radar-based systems. Digital networks usually utilize detectors and cameras to identify weapons nearby. Real-time data from a variety of sources, including security cameras, sensors, and motion detectors, can collect over these networks (Sharma and Mullana, 2020). As a result, the system can instantly identify dangers and notify the proper authorities of any questionable conduct. Furthermore, sophisticated algorithms are frequently incorporated into the construction of digital networks, enabling them to recognize objects of any size or shape and assisting in the reduction of false alarms brought on by outside noise.

5. Overview Computer Vision

These devices function by detecting metal objects, such as knives or guns. Furthermore, modern technology is increasingly utilized for similar purposes, such as security X-ray equipment and thermal imaging cameras. [25]. This enables security agents to evaluate potentially dangerous products more precisely and accurately. The ability of advanced weapon detection systems to accurately identify and detect threats is based on sophisticated analysis and signal processing algorithms. Because of this, the system requires a data-rich model of an object, such as a gun, in order to determine whether it is a real weapon. Tests conducted on the object's physical attributes to develop this model. Radar-based systems are another kind of weapon-detecting system employed in security today. These systems use electromagnetic waves to identify the location, velocity, and existence of objects. These systems have drawbacks despite their propensity for great accuracy. Digital network technology is another option for weapon detection in addition to radar-based systems. Digital networks usually utilize detectors and cameras to identify weapons nearby. Real-time data from a variety of sources, including security cameras, sensors, and motion detectors, can collected over these networks [26]. As a result, the system can instantly identify dangers and notify the proper authorities of any questionable conduct.

Furthermore, sophisticated algorithms are frequently incorporated into the construction of digital networks, enabling them to recognize objects of any size or shape and assisting in the reduction of false alarms brought on by outside noise.

6. Overview Edge Computing

In edge computing, data from clients processed at the network's edge, which is near the data's original generation point. This is a distributed information technology architecture. One of the most significant resources for contemporary firms is data, which not only offers insightful information but also plays a crucial role in decision-making for efficient corporate operations. With the right system in place to safeguard data from unwanted access and enable real-time operations from many locations and connected devices, the deluge of data may handle and regulated [30,31]. It is difficult to manage the data flow when integrating a standard cloud computing network. Edge computing is therefore necessary in cloud networks to guarantee optimal information flow.

7. Materials and Methods

Raspberry Pi 4 Model B (4 GB) with a camera used to receive auditory notifications regarding armed threats and to charge the Raspberry Pi, headphones and a battery bank utilized. Raspberry Pi OS picked as the operating system. There are IoT cloud platforms used to collect analytics formation because of visual infographic expertise.

7.1. Edge Node

The Python Language has been chosen for computer vision libraries and frameworks, Numpy, TensorFlow, Python Imaging Library, and Pi camera, as 2230 images from the GitHub dataset, show types of weapons. Weapons few samples have picked for model training. Figure 3 *Overview* of model training using TensorFlow and Google Colab.

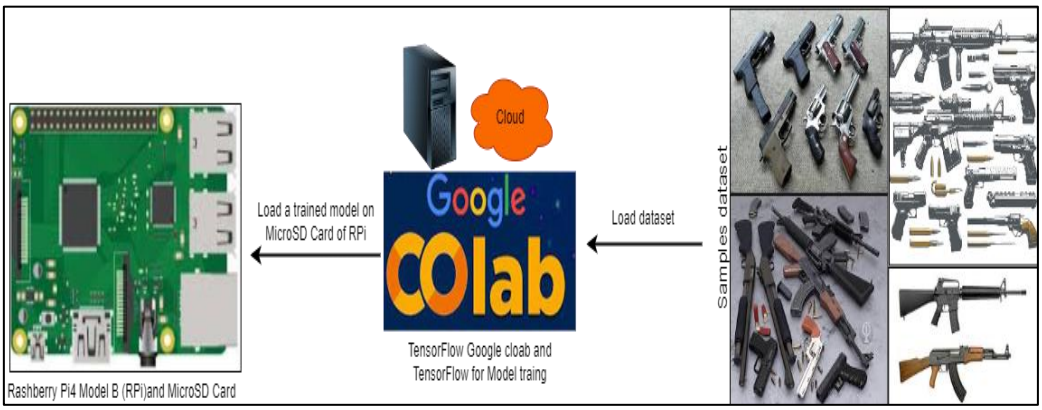

Figure 3. Overview of model training using TensorFlow and Google Colab.

7.2. Dataset

We collected the dataset from GitHub https://github.com/ari-dasci. Given the rising turmoil, we should equip security cameras with innovative technology. Thus, implementing AI in security cameras to recognize weapons automatically and notify owners will way implement AI in security. The weapon detection annotation in the Pascal VOC format is present in this dataset. We have chosen the EfficientDet model for weapons identification because it produces a smaller output model file, uses less computational power, and executes algorithms more quickly. Overview EfficientDet architecture is in Figure 4.

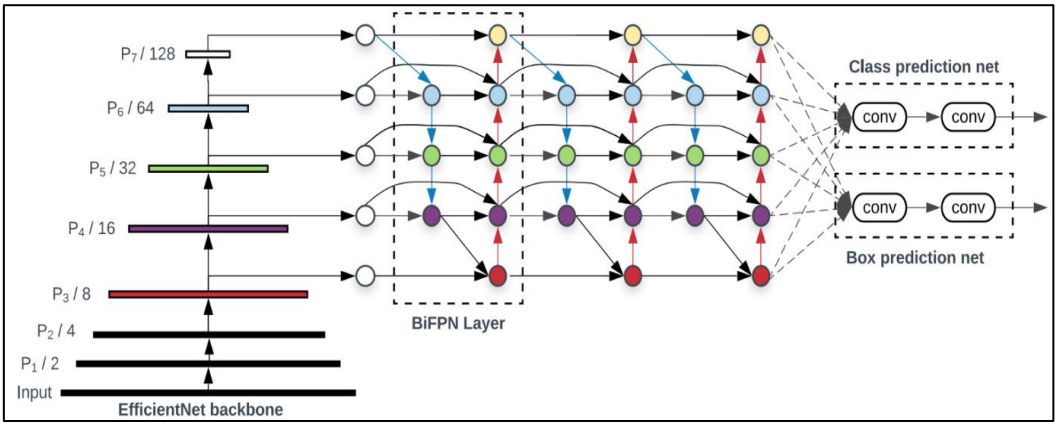

Figure 4. Overview EfficientDet architecture.

With EfficientNet serving as the backbone network, EfficientDet can be thought of as a one-stage detector paradigm. The feature network, known as the bi-directional feature pyramid network (BiFPN), makes use of the level 3–7 features up from the backbone network. It continuously performs top-down and bottom-up bidirectional feature fusion, producing fused features. Presents the results and checkpoints are shown in Table I.

Table 1. presents the Efficientdet-Lite Results and Checkpoints.

Model	Mean	Quantized Mean Average Precision	Parameters Millions	Mobile Latency, Milliseconds
EfficienDt-Lite0	26.40	26.9	3.2	35
EfficienDt-Lite0	31.51	31.11	4.2	48
EfficienDt-Lite0	35.05	34.68	5.3	68

EfficientDet-Lite0 has been selected because it is imperative to emphasize safety while offering the fastest item detection speed possible. The following would be the general equation for the EfficientDet model's compound scaling:

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

where f is a network scaling factor, φ is a number of network variations, β is a width scaling factor, γ is a resolution scaling factor, and α is a depth scaling factor. Scaling equities would be used for the BiFPN network depth and width:

$$W\ 64\ (1.35 = \times \text{bifpn}\ \varphi) \quad (2)$$

$$D = + \text{bifpn}\ 3\ \varphi \quad (3)$$

The following equation would be used to scale the box/class prediction network:

$$D\ D = = + |\ |\ \text{class}\ 3 \lfloor \varphi/3 \rfloor \quad (4)$$

The following scaling equation is used to input the image resolution:

$$R = + \times 512\ \varphi\ 128 \quad (5)$$

Therefore, compared to the majority of previously examined detectors, EfficientDet enables us to reduce the size of the model file by 4×–9× and require 13×–42× less floating-point operations per second (FLOPs). Figure 5 Overview of the flowchart of the weapons detection process.

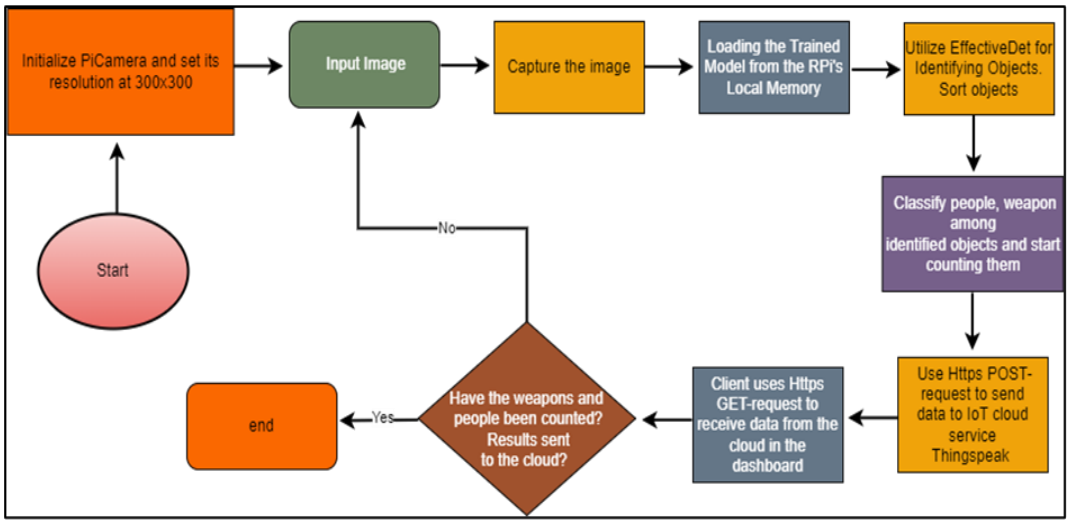

Figure 5. Overview of the flowchart of the weapons detection process.

Firstly, the resolution of the Pi's camera was set to 300x300 after it had been initialized. After that, an algorithm began using TensorFlow Lite and Google Colab to load a trained model and capture an image. Using that model and the EfficientDet architecture made it possible to identify items in the photographed data. A model was used to count and categorize the sorted items into four categories: human, rifle, pistol (handgun), and knife. Eventually, an HTTP request was used to transfer the outcomes to the IoT cloud platform "Thingspeak". Subsequently, a subscriber can retrieve results by sending an HTTP GET request. The technology would notify the user audibly through headphones if an armed threat identified.

8. Conclusions

In this paper, we used computer vision and edge computing, based on the Raspberry Pi, to build a model for detecting weapons such as pistols and rifles system have developed. The data has taken from the Kaggle dataset. The proposed approach successfully overcomes. The web application's data presentation enables the operator to generate a report. Moreover, one suggestion is to develop an autonomous weapon recognition system that can identify weapons in 1.30 s and operate without an Internet connection. It proposed to extend our research in the future to include the detection of unmanned aerial vehicles, large tanks, and explosive devices. However, there might be problems with detecting quickly moving objects, bad illumination, and image quality, all of which can resolved with an FPGA and a high-megapixel infrared camera.

Author Contributions:

Funding:

Institutional Review Board Statement:

Informed Consent Statement:

Data Availability Statement:

Conflicts of Interest:

References

1. Abdulsalam, Y.S.; Hedabou, M. Security and privacy in cloud computing: Technical review. *Futur. Internet* **2021**, *14*, 11. https://doi.org/10.3390/fi14010011.
2. Al-Dulaimy, A., Sharma, Y., Khan, M.G. & Taheri, J. Introduction to edge computing. In *Edge Computing: Models, Technologies and Applications*; 2020; pp. 3–25.

3. Alaqil, R.M., Alsuhaibani, J.A., Alhumaidi, B.A., Alnasser, R.A., Alotaibi, R.D. and Benhidour, H. Automatic gun detection from images using faster r-cnn. In Proceedings of the 2020 First international conference of smart systems and emerging technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; IEEE; pp. 149–154.
4. Arif, E.; Shahzad, S.K.; Mustafa, R.; Jaffar, M.A.; Iqbal, M.W. Deep Neural Networks for Gun Detection in Public Surveillance. *Intell. Autom. Soft Comput.* **2022**, *32*, 909–922. https://doi.org/10.32604/iasc.2022.021061.
5. Arslan, Y. and Canbolat, H. Performance of deep neural networks in audio surveillance. In Proceedings of the 2018 6th International Conference on Control Engineering & Information Technology (CEIT), Istanbul, Turkey, 25–27 October 2018; IEEE; pp. 1–5.
6. Atanov, S.K.; Seitbattalov, Z.Y.; Moldabayeva, Z.S. Development an intelligent task offloading system for edge-cloud computing paradigm. In Proceedings of the 2021 16th International Conference on Electronics Computer and Computation (ICECCO), Kaskelen, Kazakhstan, 25–26 November 2021; pp. 1–6.
7. Brimzhanova, S.S., Atanov, S.K., Khuralay, M., Kobelekov, K.S. and Gagarina, L.G. Cross-platform compilation of pro-gramming language Golang for Raspberry Pi. In Proceedings of the 5th International Conference on Engineering and MIS, Astana Kazakhstan, 6–8 June 2019; pp. 1–5.
8. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An overview on edge computing research. *IEEE Access* **2020**, *8*, 85714–85728. https://doi.org/10.1109/access.2020.2991734.
9. Castillo, A.; Tabik, S.; Pérez, F.; Olmos, R.; Herrera, F. Brightness guided preprocessing for automatic cold steel weapon detection in surveillance videos with deep learning. *Neurocomputing* **2019**, *330*, 151–161. https://doi.org/10.1016/j.neucom.2018.10.076.
10. Dang, T.-V. Smart home management system with face recognition based on arcface model in deep convolutional neural network. *J. Robot. Control.* **2022**, *3*, 754–761. https://doi.org/10.18196/jrc.v3i6.15978.
11. Debnath, R.; Bhowmik, M.K. Novel framework for automatic localisation of gun carrying by moving person using various indoor and outdoor mimic and real-time views/Scenes. *IET Image Process.* **2020**, *14*, 4663–4675. https://doi.org/10.1049/iet-ipr.2020.0706.
12. Debnath, R.; Bhowmik, M.K. A comprehensive survey on computer vision based concepts, methodologies, analysis and applications for automatic gun/knife detection. *J. Vis. Commun. Image Represent.* **2021**, *78*, 103165. https://doi.org/10.1016/j.jvcir.2021.103165.
13. Duan, Q.; Wang, S.; Ansari, N. Convergence of networking and cloud/edge computing: Status, challenges, and opportunities. *IEEE Netw.* **2020**, *34*, 148–155. https://doi.org/10.1109/mnet.011.2000089.
14. El Den Mohamed, M.K.; Taha, A.; Zayed, H.H. Automatic gun detection approach for video surveillance. *Int. J. Sociotechnol. Knowl. Dev.* **2020**, *12*, 49–66.
15. Goenka, A. and Sitara, K. Weapon detection from surveillance images using deep learning. In Proceedings of the 2022 3rd International Conference for Emerging Technology (INCET), Belgaum, India, 27–29 May 2022; IEEE; pp. 1–6.
16. González, J.L.S.; Zaccaro, C.; Álvarez-García, J.A.; Morillo, L.M.S.; Caparrini, F.S. Real-time gun detection in CCTV: An open problem. *Neural Netw.* **2020**, *132*, 297–308. https://doi.org/10.1016/j.neunet.2020.09.013.
17. Haq, N.U.; Fraz, M.M.; Hashmi, T.S.; Shahzad, M. Orientation aware weapons detection in visual data: A benchmark dataset. *Computing* **2022**, *104*, 2581–2604. https://doi.org/10.1007/s00607-022-01095-0.
18. Hnoohom, N.; Chotivatunyu, P.; Jitpattanakul, A. ACF: An armed cctv footage dataset for enhancing weapon detection. *Sensors* **2022**, *22*, 7158. https://doi.org/10.3390/s22197158.
19. Ingle, P.Y.; Kim, Y.-G. Real-time abnormal object detection for video surveillance in smart cities. *Sensors* **2022**, *22*, 3862. https://doi.org/10.3390/s22103862.
20. Ismail, M.G., Tarabay, F.H., El-Masry, R., Abd El Ghany, M. and Salem, M.A.M. Smart Cloud-Edge Video Surveillance System. In Proceedings of the 2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 8–10 June 2022; IEEE; pp. 1–4.
21. Lamas, A.; Tabik, S.; Montes, A.C.; Pérez-Hernández, F.; García, J.; Olmos, R.; Herrera, F. Human pose estimation for mitigating false negatives in weapon detection in video-surveillance. *Neurocomputing* **2022**, *489*, 488–503. https://doi.org/10.1016/j.neucom.2021.12.059.
22. Nassif, A.B.; Abu Talib, M.; Nasir, Q.; Albadani, H.; Dakalbab, F.M. Machine Learning for Cloud Security: A Systematic Review. *IEEE Access* **2021**, *9*, 20717–20735. https://doi.org/10.1109/access.2021.3054129.
23. Rahmaniar, W. & Hernawan, A. Real-time human detection using deep learning on embedded platforms: A review. *J. Robot. Control* **2021**, *2*, 462–468.
24. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. https://doi.org/10.1109/mc.2017.9.
25. Seitbattalov, Z.Y.; Canbolat, H.; Moldabayeva, Z.S.; Kyzyrkanov, A.E. An Intelligent Automatic Number Plate Recognition System Based on Computer Vision and Edge Computing. In Proceedings of the 2022 International Conference on Smart Information Systems and Technologies (SIST), Nur-Sultan, Kazakhstan, 28–30 April 2022; pp. 1–5.
26. Shah, I.A., Jhanjhi, N.Z. and Brohi, S.N. IoT Smart Healthcare Security Challenges and Solutions. Advances in Computational Intelligence for the Healthcare Industry 4.0. In *Advances in Computational Intelligence for the Healthcare Industry 4.0*; IGI Global: Hershey, PA, USA, 2024.
27. Shah, I.A., Jhanjhi, N.Z. and Brohi, S.N. Use of AI-Based Drones in Smart Cities. Cybersecurity Issues and Challenges in the Drone Industry. In *Cybersecurity Issues and Challenges in the Drone Industry;* IGI Global: Hershey, PA, USA, 2024.

28. Shah, I.A., Jhanjhi, N.Z. and Rajper, S. Use of Deep Learning Applications for Drone Technology. In *Cybersecurity Issues and Challenges in the Drone Industry*; IGI Global: Hershey, PA, USA, 2024.
29. Sharma, A. and Mullana, M.M.U. Emerging Trends in Safety Issues in Cloud the Potentials of Threat Model. *Int. J. Future Revolut. Comput. Sci. Commun. Eng.* **2020**, *3*, 260–263.
30. Veranyurt, O.; Sakar, C.O. Hand-gun detection in images with transfer learning-based convolutional neural networks. In Proceedings of the 2020 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey, 5–7 October 2020; pp. 1–4.
31. Wu, R., Li, J., Ablan, C., Guan, S. & Yao, J. Preprocessing Techniques' Effect On Overfitting for VGG16 Fast-RCNN Pistol Detection. *Int. J. Comput. Appl.* **2021**, *28*, 1.