The Internet of Things (IoT) has become an increasingly popular technology in recent years, enabling interconnectivity and communication between devices and systems. With the proliferation of IoT devices, there has been a vast increase in the volume of data generated by these devices. This massive influx of data presents both challenges and opportunities, as traditional data analysis methods may not be sufficient to handle the sheer volume of data. As a result, there is a growing need for advanced data analysis techniques and artificial intelligence (AI) methods to process, analyze, and extract valuable insights from IoT data. In this context, data analysis and AI play a critical role in enabling the effective implementation of IoT technologies and realizing their full potential. This Special Issue explores the importance of data analysis and AI for IoT. It discusses the various techniques and approaches that can be used to leverage IoT data for actionable insights effectively. Therefore, this Special Issue covers nine papers, summarized as follows:

The paper “Application of Machine Learning Algorithms for the Validation of a New CoAP-IoT Anomaly Detection Dataset” [1] addresses the need for developing an anomaly-based intrusion detection system for the CoAP-IoT environment, which is vulnerable to security threats due to its power-, bandwidth-, and memory-constrained sensing devices. The paper presents a complete and labeled CoAP-IoT anomaly detection dataset (CIDAD) based on real-world traffic, including three types of anomalies in the CoAP data. The dataset is validated using five shallow machine learning techniques, and the evaluation metrics used in the performance comparison are accuracy, precision, recall, F1 score, and kappa score. The results show that the system achieved 99.9% accuracy for decision tree models, and random forest established itself as the best model, obtaining a 99.9% precision and F1 score, 100% recall, and a Cohen’s kappa statistic of 0.99. The paper provides a valuable contribution to the field of anomaly-based intrusion detection systems, which are crucial for securing the CoAP-IoT environment against security threats.

The proposed technique for tracking a moving object of interest in a noisy video using a modified simplest color balance algorithm and a binarization algorithm proved to be effective in building training data for machine learning. The detection accuracy for ambiguous objects was over 95%, and the approach reduced the tracking loss rate to 10%.

The paper “An Effective Motion-Tracking Scheme for Machine-Learning Applications in Noisy Videos” [2] proposes a novel feature selection and extraction approach for anomaly-based intrusion detection systems in the Internet of Things (IoT) environment. The approach uses entropy-based methods to select and extract relevant features, followed by mathematical set theory to extract the best features. The proposed model framework is trained and tested on the IoT intrusion dataset 2020 (IoTID20) and NSL-KDD dataset using four machine learning algorithms. The approach resulted in 11 and 28 relevant features on IoTID20 and 15 and 25 relevant features on NSL-KDD, using intersection and union, respectively. The performance of the proposed model was compared with other state-of-the-art studies, and it was found that the model outperformed others, achieving a classification accuracy of 99.98%.

The proposed feature selection and extraction approach...
addresses the challenge of exploiting all features and attributes for IDS self-protection, making it a competent and superior model for IoT intrusion detection.

In conclusion, the proposed technique for tracking a moving object of interest in a noisy video using a modified simplest color balance algorithm and a binarization algorithm proved effective in building training data for machine learning. The detection accuracy for ambiguous objects was over 95%, and the approach reduced the tracking loss rate to 10%.

The study presented in this abstract [3] “A Study on Pine Larva Detection System Using Swin Transformer and Cascade R-CNN Hybrid Model” aimed to build an intelligent system for parcel storage by studying parcel box recognition using AI’s deep learning technology. The researchers used the YOLOv5 model for parcel recognition, which is faster and has better object recognition than previous models. They compared and analyzed four different YOLOv5 models and found that the YOLOv5large model showed the strongest performance with precision, recall, and F1 scores of 0.966, 0.899, and 0.932, respectively. The YOLOv5large model is also half the size of the YOLOv5xlarge model, making it more efficient. The researchers concluded that the YOLOv5large model could be used to build an intelligent parcel storage system that shows optimal efficiency in real-time object recognition.

The paper aimed to study parcel box recognition using the YOLOv5 model to develop an intelligent parcel storage system. Four different versions of the model were analyzed based on their performance and size, and it was found that the YOLOv5l model showed the strongest performance in terms of precision, recall, and F1 score.

The paper “Parcel Classification and Positioning of Intelligent Parcel Storage System Based on YOLOv5” [4] proposes a novel feature selection and extraction approach for anomaly-based intrusion detection systems in the Internet of Things (IoT) environment. The approach uses entropy-based methods to select and extract relevant features, followed by mathematical set theory to extract the best features. The proposed model framework is trained and tested on the IoT intrusion dataset 2020 (IoTID20) and NSL-KDD dataset using four machine learning algorithms. The approach resulted in 11 and 28 relevant features.

This study on parcel recognition using the YOLOv5 model for building an intelligent parcel storage system has identified several limitations and future research tasks. The need for conducting experiments in more diverse environments and datasets by securing additional data was identified. The study also highlighted the need to explore the latest model (YOLOv7) and investigate the potential of model transformation through pruning to optimize parcel recognition. Additionally, future research will focus on applying the object recognition model to the parcel storage system under development to confirm its performance in the real environment. These proposed future works will help to improve the performance and efficiency of the intelligent parcel storage system, making it a more reliable and effective solution for last-mile delivery services.

This paper [5] presents a novel high-gain THz antenna array that can be utilized for various THz band space communication applications. The proposed antenna is designed in four steps and operates at two frequencies with good bandwidths and gain. The multiple-order antenna arrays are designed to achieve a high gain, and their performance is analyzed in different simulators, resulting in strong agreement. Moreover, the parametric analysis is done for the proposed type C antenna array with different separations among the radiating elements, which shows that the 128 × 1 antenna array provides a high gain and directivity with good efficiency at both operating frequencies. Overall, the results obtained in this study demonstrate that the proposed antenna array design is a feasible option for high-speed and free-space wireless communication systems in the THz band.

The results show that the proposed THz array antenna has a directivity and gain of 12.5 and 11.23 dB as well as 12.532 and 11.625 dBi at 0.714 and 0.7412 THz, respectively, with high radiation efficiency. The simulated type C antenna’s minimal return loss is less than −37 dB at a resonant frequency of 0.7123 THz with a corresponding separation distance of 533 µm. The study also concludes that the antenna bandwidth decreases significantly
with the increase in the number of radiation elements. Overall, the proposed antenna array shows excellent potential for use in earth exploration satellite and space research.

This paper [6] describes the design of three types of dual-band microstrip patch antennas for wearable devices. The first is a conventional ground plane antenna, while the other two are based on two different types of electromagnetic band gap (EBG) structures. The study shows that the two EBG-based antennas improve bandwidth and gain compared to the conventional ground plane antenna. Furthermore, the authors have demonstrated that the mushroom-like EBG and the EBG with plus-shaped slots enhance the bandwidth and gain at both lower and higher resonance frequencies. Additionally, the study investigates the conventional ground plane antenna under various bending conditions. It evaluates its specific absorption rate (SAR) on the human body using tissue models, concluding that the proposed antenna reduces SAR effects on the human body, making it useful for various wearable applications.

This paper presents the design and analysis of a compact dual-band microstrip patch antenna operating at 2.5 and 5.2 GHz. The proposed antenna is designed to enhance its performance with two different electromagnetic band gap (EBG) ground planes. Results indicate that EBG-inspired antennas perform better than those with a conventional ground plane. The proposed antenna was tested in various bending conditions and remained tuned regardless of the bending radii. The SAR analysis revealed that the SAR value of the conventional antenna is within the standard SAR limit prescribed by European standards in both conditions when the antenna is placed over the flat body phantom or wrapped around the rounded body parts. The authors concluded that the proposed antenna design could be useful for various applications, including personal communications gadgets, equipment for combat and rescue operations, and health devices without compromising the wearer’s health.

This paper [7] addresses the challenges Intrusion Detection Systems (IDS) face in the Internet of Things (ICT) context due to IoT data’s high dimensionality and diversity. The authors propose a novel feature selection and extraction approach using two entropy-based methods, information gain (IG) and gain ratio (GR), and mathematical set theory (union and intersection) to extract the best features. The proposed approach is trained and tested on the IoT intrusion dataset 2020 (IoTID20) and NSL-KDD dataset using four machine learning algorithms. The results show that the proposed method outperforms state-of-the-art studies, achieving 99.98% classification accuracy. The authors suggest that this approach can be useful for self-protective IDSs against various cyber-attacks in the IoT ecosystem.

The paper presents a feature selection approach for intrusion detection systems (IDS) using mathematical set theory to extract efficient subsets of features. The developed IDS scheme consists of three phases: data preprocessing, dimensionality reduction, feature selection, and model training and classification. The dimensionality reduction phase uses IG and GR filter-based approaches to rank features and develops a hybrid feature selection approach using intersection and union rules to optimize performance. The model training and classification phase applies five machine learning algorithms to classify generated subsets of traffic features into standard or intrusion classes for binary and multi-classification purposes. The results indicate that the ensemble-based hybrid approach provides optimum results by eliminating irrelevant features before training. This approach outperforms related works and unique machine learning algorithms in classification performance, as demonstrated by significant improvements in accuracy, precision, recall, f1-measure, and the ROC area. In future works, the proposed system will be deployed for IoT gateway devices to detect and classify cyber-attacks and intrusions within an IoT device network. Additional evaluation parameters will be investigated to enhance the studies, including resource consumption such as energy consumption, inferencing overhead, memory utilization, and processing complexity. Resource-aware IoT nodes with tiny system elements will be used for analysis.

Due to limited processing functionality, the paper “A Deep Learning Framework Performance Evaluation to Use YOLO in Nvidia Jetson Platform” highlights the challenges
of implementing deep learning-based object detection technology on embedded systems and mobile devices [8]. The paper proposes a performance inference method that fuses the Jetson monitoring tool with TensorFlow and TensorRT source code on the Nvidia Jetson AGX Xavier platform to address this. The study compares the performance of different deep learning frameworks, including TensorFlow, TensorFlow-TensorRT, TensorRT, and TensorFlow-Lite, in terms of CPU utilization, GPU utilization, object accuracy, latency, and power consumption, using the You Look Only Once Version4 (YOLOv4) model and Common Objects in Context (COCO) and PASCAL Visual Object Classes (VOC) datasets. The study shows that TensorFlow results in high latency, while TensorFlow-TensorRT and TRT using Tensor Cores provide the most efficiency. However, TF-Lite showed the lowest performance due to its limited GPU capability. The study concludes that the proposed performance inference method can efficiently develop deep learning-related object detection technology on the Nvidia Jetson platform or desktop environment.

In conclusion, this paper aimed to optimize deep learning-based object detection technology for low latency, high accuracy detection rates, and low power consumption in embedded systems. The study applied TensorFlow and TensorRT, commonly used deep learning frameworks in Nvidia Jetson AGX Xavier embedded systems. It compared them using a fusion monitoring tool that measured CPU utilization, GPU utilization, object detection accuracy, latency, and power consumption. The study found that TensorFlow used on desktops can be applied to Nvidia Jetson AGX Xavier, but it has the highest power consumption and high latency. On the other hand, TF-Lite operates efficiently only on mobile devices, while TF-TRT and pure TRT are the most efficient for embedded systems with built-in Tensor Cores. The study recommends using pure TRT if there is insufficient implementation knowledge of the TensorFlow deep learning framework. Future work will involve studying the efficient use of deep learning frameworks with large datasets such as Open Images and Image Net by applying PyTorch libraries to Nvidia Jetson AGX Xavier.

The courier and delivery service market continues to thrive despite economic crises worldwide. With 70% of parcels being delivered in metropolitan areas, this paper [9] proposes developing an eco-friendly underground logistics system (ULS) to handle freight volume in the centers of cities. The study focused on analyzing damaged parcel boxes within the ULS and utilized a convolutional neural network (CNN), MobileNet, to detect and classify them. The Google Colaboratory notebook was used for image classification, and 4882 images were collected for the experiment. Based on test time, the MobileNet algorithm was superior to other image classification models, VGG16 and ResNet50. The results show that MobileNet can be used to ensure the reliability and safety of parcel boxes in a ULS. Thus, MobileNet can potentially be used to identify damaged boxes.

In conclusion, this paper proposes using an underground logistics system (ULS) in metropolitan areas to reduce the number of freight cars and handle freight volume. An experiment was conducted to detect whether the parcel boxes were damaged or not using deep learning methods to improve the reliability and safety of parcel boxes. The MobileNet algorithm was used for image classification, and the results show that it performs relatively better than other image classification models concerning test time. The accuracy, recall, and specificity of the MobileNet algorithm were 84.6%, 82%, and 88.54%, respectively, for the testing set. Although the accuracy of MobileNet is lower than VGG16, its testing time was seven times faster. Therefore, MobileNet has the potential to be used for identifying damaged boxes in a ULS system and could be a reliable and efficient way to handle parcel boxes in metropolitan areas. This paper contributes to developing a more eco-friendly and efficient system for parcel delivery in urban areas, which could help address the challenges of increasing parcel volumes and environmental concerns.

These are various research works that involve the application of machine learning algorithms in different areas. The first paper presents a new CoAP-IoT anomaly detection dataset for machine learning algorithm validation. The second paper introduces an effective motion-tracking scheme for machine-learning applications in noisy videos. The third paper uses a hybrid model of Swin Transformer and Cascade R-CNN, focusing on pine larva
detection. The fourth paper proposes a YOLOv5-based intelligent parcel storage system for parcel classification and positioning. The fifth paper presents the design and analysis of a dual-band high-gain THz antenna array for THz space applications. The sixth paper proposes a dual-band wearable antenna design and SAR analysis for WLAN applications. The seventh paper introduces a novel feature selection method for IoT intrusion detection using machine learning. The eighth paper evaluates the performance of using the YOLO deep learning framework in the Nvidia Jetson platform. Lastly, the ninth paper focuses on the image classification of parcel boxes in the underground logistics system using CNN MobileNet. All these works aim to solve real-world problems by leveraging machine learning algorithms and techniques, making them valuable contributions to the field of artificial intelligence and its applications. However, there are still some challenges regarding the implementation of each research work as a future work.

Conflicts of Interest: The authors declare no conflict of interest.

References

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.