iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.58835

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Anomaly Detection in Crowd Surveillance using Edge Computing: A Comprehensive Survey

Ayush Juvekar[1], Shrikant Bhadgoankar[2], Ameya Ghadge[3], Madhuri Wakode[4]
Department of Computer Engineering Pune Institute of Computer Technology, Pune 411043, India

Abstract: ***As urban environments continue to witness the proliferation of surveillance systems, ensuring public safety and security has become an increasingly challenging endeavor. Anomaly detection in crowded areas has emerged as a crucial task in these settings, aimed at identifying suspicious activities or potential threats. To meet the demands of real-time monitoring and analysis, edge computing has gained prominence as a critical technology. This survey paper provides a comprehensive overview of the state-of-the-art in anomaly detection, its use in crowd surviellance and the role played by edge computing in anomaly detection .The paper reviews an extensive body of literature encompassing various techniques and methodologies employed for anomaly detection in crowded scenes. It explores the evolution of traditional video-based approaches, such as motion analysis and object tracking, and the recent advancements leveraging deep learning, including various models in machine learning. These techniques are examined for their applicability in crowd surveillance scenarios.Various commonly used datasets to measure the quality of anomaly detection are also explored, along with their attributes and descriptions.The survey analyzes how edge computing solutions, such as edge AI accelerators and edge devices, enable faster and more context-aware processing of video data, while also addressing issues related to bandwidth constraints, privacy concerns, and scalability; paving way for a further research in harnessing the power of edge computing in crowd surveillance anomaly detection.***

Index Terms: Anomaly detection, Crowd Surveillance, Real- Time Monitoring, Edge Computing, Motion Analysis, Deep Learning, Neural Networks

I. INTRODUCTION

The modern urban landscape is undergoing a profound transformation as surveillance systems become ubiquitous, and the quest for public safety and security takes center stage. The surveillance of crowded areas, in particular, presents a unique set of challenges, demanding not only vigilant monitoring but also the ability to swiftly identify anomalous activities or potential threats. In this era of fast-paced urbanization and evolving security concerns, the need for efficient and real-time anomaly detection in crowded scenes has never been more pressing.

As technology continues to advance, a significant break- through in this endeavor has been the integration of edge com- puting into the realm of crowd surveillance. Edge computing represents a paradigm shift that enables data processing to occur closer to the data source, at the network edge, rather than relying solely on centralized cloud servers. This approach not only minimizes data latency but also alleviates the load on cloud infrastructure. Consequently, edge computing has emerged as a crucial enabler for real-time monitoring, analysis, and anomaly detection in crowded environments.

This comprehensive survey paper embarks on a journey to explore the state-of-the-art in anomaly detection for crowd surveillance, shedding light on the methodologies, techniques, and technologies that have evolved to meet the ever-increasing demands of public safety. It also studies the datasets used over the years for anomaly detection along with their features and qualities. By delving into a diverse array of literature and re- search, we aim to provide a holistic perspective on the subject. Our survey encompasses traditional videobased methods such as motion analysis and object tracking, as well as cutting- edge deep learning approaches, including convolutional neural networks (CNNs), to assess their suitability and effectiveness within the context of crowd surveillance. Various scenarios where edge computing has been successfully implemented for anomaly detection are discussed to signify the possibilities it can achieve and its applicability in crowd surveillance.

II. RELATED WORK

The traditional methods for anomaly detection and their limitations were discussed by Yu et al. [1]. However, important points such as security and privacy issues of edge computing and IoT data are not discussed, as well as applications of edge computing-based anomaly detection outside IoT, like smart healthcare, smart agriculture, etc.

©IJRASET: All Rights are Reserved

Anomaly detection in video surveillance systems is surveyed by Patrikar et al. [2], focusing on various techniques applied across different scenarios such as vehicular, pedestrian, crowd, and traffic monitoring using edge computing, but there is little information about how anomaly detection is implemented using edge computing. Anomaly Detection on the Edge, specifically focusing on a technique that uses auto-encoders—a type of deep learning neural network—to identify unusual signals in data is studied by Schneible et al. [3]. An important missing aspect is the lack of mention of alternative edge computing approaches outside of auto-encoders. Edge Computing Empowered Anomaly De- tection Framework called IDForest based survey is covered in the paper [4]. This is a very narrow survey for this specific framework and no thorough comparison with other methods is done.

A survey paper by Hucˇ et al. [5] provides an analysis of machine learning algorithms for anomaly detection on edge devices, including a large imbalanced dataset (DS2OS). A lot of work is kept as future work including more imbalanced datasets, preprocessing, and optimization methods which are not covered. Offering a comprehensive overview of the field, delves into the methods, results, and implications derived from survey data. Despite its thorough exploration, the study exhibits certain methodological limitations, including a lack of specificity in findings and unclear implications for future research.

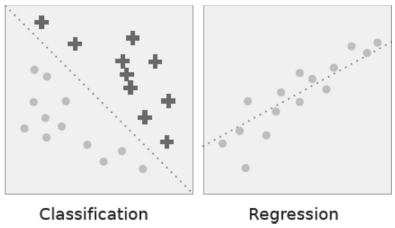


Fig. 1. Classification vs Regression [7]

III. PRELIMINARY THEORY

A. Learning Methods

1) *Supervised Learning:* Supervised learning involves the machine learning task of acquiring knowledge from labeled input-output pairs, aiming to learn a function that maps inputs to corresponding outputs. This approach utilizes labeled training data and a set of examples to deduce a function, typically driven by specific goals associated with a given input set. Common applications of supervised learning include tasks such as ”classification”, where data is categorized, and ”regression”, which involves fitting the data. An illustration of supervised learning is found in tasks like text classification, where the goal is to predict the class label or sentiment of a text, such as a tweet or a product review. [7]

Types of supervised learning [7]:

- *Classification:* Classification is a supervised learning method in machine learning where a class label is pre- dicted for a given example. It maps a function from input variables (X) to output variables (Y), such as predicting whether an email is “spam” or “not spam.” Classification problems are common in various domains. Some popular classification models used include Naive Bayes (NB), Linear Discriminant Analysis (LDA), Logistic regres- sion (LR), K-nearest neighbors (KNN), Support vector machine (SVM), Decision tree (DT), Random forest (RF), Adaptive Boosting (AdaBoost), Extreme gradient boosting (XGBoost), Stochastic gradient descent (SGD) and Rule-based classification.
- *Regression:* Regression analysis in machine learning pre- dicts a continuous result variable (y) based on predictor variables (x). Unlike classification, which predicts distinct class labels, regression deals with continuous quantities. Regression models find applications in various fields, including financial forecasting, cost estimation, trend analysis, marketing, and drug response modeling. Some of the familiar types of regression algorithms are linear, polynomial, lasso and ridge regression, etc.

2) *Unsupervised Learning:* Unsupervised learning involves the examination of unlabeled datasets without requiring human intervention, constituting a data-driven process. This method is extensively applied for extracting generative features, recog- nizing meaningful patterns and structures, identifying group- ings in outcomes, and for exploratory data analysis. Common tasks associated with unsupervised learning include clustering, density estimation, feature learning, dimensionality reduction, discovery of association rules, and anomaly detection. [7]

Types of unsupervised learning [7]:

- *Cluster Analysis:* Cluster analysis, also known as cluster- ing, is an unsupervised machine learning technique that groups related data points in large datasets. Unlike clas- sification, which predicts distinct class labels, clustering focuses on grouping objects based on similarity. It is com- monly used to discover trends or patterns in data, such as identifying groups of consumers with similar behavior.

Clustering finds applications in various domains, in- cluding cybersecurity, e-commerce, health analytics, and more. Some widely used clustering algorithms include K-means clustering, Mean-shift clustering, Density-based spatial clustering of applications with noise (DBSCAN), Gaussian mixture models (GMMs), Agglomerative hier- archical clustering, etc.

- *Dimensionality Reduction and Feature Learning:* In machine learning and data science, handling high- dimensional data is challenging. Dimensionality reduc- tion, an unsupervised learning technique, simplifies mod- els by improving human interpretations, reducing compu- tational costs, and avoiding overfitting and redundancy. It involves feature selection (keeping a subset of original features) and feature extraction (creating new features). Some popular algorithms to reduce data dimensions in- clude Variance threshold, Pearson correlation, Analysis of variance (ANOVA), Chi-square, Recursive feature elimi- nation (RFE)
- *Association Learning:* Association rule learning is a rule- based machine learning approach that discovers inter- esting relationships between variables in large datasets. It identifies ”IF-THEN” statements, such as the asso- ciation between buying a computer or laptop and also purchasing anti-virus software simultaneously. Associa- tion rules find applications in various domains, including IoT services, medical diagnosis, cybersecurity, and more. Unlike sequence mining, association rule learning does not consider the order of transactions. The usefulness of association rules is often measured using parameters like support and confidence. The most popular associa- tion rule learning algorithms are AIS and SETM, Apri- ori, quivalence Class Clustering and bottom-up Lattice Traversal (ECLAT), frequent-pattern tree (FP-tree), ABC- RuleMiner, etc.

3) *Semi-Supervised Learning:* Semi-supervised learning comes between unsupervised and supervised learning, lever- aging the advantages of both [8] [9]. It combines a limited set of labeled data with a more extensive pool of unlabeled data, exploiting the abundance of the latter. This approach is par- ticularly valuable in scenarios where acquiring labeled data is expensive or time-consuming. A fundamental concept involved in semi-supervised learning is label propagation. It involves using the labeled data to predict labels for the unlabeled data, creating a bridge between the known and unknown. Methods like self-training and co-training are commonly employed for label propagation. Semi-supervised learning often involves unique loss functions designed to accommodate both labeled and unlabeled instances. Consistency-based loss functions as used in [10], which encourage model predictions to be consis- tent on unlabeled samples, are incorporated in semi-supervised learning. Active learning strategies, where the model selects the most informative instances for labeling, are also used to optimize the learning method [11]. In image recognition, semi-supervised learning is valuable when labeling images is resource-intensive. Models like Pseudo-Labeling [12] use unlabeled images to improve performance. Semi-supervised learning has been effective in anomaly detection scenarios where normal instances are abundant, but anomalies are rare. By training on labeled normal instances and leveraging the abundance of unlabeled data, the model can detect anomalies more effectively. Self-training [8] is a classic semi-supervised learning approach where the model iteratively trains on the unlabeled data, pseudo-labels the unlabeled instances with high confidence, and adds them to the labeled dataset. This process continues iteratively, refining the model’s predictions. Co-training [8] involves training multiple models on different views of the data. Each model provides predictions for the unlabeled instances, and instances with high agreement be- tween the models are pseudo-labeled and added to the training set. Numerous implementations exist that use Generative Ad- versarial Networks [13] for anomaly detection which employ semi-supervised learning.

4) *Self-Supervised Learning:* Self-supervised learning, of- ten referred to as ”the dark matter of intelligence,” presents a promising avenue for advancing machine learning. Unlike supervised learning, which relies on labeled data availability, self-supervised approaches can glean knowledge from exten- sive unlabeled datasets. The success of self-supervised learn- ing (SSL) is notably evident in natural language processing, where it has played a pivotal role in achievements ranging from automated machine translation to the training of large language models on vast corpora of unlabeled text.

   In the realm of computer vision, SSL has expanded the horizons of data size, exemplified by models like SEER, trained on a staggering 1 billion images. Notably, SSL methods in computer vision have demonstrated the ability to match or even surpass models trained on labeled data, showcasing their prowess on competitive benchmarks such as ImageNet. Furthermore, SSL has successfully extended its applicability to diverse modalities, including video, audio, and time series.[14]

   Types of self-supervised learning [15]:

- *Self-Predictive:* Self-predictive methods in machine learn- ing involve creating a pretext task for each sample. These algorithms typically apply a transformation to the input, aiming to either predict the applied transformation or reconstruct the original input. Remarkably, these models demonstrate effectiveness even when trained solely on positive samples (in-distribution or IND samples) without requiring samples from other distributions (negatives) during training.

- *Contrastive*: Contrastive methods operate by defining a proxy task based on the relationship between pairs of samples. They commonly generate positive views of a sample by applying various geometric transformations. The objective is to bring together these positive views while simultaneously pushing them away from negative ones. In contrastive learning, samples other than the anchor sample and its augmentations within the current batch are considered negative, while positive samples arise from augmentations of the anchor. Although tech- nically contrastive algorithms can be viewed as self- predictive since they learn to predict transformations, their significant recent advancements have led to the recognition of contrastive learning as a distinct and stan- dalone category.

B. Anomaly Detection

Anomaly detection in our scope and context refers to anomalous events in video surveillance such as sudden panic in the crowd (stampede-like scenarios), a person/vehicle passing through a restricted territory, an unidentified object, violence, etc. These events are further classified in the following 5 classes [2]:

- Individual
- Crowd
- Automobiles and traffic
- Inanimate objects and events
- Interaction between humans and objects.

C. Edge Computing

Edge computing, also known as edge processing, is a network communication technique designed to optimize sys- tem performance by deploying a multitude of servers near end users and devices. In essence, it involves strategically placing servers at the edge of the network, bringing computing resources physically closer to the devices they serve. This approach is a departure from the conventional practice of cen- tralizing all data storage and processing in the cloud, instead opting for localized data handling at the network's periphery. The key benefit of this approach is the significant reduction in internet traffic and the elimination of communication delays. [16]

In the realm of network computing techniques, three promi- nent approaches stand out: edge computing, cloud computing, and fog computing. Each of these techniques processes data in distinct ways, and it's essential to understand how edge computing differs from the others. [16]

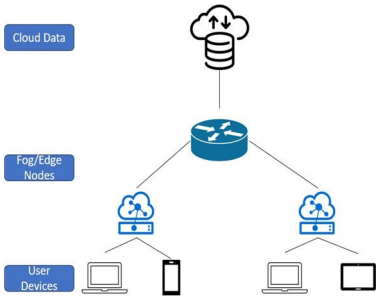


Fig. 2. Edge Computing Paradigm

The Fig. 2. depicts the edge computing paradigm.

IV. LITERATURE REVIEW

This comprehensive literature survey offers an in-depth ex- ploration of a curated selection of significant papers that make substantial contributions to the field of anomaly detection in video surveillance. Each of these papers provides unique insights, addressing diverse aspects of anomaly detection, and employs a wide array of datasets, subject detection focuses, and models, while also highlighting pertinent limitations and reporting essential evaluation metrics. Together, they collec- tively contribute to the multifaceted landscape of anomaly detection in the domain of video surveillance.

This paper [17] introduces an innovative unsupervised anomaly detection approach and utilizes UCF-Crime, Avenue, and ShanghaiTech datasets. It focuses on identifying typical occurrences in video streams, employs a Region Proposal Network (RPN), and achieves notable metrics: AUC 93%, ROC 89%, and Accuracy 87%. Focusing on crowd anomaly detection, this paper [18] works with Avenue, UCSD Ped1, and UCSD Ped2 datasets.

It targets unexpected objects, ir- regular trajectories, and restricted areas and employs pre- trained CNNs for feature extraction and various classification algorithms, achieving high AUC values. The paper [19] delves into crowd anomaly detection using Avenue, Subway, and UCSD datasets. It emphasizes spatial constraints in identifying abnormalities in crowd behavior but does not provide specific evaluation metrics. Addressing audio-visual anomaly detec- tion, this paper [20] relies on the Shade dataset. It identifies a diverse range of events and introduces the AVRL frame- work. The reported AUC is an impressive 97.7%.This paper
[21] explores online anomaly detection using Avenue, UCSD, and ShanghaiTech datasets. It identifies various anomalies like loitering, object throwing, and more, utilizing GAN and YOLOv3. Metrics are reported but exhibit lower accuracy in certain scenarios. With a focus on crowd dispersal, this paper [22] analyzes optical flow and correlation coefficients but primarily addresses one type of anomaly. It lacks metrics and comparisons with other object detection solutions.
Focusing on real-time crowd analysis, the paper [23] lever- ages VGG16 and 3DCNN. Notably, it highlights space and bandwidth inefficiencies due to the model's substantial size, but the reported metrics demonstrate strong performance for both indoor and outdoor scenarios. This paper [24] contributes to deep crowd anomaly detection, utilizing multiple datasets and reporting an average accuracy of 93%.Focusing on traffic anomaly detection, this paper [25] leverages the Track 4 test set of the 2021 AI City Challenge. It employs MOG and SENet-152 for detection, reporting F1-score and RMSE.This paper [26] introduces crowd counting and anomaly detection, relying on the VISHNU society dataset. It achieves high accu- racy in identifying and counting people with abnormal actions. This paper [27] targets the problem of online video anomaly detection, which is the task of identifying and locating abnor- mal events in video streams in real-time. The paper claims that most existing methods are offline and cannot handle the challenges of changing scenes, concept drift, and online constraints. Therefore, the paper reviews the current state-of- the-art methods and the six common datasets for online video anomaly detection, namely UMN, UCSD Pedestrian, CUHK Avenue, ShanghaiTech, UCF-Crime, and DOTA, and proposes some future research directions for online video anomaly detection. This paper [28] proposes a crowd anomaly detection algorithm based on spatio-temporal texture (STT) modeling, which is sensitive to the sudden changes of crowd motions. The paper introduces the STT structure, the feature extraction method, and the decision-making mechanism for real-time applications. The paper also evaluates the performance of the proposed algorithm against other bench-marking approaches using various datasets.
The paper [29] proposes a low computational cost approach to detect crowd anomalies using pre-trained 2D convolutional neural networks (CNNs) for motion information and a lighter form of the 2D CNN for spatial information45. This paper
[30] uses its own curated dataset named Drone-Anomaly and focuses on detecting anomalous events in aerial videos. It provides a comprehensive statistical comparison with other models and datasets commonly used and achieves better results in almost all benchmarks measured, including AUC, Recall, Precision, and F1 Score. These papers collectively enrich the multifaceted landscape of anomaly detection within the realm of video surveillance, with each research work presenting distinct and valuable insights along with innovative solutions. As a collective body of work, they contribute to advancing the state of the art in this field, paving the way for more robust, effective, and adaptable anomaly detection techniques that address the evolving challenges in the realm of video surveillance. The paper evaluates the proposed model on three public datasets: UMN, Violent Flows, and Hockey Fights, and reports the accuracy, precision, recall, and F1-score metrics.
Anomaly detection in mining scenarios is addressed through the endorsement of edge computing over traditional cloud methods, and an anomaly detection algorithm based on fuzzy theory is proposed for enhanced professionalism [38]. In [39], a framework is presented for implementing the ELM (ex- treme learning machines) model, a variation of autoencoders, validated using the NASA bearing dataset, with a specific emphasis on online anomaly detection in machinery.

TABLE I
ACCURACY AND AUC FOR THE MAJOR REVIEWED MODELS

Model	Limitations	AUC
AVRL [31]	Computationally expensive, complex training	0.9
Convolutional AE [32]	Frequent false positives, low interpretability	0.6177
RPN [33]	Needs adaptation, object-background issues	0.85
GAN+Yolov3 [21]	High false positives, data balancing	0.8

	challenge	
Yolov5 [34]	Small object detection, Localization errors, No official paper, Hardware requirements	0.9494
VGG16 [35]	Limited flexibility, relies on transfer learning	0.987
AlexNet [36]	Inconsistent results, struggles with complex anomalies	0.9
MOG [37]	Quality of input data, Computational complexity	0.969

Addition-ally, a VLSI architecture is defined to enable edge anomaly detection with reduced power consumption. The methodology in [40] involves a two-part process: initial distribution of basic classification tasks to edge devices, specifically mobile devices, employing a random forest classifier for classification; subsequently, the detection of anomaly types is carried out on the cloud using a collective of transformation-based encoders (COTE). The study concentrates on road anomalies, obtaining data through crowdsourcing on mobile devices and utilizing datasets by Carsim® to simulate vehicles driving over potholes and other anomalies. Hierarchical Edge Computing (HEC) is employed for anomaly detection here [41], involving the cre- ation of anomaly detection deep neural network (DNN) models with varying complexities aligned with corresponding layers in the hierarchy. A reinforcement learning policy network is then utilized for optimal model selection, resulting in high accuracy and F1 scores during testing on both univariate and multivariate Internet of Things (IoT) datasets. An unsupervised anomaly detection algorithm and autoencoder are implemented on ESP32 for predictive maintenance purposes [42].

V. CONCLUSION

In our survey, we've journeyed through the dynamic land- scape of anomaly detection in video surveillance, delving into core concepts and diverse learning approaches. Supervised and unsupervised learning methodologies, along with semi- supervised and self-supervised paradigms, were explored in detail. Each of these methods holds promise for anomaly de- tection, depending on the specific application and dataset. Our analysis of key influential papers highlighted innovations in real-time crowd analysis, audio-visual anomaly detection, and more, shedding light on the multifaceted challenges faced by researchers in this field. The survey underscores that anomaly detection in video surveillance is a thriving and evolving domain. The convergence of edge computing and anomaly detection offers exciting prospects for real-time, intelligent surveillance. Challenges persist, including model limitations, dataset diversity, and edge computing complexities.

TABLE II
SURVEY OF DATASETS

Dataset	Papers using this dataset	Description
PASCAL VOC	[9], [33]	Object detection, segmentation, 21k images, 20 classes
MSCOCO	[9], [33]	Object detection, captioning, 330k images, 80 classes, 250k instances
SQuAD	[10]	Reading comprehension, 100k+ questions, 500+ articles

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

NewsQA	[10]	Question answering, 100k+ news articles, 500k+ questions
DBLP	[11]	Computer science publications, 20 million+ articles, conferences, books
UCSD	[12], [13], [18], [19], [21], [24], [28], [34], [36]	Anomaly detection, video, 1617 videos, normal/abnormal activities
CUHK Avenue	[12], [13], [17], [18], [19], [21], [24], [34], [36]	Pedestrian re-identification, high-resolution, 31k images, 1.5k identities
ShanghaiTech	[12], [17], [21], [24], [34]	Person re-identification, large-scale, 486 cameras, 306k images, 111k identities
UMN	[13], [22], [24], [28], [29], [34]	UAV imagery, urban environments, RGB & LiDAR, 3 months
PETS	[13]	Animal tracking, video, cats, dogs, people, outdoor
UCF-Crime	[17] [34]	Action recognition, criminal activities, 113 videos, 10 categories
Subway	[19] [34]	Anomaly detection, video, subway, 1.2 million clips, 10 anomaly categories
SHADE	[20] [31]	Shadow removal, single images, 131 images, ground-truth masks
2021 AI City Challenge	[25]	Traffic flow forecasting, anomaly detection

©IJRASET: All Rights are Reserved

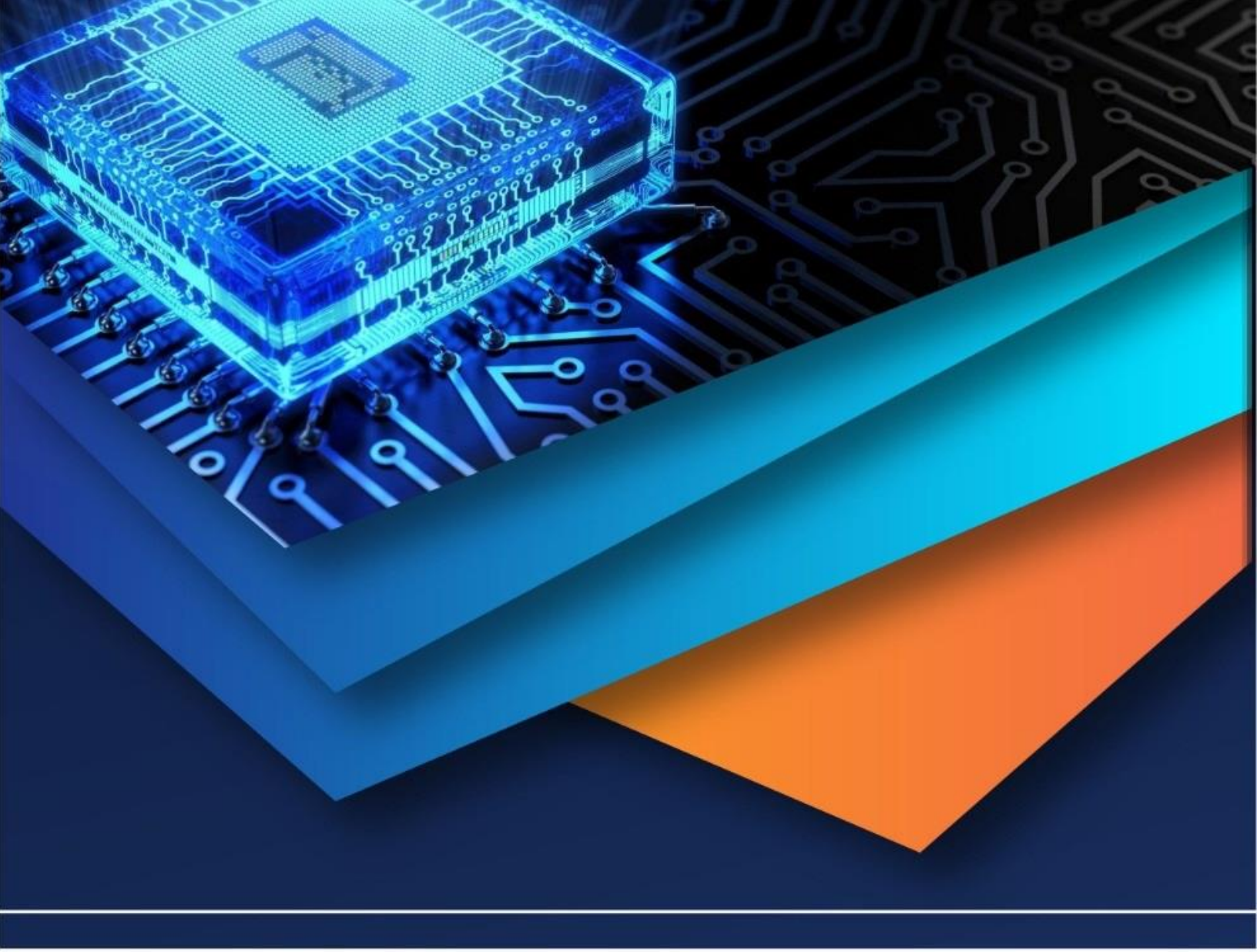
Vishnu Society Data	[26]	Gated community, India, vehicles, pedestrians, events, images, videos
Hockey Fights	[29]	Video, hockey fights, 11k videos, fight detection, outcome
Violent Flows	[29]	Video, crowd anomaly detection, 126 videos, violent/non-violent events

How-ever, through collaborative efforts and diverse methodologies, the surveyed papers are expanding the horizons of what's achievable, enhancing public safety and security. As the field continues to evolve, it is the intersection of these insights that will pave the way for the future of anomaly detection in video surveillance, ensuring a safer world.

REFERENCES

[1] Yu, Xiang, Xianfei Yang, Qinji Tan, Chun Shan and Zhihan Lv. "An edge computing based anomaly detection method in IoT industrial sustainability." Appl. Soft Comput. 128 (2022): 109486.
[2] Patrikar, Devashree R. and Mayur Rajaram Parate. "Anomaly detection using edge computing in video surveillance system: review." Interna- tional Journal of Multimedia Information Retrieval 11 (2021): 85 - 110.
[3] Schneible, Joseph and Alex Lu. "Anomaly detection on the edge." MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM) (2017): 678-682.
[4] Xiang, Haolong and Xuyun Zhang. "Edge computing empowered anomaly detection framework with dynamic insertion and deletion schemes on data streams." World Wide Web 25 (2022): 2163 - 2183.
[5] Huc˘, Aleks, Jakob S˘alej, and Mira Trebar. 2021. "Analysis of Machine Learning Algorithms for Anomaly Detection on Edge Devices" Sensors 21, no. 14: 4946. https://doi.org/10.3390/s21144946
[6] Sivapalan, Gawsalyan, Koushik Kumar Nundy, Soumyabrata Dev, Barry Cardiff and Deepu John. "ANNet: A Lightweight Neural Network for ECG Anomaly Detection in IoT Edge Sensors." IEEE Transactions on Biomedical Circuits and Systems 16 (2022): 24-35.
[7] Sarker, Iqbal H.. "Machine Learning: Algorithms, Real-World Appli- cations and Research Directions." Sn Computer Science 2 (2021): n. pag.
[8] van Engelen, Jesper E. and Holger H. Hoos. "A survey on semi- supervised learning." Machine Learning 109 (2019): 373-440.
[9] Jeong, Jisoo, Seungeui Lee, Jeesoo Kim and Nojun Kwak. "Consistency- based Semi-supervised Learning for Object detection." Neural Informa- tion Processing Systems (2019).
[10] Leng, Yan, Xinyan Xu and Guanghui Qi. "Combining active learning and semi-supervised learning to construct SVM classifier." Knowl. Based Syst. 44 (2013): 121-131.
[11] Cascante-Bonilla, Paola, Fuwen Tan, Yanjun Qi and Vicente Ordonez. "Curriculum Labeling: Revisiting Pseudo-Labeling for Semi-Supervised Learning." AAAI Conference on Artificial Intelligence (2020).
[12] Dong, Fei, Yu Zhang and Xiushan Nie. "Dual Discriminator Generative Adversarial Network for Video Anomaly Detection." IEEE Access 8 (2020): 88170-88176.
[13] Wang, Tian, Meina Qiao, Zhiwei Lin, Ce Li, Hichem Snoussi, Zhe Liu and Chang Choi. "Generative Neural Networks for Anomaly Detection in Crowded Scenes." IEEE Transactions on Information Forensics and Security 14 (2019): 1390-1399.
[14] Balestriero, Randall, Mark Ibrahim, Vlad Sobal, Ari S. Morcos, Shashank Shekhar, Tom Goldstein, Florian Bordes, Adrien Bardes, Gre´goire Mialon, Yuandong Tian, Avi Schwarzschild, Andrew Gordon Wilson, Jonas Geiping, Quentin Garrido, Pierre Fernandez, Amir Bar, Hamed Pirsiavash, Yann LeCun and Micah Goldblum. "A Cookbook of Self-Supervised Learning." ArXiv abs/2304.12210 (2023): n. pag.
[15] Hojjati, Hadi, Thi Kieu Khanh Ho and Narges Armanfard. "Self- Supervised Anomaly Detection: A Survey and Outlook." ArXiv abs/2205.05173 (2022): n. pag.
[16] Kaur, Gagandeep and Ranbir Singh Batth. "Edge Computing: Classifica- tion, Applications, and Challenges." 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (2021): 254-259.
[17] Liu, Gang, Lisheng Shu, Yuhui Yang and Chen Jin. "Unsupervised video anomaly detection in UAVs: a new approach based on learning and inference." Frontiers in Sustainable Cities (2023).
[18] Khan, Arfat Ahmad, Muhammad Asif Nauman, Muhammad Shoaib, Rashid Jahangir, Roobaea Alroobaea, Majed Alsafyani, Ahmed Binmah- foudh and Chitapong Wechtaisong. "Crowd Anomaly Detection in Video Frames Using Fine-Tuned AlexNet Model." Electronics (2022): n. pag.
[19] Feng, Ji, Dini Wang and Li Zhang. "Crowd Anomaly Detection via Spatial Constraints and Meaningful Perturbation." ISPRS Int. J. Geo Inf. 11 (2022): 205.
[20] Gao, Junyu, Maoguo Gong and Xuelong Li. "Audio-visual Representation Learning for Anomaly Events Detection in Crowds." ArXiv abs/2110.14862 (2021): n. pag.

[21] Doshi, Keval and Y. Yilmaz. "Online Anomaly Detection in Surveil- lance Videos with Asymptotic Bounds on False Alarm Rate." Pattern Recognit. 114 (2020): 107865.
[22] Chakole, Pallavi D, Vishal R. Satpute and Naveen Cheggoju. "Crowd behavior anomaly detection using correlation of optical flow magni- tude." Journal of Physics: Conference Series 2273 (2022): n. pag.
[23] AMINA P, Dr. Binu L S. Real Time Crowd Analysis and Anomaly Detection, 08 September 2022, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-1977255/v1]
[24] Sharif, Md. Haidar, Lei Jiao and Christian Walter Peter Omlin. "Deep Crowd Anomaly Detection by Fusing Reconstruction and Prediction Networks." Electronics (2023): n. pag.
[25] Doshi, Keval and Yasin Yılmaz. "An Efficient Approach for Anomaly Detection in Traffic Videos." 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021): 4231- 4239.
[26] Pokkuluri, DR., Kiran Sree, DR. G. Srinivasa Rao and DR. P. Srinivasa Raju. "CROWD COUNTING AND ANOMALY DETECTION FROM CCTV FOOTAGES USING DEEP LEARNING AUGMENTED WITH CELLULAR AUTOMATA." .
[27] Zhang, Yuxing, Jinchen Song, Yuehan Jiang, and Hongjun Li. 2023. "Online Video Anomaly Detection" Sensors 23, no. 17: 7442.
[28] Wang, Jing, and Zhijie Xu. "Spatio-temporal texture modelling for real- time crowd anomaly detection." Computer Vision and Image Under- standing 144 (2016): 177-187.
[29] Mehmood, Abid1. "Efficient Anomaly Detection in Crowd Videos Using Pre-Trained 2D Convolutional Neural Networks."23 IEEE Access 9 (2021): 138283-138295.
[30] P. Jin, L. Mou, G. -S. Xia and X. X. Zhu, "Anomaly Detection in Aerial Videos With Transformers," in IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-13, 2022
[31] Gao, Junyu, Maoguo Gong and Xuelong Li. "Audio-visual Repre- sentation Learning for Anomaly Events Detection in Crowds." ArXiv abs/2110.14862 (2021): n. pag.
[32] Schneider, Sarah, Doris Antensteiner, Daniel Soukup and matthias. scheutz. "Autoencoders - A Comparative Analysis in the Realm of Anomaly Detection." 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2022): 1985-1991.
[33] Ren, Shaoqing, Kaiming He, Ross B. Girshick and Jian Sun. "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks." IEEE Transactions on Pattern Analysis and Machine Intel- ligence 39 (2015): 1137-1149.
[34] Ali, Manal Mostafa. "Real-time video anomaly detection for smart surveillance." IET Image Process. 17 (2022): 1375-1388.
[35] Tammina, Srikanth. "Transfer learning using VGG-16 with Deep Convo- lutional Neural Network for Classifying Images." International Journal of Scientific and Research Publications (IJSRP) (2019): n. pag.
[36] Khan, Arfat Ahmad, Muhammad Asif Nauman, Muhammad Shoaib, Rashid Jahangir, Roobaea Alroobaea, Majed Alsafyani, Ahmed Binmah- foudh and Chitapong Wechtaisong. "Crowd Anomaly Detection in Video Frames Using Fine-Tuned AlexNet Model." Electronics (2022): n. pag.
[37] Ran, Qiong, Zedong Liu, Xiaotong Sun, Xu Sun, Bing Zhang, Qiandong Guo and Jinnian Wang. "Anomaly Detection for Hyperspectral Images Based on Improved Low-Rank and Sparse Representation and Joint Gaussian Mixture Distribution." IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 14 (2021): 6339-6352.
[38] Liang, Haolan, Chunxiao Ye, Yuangao Zhou and Hongzhao Yang. "Anomaly Detection Based on Edge Computing Framework for AMI." 2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT) (2021): 385-390.
[39] Bose, Sumon Kumar, Bapi Kar, Mohendra Roy, Pradeep Kumar Gopalakrishnan and Arindam Basu. "ADEPOS: anomaly detection based power saving for predictive maintenance using edge computing." Proceedings of the 24th Asia and South Pacific Design Automation Conference (2018): n. pag.
[40] Zheng, Zengwei, Mingxuan Zhou, Yuanyi Chen, Meimei Huo and Dan Chen. "Enabling real-time road anomaly detection via mobile edge computing." International Journal of Distributed Sensor Networks 15 (2019): n. pag.
[41] Ngo, Mao V., Tie Luo and Tony Q. S. Quek. "Adaptive Anomaly Detection for Internet of Things in Hierarchical Edge Computing: A Contextual-Bandit Approach." ArXiv abs/2108.03872 (2021): n. pag.
[42] Bratu, Dragos-Vasile, Rares Stefan Tiberius Ilinoiu, Alexandru Cristea, Maria-Alexandra Zolya and Sorin-Aurel Moraru. "Anomaly Detection Using Edge Computing AI on Low Powered Devices." Artificial Intel- ligence Applications and Innovations (2022).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)