

# Recent Advancement in Anomaly Detection in Surveillance Videos



Priyanka Patel, Amit Thakkar

**Abstract:** *Detection of Anomaly is of a notable and emergent problem into many diverse fields like information theory, deep learning, computer vision, machine learning, and statistics that have been researched within the various application from diverse domains including agriculture, health care, banking, education, and transport anomaly detection. Newly, numbers of important anomaly detection techniques along with diverseness of sort have been watched. The main aim of this paper to come up with a broad summary of the present development on detection of an anomaly, exclusively for video data with mixed types and high dimensionalities, where identifying the anomalous behaviors and event or anomalous patterns is a significant task. The paper expresses the advantages and disadvantages of the detection methods the experiments tried on the publically available benchmark dataset to assess numerous popular and classical methods and models. The objective of this analysis is to furnish an understanding of recent computer vision and machine algorithms methods and also state-of-the-art deep learnings techniques to detect anomalies for researchers. At last, the paper delivered roughly directions for future research on an anomalies detection.*

**Index Terms:** *Anomaly, Detection, Surveillance, Locality, Outlier Detection, Unseen Pattern Detection, Video Understanding.*

## I. INTRODUCTION

Anomaly detection is of major attention to many different areas within deep learning, statistics, machine learning. The main objective to detect and identify those areas of the region whose pattern or behaviors do not conform to expected in that dataset. These unexpected events which are remarkably different from an observation data set, these are called anomalies. Unobserved pattern or novelty fluctuation in data is also a anomaly [9]. In spite of this, still, there is a no solid standard definition of this concept. An abnormality is likewise alluded to as a special case like an exception, outlier, variation conflicting object and it's by and large relying upon various applications. To detect or identify outliers or unexpected patterns are significant in numerous domains including business intelligence, machine learning, deep learning, decision making, network transmission, transport,

production. For example, an abnormal event is accrued in the surveillance video, and unexpected block in the brain veins which can be a precursor of a brain tumor. As a result of this reality, anomaly discovery has a wide scope of domain. They are a fraud in credit card, health care, Agriculture, computer network, cleaning of data, video surveillance. After developing in machine learning the deep learning techniques has performed a vital role. Nowadays due to the wide range of smart gadgets are used, due to these information gathered from the real world are increasing and bigger which is likewise vast by size and Dimensionality. The property of the high-dimensional makes the data objects nearly equidistant to one another. Which will indicate that any data objects become very close as the dimensionality of data increases, resulting in the insignificant nature of their respective distances. Due to this nature, the standard methods for detecting anomaly cannot impressively manage high-dimensional data. Standard anomaly detection methods work better on the same type of patterns or features. But in real-world applications often have different types of patterns and features like nominal, binary, numerical, or categorical. This types of an anomaly lead to increased difficulty in detection of an anomaly in the dataset. Since many potential applications of detection of anomaly has been proposed and a wide range of detection algorithms are also developed from the past many years. In this paper, the concise audit of the present works and spot unique spotlight on the ones for that complicated video information with high dimensionalities and mixed types. Almost from the century, people are working on the security, to detect anomalies from surveillance video is a not a trivial job, to find anomaly is exceptionally important, specifically for video surveillance. Detection of Anomaly events in surveillance video refers to the task of finding observations that do not conform to the normal or predictable behavior. At the present time, many devices and measurements have been anticipated based on hand-crafted features. On the other hand, it remains challenging to efficiently distinguish abnormal entity from normal ones.

## II. ANOMALY AND ANOMALY DETECTION

Anomalies are pattern or observation in the data that do not conform to the normal or expected behavior. Detection of Anomaly is an approach to discovery the patterns from given dataset whose behavior is not normal on expected. These unexpected behaviors are characterized as the outliers or anomalies.

**Revised Manuscript Received on 30 July 2019.**

\* Correspondence Author

**Priyanka Patel\***, U & P U. Patel Department of Computer Engineering, CSPIT, Charotar University of Science and Technology, Anand, India

**Dr. Amit Thakkar**, 2Department of Information Technology, CSPIT, Charotar University of Science and Technology, Anand, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

## Recent Advancement in Anomaly Detection in Surveillance Videos

Anomaly some time also referred as Noise and detection of anomaly is referred as noise removal [8]. Removal Represents anomalies in a simple two-dimensional dataset as shown in Figure 1. In the whole dataset, there are two normal regions which are R1 and R2, since almost all observations fall under these two regions. Pints G2, G3, & G4 are far away from R1 and R2 region. R1 & R2 are considered as normal regions. Here the G1 region is also anomalies as it does not fall under normal regions R1 & R2.

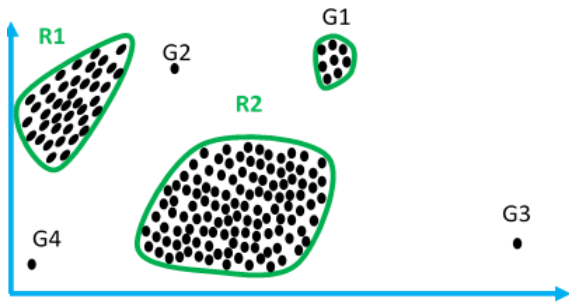


Figure 1 Example of G1-G4 Anomalies in 2D dataset

### III. BACKGROUND INFORMATION BACKGROUND ASPECTS OF ANOMALY DETECTION

In this section, we have discovered almost all available previous research that sort of data are there refer figure 2. What types of methods, which video based anomaly detection techniques are available, what sort of labels on the instance, and models [1, 5].

#### A. Type of Data

The idea of properties decides the appropriateness of abnormality identification systems. The fundamental key part of any anomaly detection method is the idea of information as you taking as input. The information is commonly a gathering of information examples which alluded to a point, record, object, vectors, design, occasion, case, tests, perception, and substance. Refer figure 3.

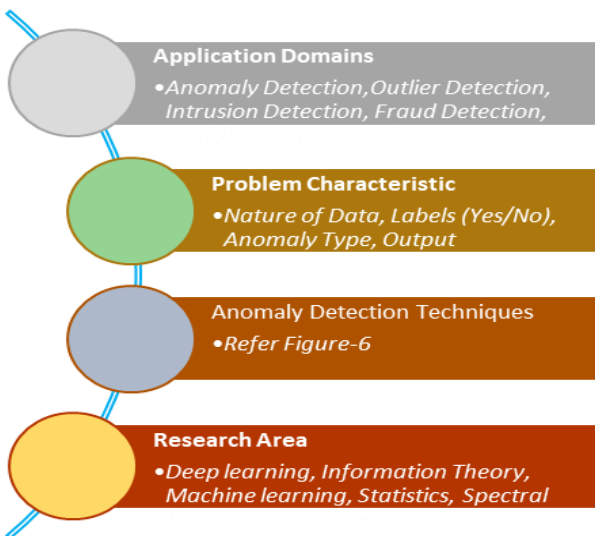


Figure 2 Aspects of anomaly detection problem

#### B. Nature of Data

Dataset Description: 1)UCSD-total 98 videos are available

which acquired pedestrian walkway. A stationary camera fixed at an elevation, supervising whole pedestrian path. 2) Caltech Pedestrian Detection dataset- 2300 unique pedestrians in 10 hours video. 3) Crowd activity datasets- University of Minnesota multiple dataset for monitoring human activity. 4) USC's dataset- USC's School of Engineering, A number of fairly small pedestrian datasets taken largely from surveillance video. 5) Anomalous Behaviour Data Set- it's a multiple dataset for anomalous behaviour detection in video. 6) Virat- Approx. A8.5 hours of videos which surveillance data for human activity/ event detection. 7) McGill University Dominant and Rare Event Detection Data- 3 video clips (43, 96 mins) - it's a video surveillance data for dominant and rare event detection captured by cameras from a subway station. 8) UCF Crime dataset-biggest dataset total 128 hours with 13 classes and 1900 videos. Untrimmed surveillance videos with 13 real world anomalies like arson, arrest, abuse, assault, road accident, burglary, explosion, fight, stealing, shooting, etc...

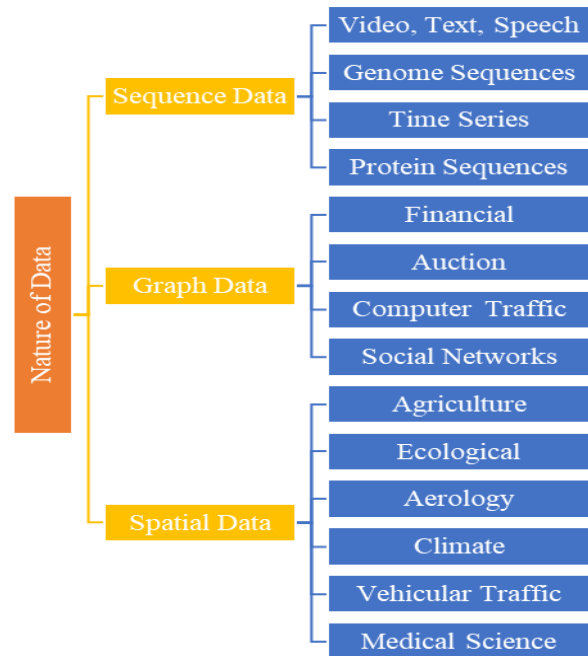


Figure 3 Nature of data

#### C. A deep learning architecture with respect to the dataset

Table 1 A deep learning architectures with respect to the dataset

Type	Example of Data Type	Deep learning Architecture
Sequential	Video, Text, speech, time series, signal, protein sequence, Genome Sequences	Convolution Neural Network, Recurrent Neural Network, Long Short-Term Memory

Type	Example of Data Type	Deep learning Architecture
Graph	Financial, Auction, Computer Traffic, Social Networks	Convolution Neural Network, Deep Convolution Neural Network, Deep Graph Convolutional Neural Network
Non-Sequential	Image, sensors, other	Convolution Neural Network, Auto encoder and its modifications
Spatial	Agriculture, Ecological, Aerology, Climate, Vehicular, Traffic, Medical Science	Convolution Neural Network, Deep Convolution Neural Network

- More significant technique than supervised.
- Build a model for normal class and use it to identify Anomaly class.

**E. Type of Anomaly**

It can be shared into below mention types: Point, Contextual, and Contextual Anomaly.

**I. Point/ Global anomaly:** It has been observed during reviewing previous research work and it is well explored in literature, the point anomaly is a commonest and most used type. Figure-2 illustrate the point G1 is measured as point anomaly and arena G2 is measured as global anomalies as both are outside of R1 and R2 region. This type of anomalies also can be defined as an individual object/entity which is measured as anomalous with regards to other data in region and it is also known as global outliers as like point arena G2[1]. Means a data point is considered a global anomaly if its value is far outside the entirety of the data set in which it is found. For example: A employer who normally deposits salary of one employee is 450000 per month in checks at a local ATM suddenly makes two cash deposits of 100000 each in the span of two weeks is a global anomaly, because this event has never before occurred in this employee’s history. The time series data of their weekly deposits would show an unexpected recent spike/point. Such a drastic change would raise alarms as these large deposits could imply illegal commerce or money laundering.

**D. Type of Labels on Instance in Anomaly Detection**

**I. Supervised**

- Training dataset with labelled instance (normal and anomaly). To propose a predictive model for abnormal and normal classes. So any unnoticed action or instance will further match and compare with the model to determine the classes (Anomaly/Normal).Issues with this method:
- Issues with this method:
  - o During Training time: Anomalous instance are far fewer than Normal instance due to this imbalance classes distribution may occurred.
  - o It is usually challenging for obtaining exact and representative labels, especially for anomaly classes.
- Supervised Anomaly detection problem is as same as building predictive model.

**II. Unsupervised [15]**

- This method do not required training data.
- It is mostly based on the assumptions that normal instance are far more frequent than anomalies in the dataset. Due to these sometime this technique suffers from high false alarm rate.
- Numerous semi-supervised techniques can be adjusted to work in an unsupervised mode by utilizing a sample of the unlabelled dataset as preparing data.

**III. Semi Supervised**

- Training Data- With assumption that only normal class are labelled in training data.
- Do not require labels for anomaly class.

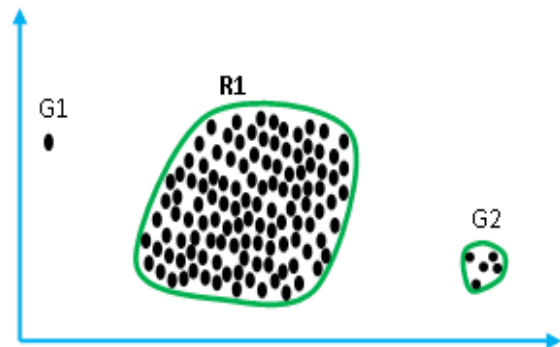


Figure 4 G1 & G2 are Global Anomaly for Normal Region R1

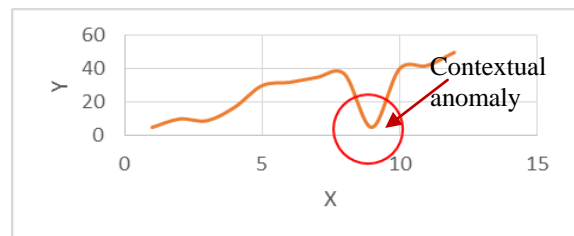


Figure 5 example of conditional anomaly

**I. Contextual Anomaly:** It may be characterized as in some particular condition or context in the event that a data instance is an outlier, at that point, it is a contextual anomaly. In spatial data and time series data, these types of anomalies are usually discovered. Some time it is also denoted to as outlier or conditional anomaly.



## Recent Advancement in Anomaly Detection in Surveillance Videos

**II. Collective Anomaly:** A collection of related data instances is anomalous. Requires a relationship among data instances like Sequential Data, Spatial Data, and Graph Data. The individual instances within a collective anomaly are not. Collective anomaly are Anomalous by themselves.

examiner may pick initial 5-10 abnormalities or may pick through some threshold values to select anomalies.

### F. Type of Output

Finally, the model produced output with two types: 1) Label: It will assign a Normal and Anomaly labels to each instance. 2) Score: The score will assign to each instance of the test data and after depending upon that instance is considered as an anomaly. This method creates a Rank list of anomalies an

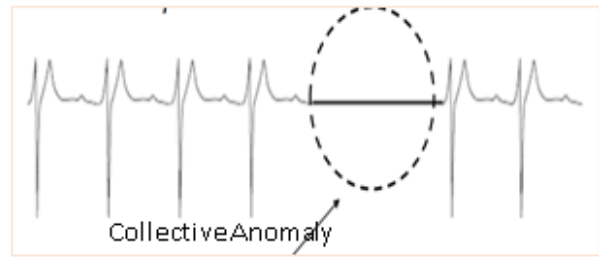


Figure 6 Example of collective Anomaly

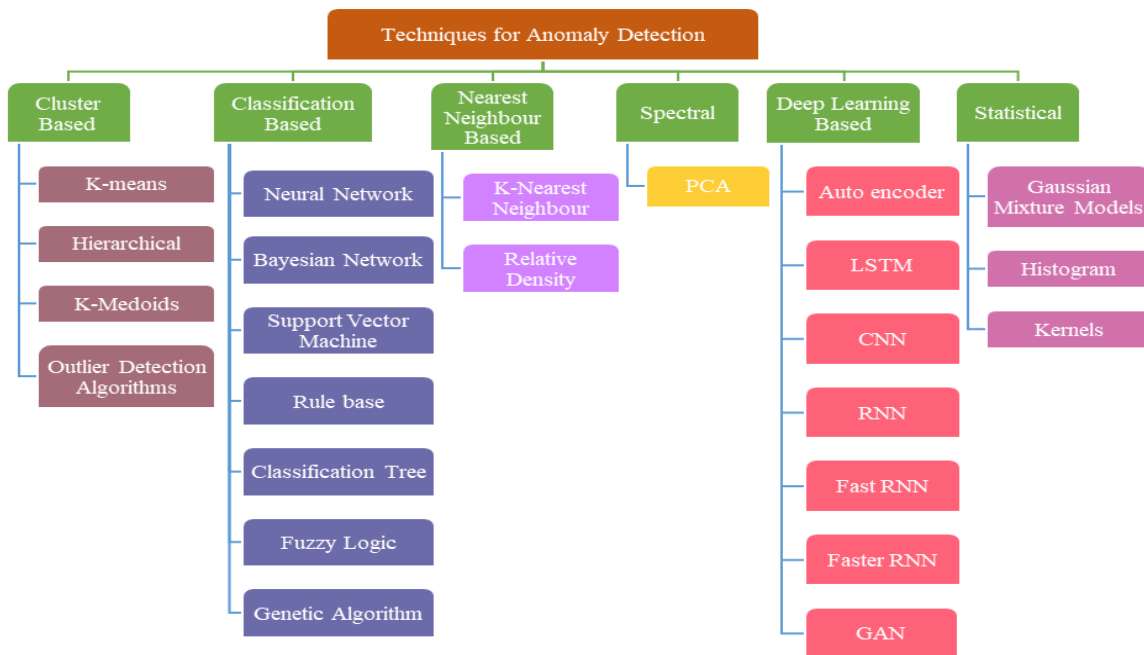


Figure 7 Anomaly Detection Techniques Classification

### G. Type of Techniques

Various existing anomaly detection techniques has been classified in figure-5 that are generally used for detecting anomalies in various domains and mainly five different classes for different applications domains are listed. Paper focused on video surveillance domain and in surveillance domain various open applications including computer network, land transport, banking, agriculture, education, and security. Some deep learning techniques are also available for anomaly detection is also available including Auto-encoders, Long Short Term Memory Networks, Restricted Boltzmann Machines, Deep Neural Networks Gated Recurrent Unit, Recurrent Neural Networks, Convolutional Neural Networks, Variation Auto-encoders, Generative Adversarial Networks. Nowadays, deep learning techniques achieves good performance and flexibility by learning to represent the data as a nested hierarchy of concepts within layers of the neural network. Deep learning outperforms the traditional machine learning as the scale of data increases as illustrated in Figure 7[5].

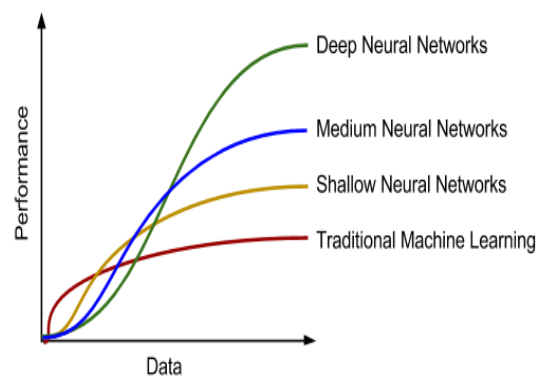


Figure 8 Performance Comparison of Deep learning-based algorithms Vs Traditional Algorithms Alejandro [2016].

## IV. RELATED WORK

Table-1 shows the survey of techniques and application domain of resent trends. Despite of application domain and particular traditional techniques nowadays researchers are using hybrid approach to solve the problems.



During 2006 and afterwards people are more doing research on how deep learning methods are used to solve different types infect despite of any domain how it will work. The advance techniques of deep learning has impressed the

researchers because these techniques gives better results and good accuracy but to achieve those benchmark result one need to high performance GPUs.

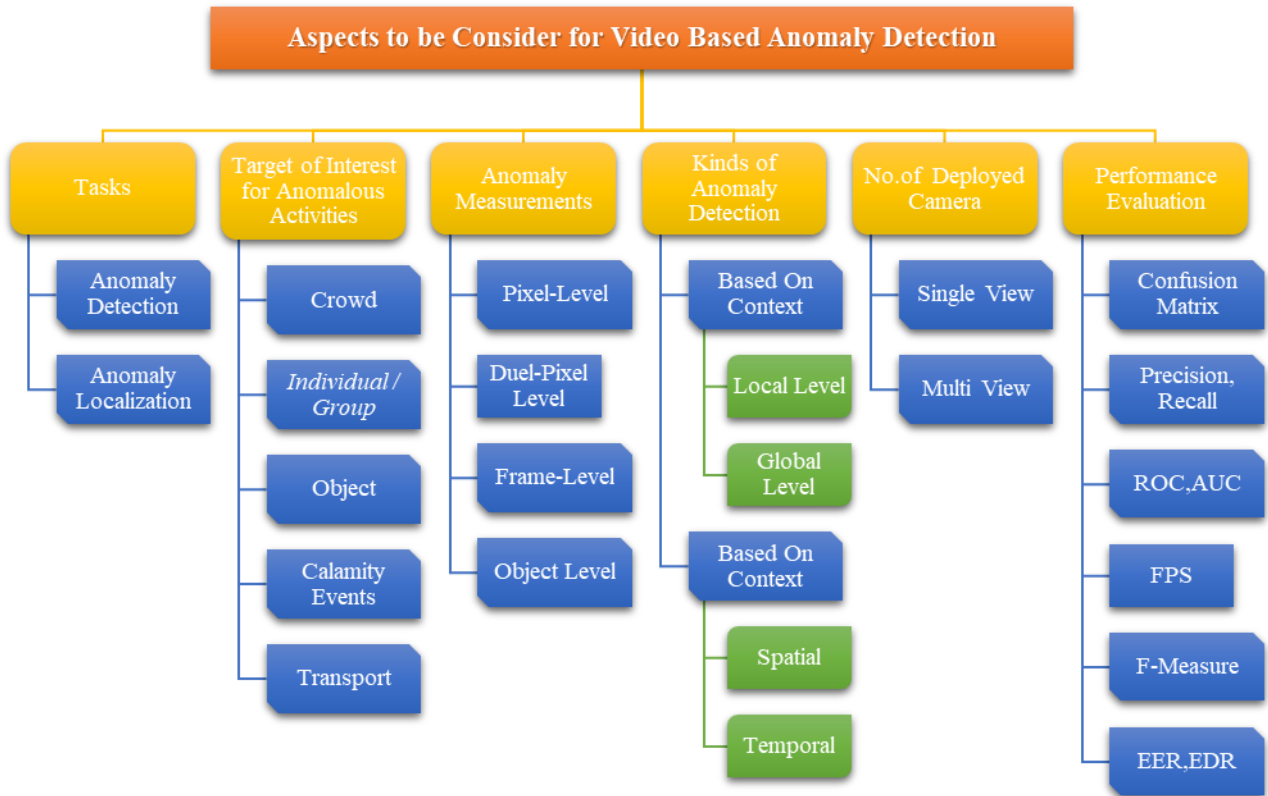


Figure 9 Anomaly detection approaches

Table 2 Comparison of our Survey to Related Survey Articles. 1 - Landi, Federico, Cees GM Snoek, and Rita Chuchvara [2019][4,10,11], 2- Lebichot, Bertrand, et al.[ 2019][4], 3 - Niculescu-Mizil, Alexandru, Eric Cosatto, and Felix Wu.[2018], Joshi, Shilpa, and R. K. Kulkarni [2019], Wu, Xiaohua, and Yan Nei Law [2018], 5- Mohammadi, Sara, et al. [2019], Kwon and Donghwoon Kwon et al. [2017], 6-Alnafessah, Ahmad, and Giuliano Casale [2019] 7 —Geert and Kooi et.al Litjens et al. [2017]. Rodriguez, Aitor Corchero, and Mario Reyes de los Mozos[2010], 8- Erfani, Sarah M., et al.[2016], 9- Xie, Junyuan, Linli Xu, and Enhong Chen.[ 2012],10- our Survey.

		1	2	3	4	5	6	7	8	9	10
	Detection										
	Log-Anomaly Detection							✓			✓
	Deep anomaly detection								✓		✓
	Image Processing									✓	✓

		1	2	3	4	5	6	7	8	9	10
Techniques	Supervised	✓	✓							✓	✓
	Unsupervised	✓									✓
	Semi Supervised	✓									✓
	Hybrid Models	✓	✓							✓	✓
	Neural Networks									✓	✓
	Deep Neural Network	✓	✓					✓		✓	✓
	one-Class Neural Networks							✓	✓		✓
	Deep Learning	✓						✓			✓
	Data Mining						✓	✓			✓
	Applications	Video Surveillance	✓								
Fraud Detection			✓								✓
Medical Anomaly Detection				✓							✓
Product Damage Detection					✓						✓
Cyber-Intrusion Detection						✓					✓
Big-data Anomaly							✓				✓

V. IMPLEMENTATION DETAILS FOR PROPOSED MODEL

The anomalies can't be always classified as an assault however it tends to be surprising action which is earlier not known. It might possibly be outliers. Detection of Anomaly is of a notable and emergent problem into many diverse fields like information theory, deep learning, computer vision, machine learning, and statistics that has been researched within various application from divers' domain including agriculture, health care, banking, education, and transport anomaly detection. Nowadays, at the point when information must be examined so as to discover a relationship or to predict known or unknown, classification, regression, and clustering, machine learning based, data mining based, and deep learning based strategies and techniques are utilized. To achieve a higher level accuracy rate (Sensitivity), and find Specificity rate of detected anomalous event or action from the information or data. Currently deep learning based hybrid approaches are also being developed and explored.



## Recent Advancement in Anomaly Detection in Surveillance Videos

The proposed methodology is abridged in Figure 10, the flow of the model first starts with collecting video data and convert them first into frames.

Segmented frames further divided into two categories normal class and abnormal class. Here normal means negative class. And abnormal means positive class. The normal class having

all normal frames and one in abnormal class must have at least one anomaly action or event should be present. Next step is to create features set from below display model (refer figure 10). Once received the feature set further proceed for object segmentation. The training of anomaly detection model using the proposed deep multiple instance learning (DMIL).

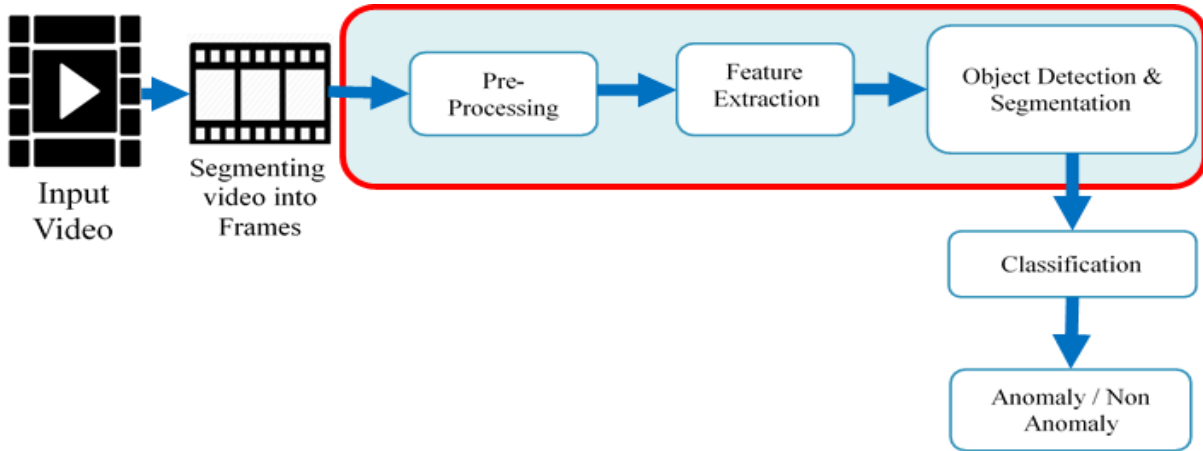


Figure 10 Flow of Detecting Anomalies from Surveillance Video Using Deep Learning

## VI. RESULTS

Refer below results of model which can detect and recognize the object. Some statistics given here based on own dataset. Here the comparison statistics are not mention. But the performance evaluation is done through above mention permeates (refer figure 9).

Confusion Matrix:

True positives (TP): These are cases in which we predicted yes.

True negatives (TN): These are cases in which we predicted No.

False positives (FP): Also known as a Type I error.

False negatives (FN): Also known as a Type II error.

Table 3 Confusion Matrix

	Predicted: NO	Predicted: YES
Actual: NO	TN	FP
Actual: YES	FN	TP

Accuracy:  $(TP+TN)/total$

Misclassification Rate :  $(FP+FN)/total$

True Positive Rate / Recall:  $TP/actual\ yes$

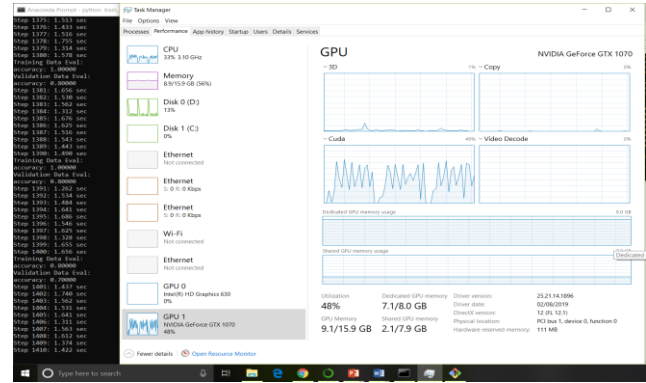
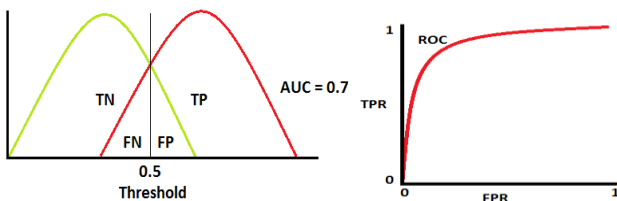
False Positive Rate:  $FP/actual\ no$

True Negative Rate/specificity:  $TN/actual\ no$

Precision:  $TP/predicted\ yes$

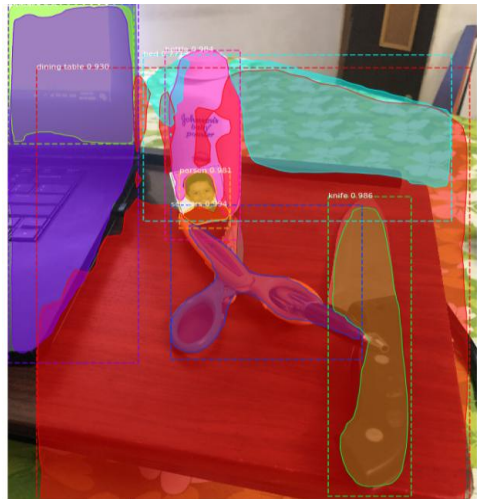
Prevalence:  $Actual\ yes/total$

ROC Curve, AUC:



Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, 112, 112, 16, 3)	0
conv3d_1 (Conv3D)	(None, 112, 112, 16, 64)	5248
max_pooling3d_1 (MaxPooling3)	(None, 56, 56, 16, 64)	0
conv3d_2 (Conv3D)	(None, 56, 56, 16, 128)	221312
max_pooling3d_2 (MaxPooling3)	(None, 28, 28, 8, 128)	0
conv3d_3 (Conv3D)	(None, 28, 28, 8, 128)	442496
max_pooling3d_3 (MaxPooling3)	(None, 14, 14, 4, 128)	0
conv3d_4 (Conv3D)	(None, 14, 14, 4, 256)	884992
max_pooling3d_4 (MaxPooling3)	(None, 7, 7, 2, 256)	0
conv3d_5 (Conv3D)	(None, 7, 7, 2, 256)	1769728
max_pooling3d_5 (MaxPooling3)	(None, 4, 4, 1, 256)	0
flatten_1 (Flatten)	(None, 4096)	0
dense_1 (Dense)	(None, 2048)	8390656
dropout_1 (Dropout)	(None, 2048)	0
dense_2 (Dense)	(None, 2048)	4196352
dropout_2 (Dropout)	(None, 2048)	0
dense_3 (Dense)	(None, 101)	206949
activation_1 (Activation)	(None, 101)	0
Total params: 16,117,733		
Trainable params: 16,117,733		
Non-trainable params: 0		

VII. MATH



VIII. CONCLUSION

The Proposed multi-instance learning model is a way to deal with identifying inconsistencies and abnormalities in surveillance videos. Because of the complexity of realistic anomalies, through only normal data may not be optimal for anomaly detection, the nature of these practical abnormalities, utilizing just normal class may not be ideal for discovery of the abnormal event. Here endeavor design for both positive and negative class videos. To avoid labor-intensive temporal annotations of anomalous segments in training videos, try to learn a general model of anomaly detection using Multiple Instance Learning frameworks with weakly labelled data. For validation, an introduce verity of anomaly dataset having different types of an anomaly. The exploratory results of object segmentation on some benchmark dataset and private small dataset demonstrate that the proposed abnormality identification approach performs essentially improved.

REFERENCES

1. Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Outlier detection: A survey." ACM Computing Surveys 14 (2007): 15.
2. Hawkins, Douglas M. Identification of outliers. Vol. 11. London: Chapman and Hall, 1980.
3. Lin, Tsung-Yi, et al. "Microsoft coco: Common objects in context." European conference on computer vision. Springer, Cham, 2014.
4. Waqas Sultani, Chen Chen, and Mubarak Shah, "Real-world anomaly detection in surveillance videos", in CVPR, 2018.
5. Bahnsen Alejandro, Correa. Building ai applications using deep learning. 2016. URL <https://blog.easysol.net/wp-content/uploads/2017/06/image1.png>.
6. "Unusual crowd activity dataset of university of minnesota", <http://mha.cs.umn.edu/>.
7. Chalapathy, Raghavendra, and Sanjay Chawla. "Deep Learning for Anomaly Detection: A Survey." arXiv preprint arXiv:1901.03407 (2019).
8. Srivastava, Nitish, Elman Mansimov, and Ruslan Salakhudinov. "Unsupervised learning of video representations using lstms." International conference on machine learning. 2015.
9. Miljković, Dubravko. "Review of novelty detection methods." The 33rd International Convention MIPRO. IEEE, 2010.
10. Landi, Federico, Cees GM Snoek, and Rita Cucchiara. "Anomaly Locality in Video Surveillance." arXiv preprint arXiv:1901.10364 (2019).
11. Sun, Jiayu, Jie Shao, and Chengkun He. "Abnormal event detection for video surveillance using deep one-class learning." Multimedia Tools and Applications 78.3 (2019): 3633-3647.

12. Lebichot, Bertrand, et al. "Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection." INNS Big Data and Deep Learning conference. Springer, Cham, 2019.
13. Niculescu-Mizil, Alexandru, Eric Cosatto, and Felix Wu. "Reconstructor and contrastor for medical anomaly detection." U.S. Patent Application No. 15/983,392.
14. Joshi, Shilpa, and R. K. Kulkarni. "Medical Image Enhancement Using Hybrid Techniques for Accurate Anomaly Detection And Malignancy Predication." Third International Congress on Information and Communication Technology. Springer, Singapore, 2019.
15. Wu, Xiaohua, and Yan Nei Law. "Anomaly Detection for Medical Samples under Multiple Settings." U.S. Patent Application No. 15/447,315.
16. Michalski, Christoph W., et al. "Prophylactic onlay reinforcement with absorbable mesh (polyglactin) is associated with less early wound complications after kidney transplantation: A preliminary study." Journal of Biomedical Materials Research Part B: Applied Biomaterials (2019).
17. Kwon, Donghwoon, et al. "A study on development of the blind spot detection system for the IoT-based smart connected car." 2018 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2018.
18. Rodriguez, Aitor Corchero, and Mario Reyes de los Mozos. "Improving network security through traffic log anomaly detection using time series analysis." Computational Intelligence in Security for Information Systems 2010. Springer, Berlin, Heidelberg, 2010. 125-133.
19. Erfani, Sarah M., et al. "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning." Pattern Recognition 58 (2016): 121-134.
20. Yu, Jiahui, et al. "Unitbox: An advanced object detection network." Proceedings of the 24th ACM international conference on Multimedia. ACM, 2016.
21. Alnafessah, Ahmad, and Giuliano Casale. "Anomaly Detection for Big Data Technologies." 2018 Imperial College Computing Student Workshop (ICCSW 2018). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.
22. Xie, Junyuan, Linli Xu, and Enhong Chen. "Image denoising and inpainting with deep neural networks." Advances in neural information processing systems. 2012.

AUTHORS PROFILE



**Priyanka Patel** is working as an Assistant Professor at Department of Information Technology in Chandubhai S Patel Institute of Technology, CHARUSAT since May, 2013. She has received her Bachelor degree in Information Technology in the year 2006 with First Class. She got Master degree in Computer Engineering from Chandubhai S Patel Institute of Technology, CHARUSAT, in the Year 2013. Her area of interest is in Image and Video Processing, Programing in C, Object oriented programming, Software Engineering. She is a life time member of Professional Society CSI. She has more than eleven years of teaching experience at UG level. She is having good teaching and research interest in Image and Video Processing. She has previously worked in A.D.Patel Institute of Engineering collage, New Vallabh Vidya Nagar in year of 2008 to 2009 as a lecturer. She has qualified GATE in the year 2010.



**Dr. Amit Thakkar** is working as an Assistant Professor at Department of Information Technology in Chandubhai S Patel Institute of Technology, CHARUSAT since 2002. He has 19 years of teaching experience. He is having good teaching and research interest in data mining, Machine learning, deep learning. He has published more than 50+ research papers in reputed journals.