GMR Institute of Technology
An Autonomous Institute Affiliated to JNTUK, Kakinada

GMRIT
Training Tomorrow's Engineers Today

ANOMALY DETECTION TECHNIQUES IN CROWDED AREAS

A project report submitted in partial fulfilment of the requirement for the award of degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

Submitted by

POTNURU DEEPIKA
(19341A05D5)

UPPARAPALLI RAMESH
(19341A05H5)

SAPPA SIVA SANKAR
(19341A05F1)

BODDU ANITHA
(20345A0517)

PULAVARTI PREETHI
(19341A05D8)

Under the esteemed guidance of

DR. R. SRINIVASA RAO

Assistant Professor, Dept. of CSE

GMR Institute of Technology
An Autonomous Institute Affiliated to JNTUK, Kakinada
(Accredited by NBA, NAAC with 'A' Grade & ISO 9001:2008 Certified Institution)

GMR Nagar, Rajam – 532127,
Andhra Pradesh, India

April 2020

GMR Institute of Technology
An Autonomous Institute Affiliated to JNTUK, Kakinada

GMRIT
Training Tomorrow's Engineers Today

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the thesis entitled **ANOMALY DETECTION TECHNIQUES IN CROWDED AREAS** submitted by **Potnuru Deepika (19341A05D5), Upparapalli Ramesh (19341A05H5), Sappa Siva Sankar (19341A05F1), Boddu Anitha (20345A0517)** and **Pulavarti Preethi (19341A05D8)** has been carried out in partial fulfilment of the requirement for the award of degree of **Bachelor of Technology** in **Computer Science and Engineering** of **GMRIT, Rajam** affiliated to **JNTUK, KAKINADA** is a record of bonafide work carried out by them under my guidance & supervision. The results embodied in this report have not been submitted to any other University or Institute for the award of any degree.

Signature of Supervisor
Dr.R. Srinivasa Rao
Assistant Professor
Department of CSE
GMRIT, Rajam.

Signature of HOD
Dr. A. V. Ramana
Professor& Head
Department of CSE
GMRIT, Rajam.

The report is submitted for the viva-voce examination held on ……..

Signature of Internal Examiner

Signature of External Examiner

ACKNOWLEDGEMENT

It gives us an immense pleasure to express deep sense of gratitude to my guide **Dr. R. Srinivasa Rao,** AssistantProfessor, Department of Computer Science and Engineering for his whole hearted and invaluable guidance throughout the project work. Without his sustained and sincere effort, this project work would not have taken this shape. He encouraged and helped us to overcome various difficulties that we have faced at various stages of our project work.

We would like to sincerely thank our Head of the department **Dr. A. V. Ramana**, for providing all the necessary facilities that led to the successful completion of our project work.

We would like to take this opportunity to thank our beloved Principal **Dr.C.L.V.R.S.V.Prasad**, for providing all the necessary facilities and a great support to us in completing the project work.

We would like to thank all the faculty members and the non-teaching staff of the Department of Electronics and Communication Engineering for their direct or indirect support for helping us in completion of this project work.

Finally, we would like to thank all of our friends and family members for their continuous help and encouragement.

Potnuru Deepika	**19341A05D5**
Upparapalli Ramesh	**19341A05H5**
Sappa Siva Sankar	**19341A05F1**
Boddu Anitha	**20345A0517**
Pulavarti Preethi	**19341A05D8**

ABSTRACT

Anomaly detection is the approach to determine unusual conditions or observations that are statistically different from the rest of the observations. It is used for detecting abnormal events in crowded areas like roads, rallies, hospitals, any public gatherings and traffic signals etc. Now-a-days, popularity of surveillance cameras is increasing. There are protection cameras in public places like railway station, airport and many others. Private organizations also have security cameras in their premises to deal with security challenges like robbery, fire accidents or any abnormal situations. If the situation is significantly different from the normal situation then it is detected as abnormal situation. From these security cameras, detecting abnormal events manually requires a security person completely hired which results in additional budget to the organization. But, there exist a lot of methods to detect abnormal activities in a given video stream without man power. Now-a-days, Deep learning has clearly proven its functionalities in a wide range of domains, including sounds, images, videos, and Natural Language Processing. Deep Learning techniques such as Convolutional Neural Networks (CNNs), Graph Neural Networks (GNNs) etc are abundantly used for handling abnormal event detection in fast and efficient manner. In this project, recent 3D CNN based models will be used for handling abnormal event detection. For the experimentation, Avenue dataset is considered with normal and abnormal crowd behavior videos of different scenes. The performance of the model is evaluated with an accuracy metric that gives the percentage of correctly classified frames in comparison to the ground truths.

Keywords: *Anomaly Detection, video surveillance, Deep learning, Convolutional Neural Network, Spatio-Temporal Autoencoder* .

TABLE OF CONTENTS

LISTOF TABLES

LISTOF FIGURES

LIST OF SYMBOLS & ABBREVIATIONS

AUC : Area Under Curve

CA(F) : Certain Activation (Function)

CIC-IDS : Canadian Cyber Security Institute Dataset

CNN : Convolutional Neural Network

DL : Deep Learning

EER : Equal Error Rate

FCN : Full Connected Neural

FPS : Frame Per Second

ISTL : Incremental Spatio Temporal Learner

IT : Information Technoloy

MAD : Magnetic Anomaly Detection

MII : Motion Information Image

ML : Machine Learning

MSA : Multi Staged Attention

OBF : Orthonormal Basic Function

PL : Pooling Layer

RNN : Recurrent Neural Network

STAE : Spatio Temporal Auto Encoder

STFT : Short Term Fourier Transform

SVM Support Vector Machine

1.INTRODUCTION

In recent times, the evolved countries are enhancing the security devices to safe guard and control the public and private crowd. Anomaly detection is a significant issue in a crowded region. Since, people have been made injuries and damages in public vicinity. So, often if any anomaly has come about in a crowded place, the anomaly detection is critical to protect humans and the surroundings without any extreme impairment. While the anomaly is perceived, alerting crowd human beings via an alerting device could be very imperative. Now- a- days, especially in non-public and public crowded place, the government desires a approach to offer protection with low cost.

Fig1.1 Security Person at CC Camera office

1.1 Why Deep Learning?

Humans want safety in mass assemblies, public and private events. Hence the Deep Learning is giving knowledge based on computer imaginative approach that gives a variety of gifted strategies for personal and public protection. This anomaly detection machine gives a solution to discover abnormal events in crowded videos and set alarm for public safety in mass gatherings. The deep learning techniques such as Convolution Neural Network(CNN) is used to come across anomaly on the preliminary level from the entire video to keep away from damages. While the anomaly is perceived, alerting crowd human beings via an alerting device could be very imperative. The alerting gadget is one kind of form which include tones,

voice and alert messages. After detecting anomaly in the crowd, the alarm gadget must intimate message or make sound mechanically While the anomaly is perceived, alerting crowd human beings via an alerting device could be very imperative. The alerting gadget is one kind of form which include tones, voice and alert messages. After detecting anomaly in the crowd, the alarm gadget must intimate message or make sound mechanically.

1.2 Abnormal Actions :

Anomaly detection from a video is one of the fundamental tasks in a video surveillance system. Surveillance cameras are increasingly being distributed and used for different purposes, such as security reasons, avoiding traffic congestion, and crowd control. An abnormal event is an event that affected by external causes; for example, an escape that may be caused by a natural disaster earthquake, or by other abnormal behavior, i.e. explosion. While abnormal behavior is an attitude related to conducting individual or group activities.

1.3 Anomaly detection :

Anomaly detection is the identification of rare events, items, or observations which are suspicious because they differ significantly from standard behaviors or patterns. Anomalies in data are also called standard deviations, outliers, noise, novelties, and exceptions.In the network anomaly detection/network intrusion and abuse detection context, interesting events are often not rarejust unusual. For example, unexpected jumps in activity are typically notable, although such a spurt in activity may fall outside many traditional statistical anomaly detection techniques.

Fig1.2 Security Team identified Anomaly Event

1.4 Why Anomaly Detection Is Important?

It is critical for network admin to be able to identify and react to changing operational conditions. Any nuances in the operational conditions of data centers or cloud applications can signal unacceptable levels of business risk. On the other hand, some divergences may point to positive growth. Therefore, anomaly detection is central to extracting essential business insights and maintaining core operations. Consider these patterns all of which demand the ability to discern between normal and abnormal behavior precisely and correctly like- An online retail commercial enterprise ought to expect which discounts, events, or new merchandise can also additionally cause boosts in income so one can growth call for on their web servers, An IT safety group prevent to save you hacking and desires to detect abnormal login patterns and user behaviours and A cloud provider has to allot traffic and services and has to assess changes to infrastructure in light of existing patterns in traffic and past resource failures.

Fig1.3 Abnormal Events

A evidence-based, well-constructed behavioural model can not only represent data behaviour, but also help users identify outliers and engage in meaningful predictive analysis. Static alerts and thresholds are not enough, because of the overwhelming scale of the operational parameters, and because it's too easy to miss anomalies in false positives or negatives. To address these kinds of operational constraints, newer systems use smart algorithms for identifying outliers in seasonal time series data and accurately forecasting periodic data patterns.

1.5 How Anomaly Events Are Detected ?

Deep learning-based anomaly detection algorithms have achieved high accuracy in automatically detecting anomalous activities such as falling of objects, anomalous access in restricted areas, traffic accidents, traffic laws violations, criminal activities, and many more. Anomaly detection algorithms usually use normal events as training data for training of models, and then apply model on online data to detect anomalies. The proposed algorithm divides video frames into variable sized cells. In the proposed particle filtering based technique, we first predict possible activities in a video frame.

Fig1.4 Normal vs Abnormal Events

These predictions are further refined with the update step where, motion, location and size features extracted from video frames along with a clustering algorithm are used. This update step evaluates the posterior distribution of possible activities in video sequences which helps to classify video frames into two classes: anomalous and normal. Deep learning mainly focuses on data represented in a vector form, which pay little attention to the impact of the internal structure characteristics of feature vector on classifying and determining abnormal events in video sequences.

1.6 Techniques for Detection :

With the development of machine learning studies, various approaches based on deep learning have achieved remarkable progress in abnormal event detection for example, Convolutional Neural Networks (CNNs), Recurrent Neural Networks(RNN). A general definition of anomaly detection is the identification of behaviors that do not conform to expected and accepted behavior i.e., normal behavior and other deep learning models can learn better feature representation than hand-crafted feature modeling. It is conductive to determinate the occurrence of abnormal event in video sequence. The proposed framework demonstrates an outstanding performance when compared with other state-of-the art online and offline anomaly detection

techniques. Anomaly detection algorithms usually use normal events as training data for training of models, and then apply model on online data to detect anomalies.

1.7 Applications :

Video surveillance is a predominant consideration in the development, operation, and sustainability of modern industrial and urban environments. It contributes toward efficiency, safety, security, and optimality of the locality, infrastructure, individuals, operations, and activities. Industrial environments are transitioning toward autonomous machinery, cyber-physical systems, and energy-efficient layouts. Urban environments are becoming densely populated, with high usage of multilevel buildings, increased vehicular, pedestrian, behavior as it evolves over time.

2.LITERATURE SURVEY

[1]Direkoglu, C. (2020). Abnormal crowd behaviour detection using motion information images and convolutional neural networks. ***IEEE Access, 8,*** **80408-80416.**

Optical flow vectors are used to generate a Motion Information Image (MII) from the video, then to train a Convolutional Neural Network (CNN) for anomaly detection in crowded region. Abnormal event detection can be differentiated into two types i.e. Local abnormal events and global abnormal events.The methods used for global crowd behaviour analysis is object-based approach. Here group of individuals are considered as objects. The object-based methods are closer in finding perfect results of crowd identification, tracking and action recognition in dense crowds etc. Anomaly detection has 2 main phases i.e. Event representation and Anomaly measurement.MII generation is based on the angle difference between optical flow vectors in consecutive frames and the optical flow magnitude in the current frame.This have used two public datasets namely UMN and PETS2009.The accuracy was 98.08% and 98.39% respectively.

[2] Nawaratne, R., Alahakoon, D., De Silva, D., & Yu, X. (2019). Spatiotemporal anomaly detection using deep learning for real-time video surveillance. ***IEEE Transactions on Industrial Informatics, 16*****(1), 393-402.**

Incremental Spatio Temporal Learner (ISTL) is unsupervised deep learning that utilizes active learning with fuzzy aggregation and distinguish the normal and abnormal events.It is unreasonable and impossible for human observers to examine and evaluate every video transmission.The method produced positive results by reconstructing input video with a ten-layered fully convolutional feed-forward autoencoder and detecting anomalies based on the reconstruction cost analysis.The three steps of ISTL are of spatiotemporal learning, anomaly detection and localization, and active learning using fuzzy aggregation.For visual anomaly identification, deep learning, convolutional neural networks (CNN), autoencoders, and recurrent neural networks (RNN) have been used.Three benchmark video surveillance datasets namely Pedestrian datasets and Avenue dataset are used.

[3] Mehmood, A. (2021). Efficient Anomaly Detection in Crowd Videos Using Pre-Trained 2D Convolutional Neural Networks. *IEEE Access, 9,* 138283-138295.

This paper mainly focused to reduce the computational cost approach in detection of crowd anomaly. It has 3 levels to detect the Abnormal situation in surveillance video. Crowd Unusual activity measured by different parameters like Movement pattern, Speed and Emerging point. The focus is about to detect the abnormal activities like Escape Panics and Violent interactions like fighting and trampling. MN, hockey fights, and violent flows datasets were experimented and efficiently detected the different abnormalities with an accuracy of 99.12%, 99.71%, and 98.81%, respectively.

[4]. Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A spectrogram image-based network anomaly detection system using deep convolutional neural network. IEEE Access, 9, 87079-87093.

The Network is secured by using authentication, firewall, and encryption are used but these security functions are not sufficient to secure the network. The main focus of the author to provide the extra security by using Convolution Neural networks, The dataset CIC-IDS2017(Canadian Cyber Security Institute Dataset) are used which contains different attacks like web attack ,port scan ,Dos .First it capture the network packets by using packet sniffing tool. the useful features are extracted and stored in a dataset and cleaned and remove the empty entries. After that the data set is normalized and encoded.The updated dataset is used for spectrogram generation by using (short term Fourier transform) STFT. The train data set is used for deep CNN model and the best model is used for testing.After that the model testing stage takes place. If any attack is detected an alarm signal is generated otherwise it will consider as normal flow.

[5] Almazroey, A. A., &Jarraya, S. K. (2020, April). Abnormal Events and Behavior Detection in Crowd Scenes Based on Deep Learning and Neighborhood Component Analysis Feature Selection. In The International Conference on Artificial Intelligence and Computer Vision (pp. 258-267). Springer, Cham..

The main aim of this paper is to reduce the man power and to save time and cost to detect abnormal events that occur in the crowded areas. The Algorithm that used in this paper is Convolution neural networks, SVM, Cosine similarity are used. The Datasets that used in this paper is USCD Ped1, UCSD Ped2, Avenue and Hockey datasets which contains abnormal events and behaviors. The detection can occurs in two stages.in stage one the input video is divided into different frames and by using cosine similarity and keyframe selection. By testing on different datasets and by comparing the set of features by the NCA which gives the less lambda value that gives high accuracy.

[6].Tariq, S., Farooq, H., Jaleel, A., & Wasif, S. M. (2021). Anomaly detection with particle filtering for online video surveillance. IEEE Access, 9, 19457-19468.

The main aim of this paper, is to detect the anomaly detection that occurs in the video surveillance. A particle filtering based anomaly detection are used in this paper size, motion and location features are used for prediction and posterior probability of activities are used for measurementsmodels. The datasets that used in this paper is USCD and LIVE datasets. The input video is divided into video frames and by using filtering-based technique are used for prediction of size motion ,location and extract features. To calculate the size of the video frame the background subtraction algorithm is used. Equal Error Rate(EER) and Area Under the Curve are the performance metric that are used to evaluate the frame work.

[7].Cruz-Esquivel, E., & Guzman-Zavaleta, Z. J. (2022). An examination on autoencoder designs for anomaly detection in video surveillance. *IEEE Access*.

Now-a-days Video monitorization generates high amount of data so it requires automatic analysis that intelligent surveillance system could perform. So that these intelligent systems should detect anomalies automatically. ST-AT,S3D-G, D3D are three novel models used for anomaly detection. The S3D-G combines 2D with 3D convolutional layers with good accuracy results and less computational resources.In videos 2D convolution are only characterised only for present frame and without relation past and future frames. a consecutive set of 2D convolutions need to solve this problem. 2D convolution was not completely discarded some modifications are applied like adding two stream approach with gaussian mixture techniques like GMM-DAE to improve results.This model evaluation uses the metrics AUC-ROC and EFF, the top-heavy model is 57% effective than 3D auto encoder, it has 87% AUC-ROC and 14 %EER.

[8].Duman, E., &Erdem, O. A. (2019). Anomaly detection in videos using optical flow and convolutional autoencoder. *IEEE Access*, 7, 183914- 183923.

Convolution autoencoders and convolution long short term memory methods have used in anomaly detection.Dense optical flow is applied so that velocity and direction of objects is extracted. the most popular feature extraction method based on spartio and temporal features is optical –flow. Convolution Trajectory -based approaches in sparse frames are used to track the velocity of object which is accurate but in crowded detecting and tracking objects is difficult.In convolution of auto encoders mainly there are 3 stages they are pre-processing aims to extract dense optical flow of each frame .In the second stage, the convolutional autoencoder is used in order to obtain the spatial structure of each dense optical flow map volume. The last stage includes a convolutional long short-term memory network to learn the temporal patterns of encoded optical flow. The inputs of the framework are formed by optical flow displacements areas between eight consecutive video frames. UCSD ped1,UCSD ped2 ,avenue are datasets taken the AUC score of datasets are 92.4%,92.7% and 89.5% respectively.

[9]Javed, A. R., Usman, M., Rehman, S. U., Khan, M. U., &Haghighi, M. S. (2020). Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4291-4300.

This paper is mainly based upon detect anomaly on vulnerable cause by faults/errors generated by sensor data which cause accidents .To help in avoiding in such accidents by timely detecting anomaly a method with a combination of multi staged attention mechanism with long short-term memory-based convolution neural network namely MSALSTM-CNN.Another method namely WAVED the method is used to detect anomaly in multi sensor streams of data using optimal weight vectors of classifier.There are mainly 4 types of anomalies added like instant, constant,gradual drift and bias.MSALSTM-CNN and WAVED methods performance are evaluated. These standard performance metrics are used for distinguish between normal and anomalous instances. SPMD is the dataset taken in the paper ,at low magnitude the accuracy score is more with Msalstm-CNN of 95.7% whereas at high magnitude the accuracy score is with waved of 99.8%.

[10]Ullah, W., Ullah, A., Haq, I. U., Muhammad, K., Sajjad, M.,&Baik, S. W. (2021). CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks. Multimedia Tools and Applications, 80(11), 16979- 16995.

CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks generate an extensive extent of video facts on a day-by-day. Features-primarily based wise anomaly detection framework which could function in surveillance networks with decreased Time complexity.In the proposed framework, we first extract spatiotemporal functions from a chain of frames by Passing everyone to a pre-educated convolutional neural community (CNN) version.The functions extracted from the Sequence of frames are valuable in capturing anomalous events. We then pass the extracted deep functions to Multilayer bi-directional lengthy brief-time period reminiscence (bd-lstm) version, that may as it should be classify ongoing Anomalous/regular occasions in complex surveillance scenes of smart cities.

[11]Ye, O., Deng, J., Yu, Z., Liu, T., & Dong, L. (2020).Abnormal event detection via feature expectation subgraph calibrating classification in video surveillance scenes. IEEE Access, 8, 97564-97575[11]

At present, the being abnormal event discovery models grounded on deep literacy substantially concentrate on data represented by a vectorial form.Once the frames of video are represented using feature expectation subgraphs, we can use them to classify and recognize anomaly. First let {G 0, y 0 i} n i=1 be the corresponding labelled feature expectation subgraphs for n frames from N training videos {Vi} N i=1, where the label y 0 i is −1 for feature expectation subgraphs of abnormal event and +1 for feature expectation subgraphs of normal event.The accuracy of abnormal event detection can be improved by using the classification of feature expectation subgraphs to calibrate the results of a single classifier.

[12]Franklin, R. J., &Dabbagol, V. (2020, January). Anomaly detection in videos for video surveillance applications using neural networks. In 2020 Fourth International Conference on Inventive Systems and Control (ICISC) (pp. 632-637). IEEE.

Anomaly discovery is a fashion used to distinguish colorful patterns and identify unusual patterns with a minimum period, this pattern is called outliers. Surveillance videos can capture a variety of realistic anomalies. Anomaly discovery in videotape surveillance involves breaking down the whole process into three layers, which are video tag, image processing, and exertion discovery.Security surveillance is decreasingly employed at public places similar as thoroughfares, hospitals, corners, shopping promenades, and banks, to guarantee public safety. Because anomalous events infrequently appear in real life, behavioral or appearance patterns swinging from normal patterns are frequently.

[13] Liu, S., Chen, Z., Pan, M., Zhang, Q., Liu, Z., Wang, S., ... & Wan, C. (2019). Magnetic anomaly detection based on full connected neural network. *IEEE Access*, *7*, 182198-182206.

Magnetic anomaly detection (MAD) is used to detect some hidden ferromagnetic objects.Orthonormal basis function (OBFs) detector is a prominent method of MAD.The result displays that proposed method i.e. FCN(Full Connected Neural) method performs better when compared to other methods. It also displays the increase in detection probability by comparing different noises.The FCN(Full Connected Neural) algorithm is used. The features are extracted from measured signal, are delivered to the neural network as inputs.Here feature extraction involved the following steps: Data preparation,Modelbuilding,Model training, Model evaluation and FCN.After the evaluation of detector's performance for detecting the anomaly signal involved in noise under different SNRs and orientations.The results proved that the proposed method has higher detection probability than traditional OBFs method.

[14] Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. *IEEE access*, *6*, 48231-48246.

A GPU-powered test-bed with keras and theano backend was used for deep model training and evaluation. To improve the reliability of model comparisons, we combined traditional ML IDS models with well-known classification techniques such as Extreme Learning Machine, k-NN, Decision-Tree, Random-Forest, Support Vector Machine, Naive-Bays, and QDA.Both DNN and traditional ML models were evaluated using well-known classification metrics such as the RoC Curve, Area under the RoC, Precision-Recall Curve, mean average precision, and classification accuracy.Both the DCNN and LSTM models performed extremely well on the test dataset.Hence by comparing, with 85 percent and 89 percent accuracy this model proved that Deep Learning is not only a workable but also an interesting technology for information security applications and other application domains.

[15] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Transactions on Network and Service Management*, *16*(3), 924-935.

This paper presents a robust hybrid model for detecting network anomalies in cloud environments, with a focus on streaming data. The model takes advantage of the benefits of multiobjective optimization and deep learning, specifically for feature extraction and anomaly detection on real-time network traffic streams. Datasets used are Benchmark dataset-DARPA'98, Benchmark dataset-KDD'99 and Synthetic dataset.GWO and CNN, two computationally efficient techniques, were used for this purpose. The combination of these techniques is promoted further by restructuring their respective standard strategies. Moreover, the proposed hybrid model was thoroughly tested on benchmark and synthetic datasets. The obtained results clearly demonstrate the good performance of the proposed model over the old systems.

Sl.no	Technique (i.e. author names with reference number)	year	Description	Limitations	Advantages	Performance metrics	Gaps
1	Cem Direkoglu	2020	Focus to detect the panic and escape behaviour in global events using Motion Information Image(MII) and Optical flow vectors	Adjustment of the input image and size according to a pre-trained network, and replace the final layers to have only two classes.	New motion information image (MII) generation using optical flow,	Accuracy. It was 98.08% and 98.39% for UMN and PETS2009 datasets respectively.	Image size taken accordingly to fill the video and frames.
2	Rashmika Nawaratne , Damminda Alahakoon, Daswin De Silva and Xinghuo Yu	2020	Humans are unrealistic and infeasible to monitor and analyse every video stream with high precision	Tightly coupled dependence on a known normality training dataset and sparse evaluation based on reconstruction error.	Good efficiency , safety and security in modern industrial and urban area.	Accuracy,Robustness,Computational overhead and contextua inducatore.	Depenedency and sparse evalution have to be taken care.

3	Abid Mehmood	2021	Implements a lighter form of the 2D CNN to achieve high recognition accuracy at low computational cost	Resource Loads	Low computational cost approach to detect the crowd anomaly.	Accuracy .UMN, hockey fights, and violent flows datasets were used and have an accuracy of 99.12%, 99.71%, and 98.81%, respectively.	Resource loads have to minimizes as possible as.
4	Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F.	2021	Provide security from cyberattacks	This method is struggled to detect the attacks with low training sample and complexity is related to detection accuracy.	Provide the extra security to the network and gives the sign if the network is attacked.	Achieving 98.75 accuracy than other DL algorithms by using the evolution metrics such as Accuracy, precision, Recall, F1-score.	Shows inefficiency to detect novel and zero day attacks which have increased the false alarm rate.
5	Almazroey, A. A., & Jarraya, S. K.	2020	It will save the man power by using CNN and NCA	In crowded scenes a trajectory based approach becomes unreliable and it is limited by occlusion.	Reduce the man power and to save time and cost to detect abnormal events that occur in the crowded areas.	Area Under ROC Curve (AUC) are used as the measurements to evaluate the model.	Hand-crafted approach that trained and designed to detect abnormal events for a particular scene under specific condition.

6	Tariq, S., Farooq, H., Jaleel, A., & Wasif, S. M	2021	Detection of anomaly behavior by using particle filtering	Shows relatively smaller detection accuracy.	Providing Security from threats and detect abnormal events.	Equal Error Rate(EER) and Area Under the Curve and the processing time .	Histograms of optical flow is analyzed to construct various models.
7	Cruz-Esquivel	2022	Mainly focused on anomaly detection also reduce computational cost with best methods.	Cost is high while using in real time application. Needs a lots of training data for more accuracy.	It shows the best feasibility of reducing the computational resources requirements with smaller architectures.	The top heavy model is 57%effective than 3D auto encoder. It has 87% AUC-ROC and 14 %EER .	The model needs more processing time to train the data.
8	Duman, E., &Erdem,	2019	Automated anomaly detection in vedio surveillance in real time with high accuracy.	Within the area is to find out in which video frames anomalies occur and to localize regions that cause anomalies within these video clips.	The main advantage of using Conv-LSTM is more robust results in complex scenes with frequent occlusions.	UCSD ped1,UCSD ped2 ,avenue are datasets taken the AUC score of datasets are 92.4%,92.7 % and 89.5% respectively. .	The interaction forces between foreground objects in addition to optical flow information without reducing model is need for real-time applications.

9	Javed, A. R., Usman, M., Rehman, S. U., Khan, M. U., & Haghighi, M. S.	2020	Sensor generated error data causes accidents and vulnerable causes cyber attacks to reduce such anomalies MSALSTM-CNN named model is used.	Poor detection performance over lower magnitudes of anomalous data.	MSALSTM-CNN effectively enhances the anomaly detection rate in both low and high magnitude cases.	The accuracy score is more with MSALSTM-CNN of 95.7% whereas at high magnitude the accuracy score is with waved of 99.8%. .	The MSALSTM-CNN method that can effectively detect anomalies with low magnitude to assure the high reliability of the fused data.
10	U., Muhammad	2021	Focus on CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks	For instance, changing the dictionary learned from normal events to anomalous events results in a high false alarm rate	CNN features from a series of video frames and feed them to the proposed residual attention-based long short-term memory (LSTM) network.	State-of-the-art models with a 1.77%, 0.76%, and 8.62% increase in accuracy on the UCF-Crime, UMN and Avenue datasets, respectively	Detected by our current framework.
11	Ye, O., Deng, J., Yu, Z., Liu, T., & Dong, L.	2020	Abnormal event detection via feature expectation subgraph calibrating classification in video surveillance scenes	Based on long-short term memory network are that the feature of noise interference will	The main adavantage of convolutional neural network and long short-term memory models to extract	UCSD ped1,UCSD ped2 ,avenue are datasets taken the AUC score of datasets are 99.59%,99.28% and 99.01% %	To improve in complex video surveillance scenes, and the graph kernel

				continue to spread in the process of recurrent neural network	thespatiotemporal features of video frame,	respectively	model also needs to improve
12	Franklin, R. J., & Dabbagol, V	2020	Anomaly detection in videos for video surveillance applications using neural networks.	Anomalous events are defined as all rare or different events, collecting sufficient training data for anomalous events can be difficult.	Advantage demand in the protection of safety, security and personal properties, the needs and deployment of video surveillance systems	Ped1 and Ped2 which contain score 89.4% ,90.1% with 40 abnormal events and 2,010 frames with 12 abnormal events and also DMN	Image size taken accordingly to fill the video and frames
13	Liu, S., Chen, Z., Pan, M., Zhang, Q., Liu, Z.,	2019	Magnetic anomaly detection based on full connected neural network.	FCN model performed well in detecting the anomaly in noise under various orientations.	Simple configuration, excellent performance, remaining unrecognized, and excellent antijamming potential surveying, traffic monitoring, and detection of hidden metal objects.	It is indicated that the proposed method has an incremental detection probability between 5% and 20% in different SNRs.	Orthonormal Basis Function Detector doesn't work effectively under the coloured noise and low Signal to Noise Ratio(SNR)

14	Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K.	2018	Enhanced Network Anomaly Detection Based on Deep Neural Networks	An intrusion detection system is forced to respond to a constantly varying threat environment as a main strength of network infrastructure.	Deep Intrusion Detection System models yielded promising results in real-world anomaly detection systems compared to other models.	Both DCNN and LSTM models showed exceptional performance with 85% and 89% Accuracy on test dataset	Sparse Autoencoder had the shortest training time among DNN models, but it didn't generate comparable results.
15	Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R.	2019	A hybrid deep learning-based model for anomaly detection in cloud data-centre networks.	Existing approaches cannot be implemented to network systems, are difficult to solve, and have a false - positive rate highly.	very useful particularly for feature extraction and anomaly detection on real-time network traffic streams.	The proposed model exhibits an overall improvement of 8.25%, 4.08% and 3.62% in terms of DR, FPR, and accuracy, respectively	SVM, MCA, FCM-ANN etc. techniques are inefficient because of their reduced accuracy and high false positive alarms.

Table 2.1 Comparison Table

3. METHODOLOGY

3.1 Dataset :

Avenue Dataset contains 16 training and 21 testing video clips. The videos are captured in CUHK campus Avenue with 1511 training frames in total with FPS of 5 value. The training videos capture normal situations. Testing videos include both normal and abnormal events. Our dataset contains the some challenges such as Slight camera shake, A few outliers are included in training data and Some normal patterns seldom appear in training data.

Fig3.1 Training Dataset

Fig3.2 Testing Dataset

3.2 Proposed Method :

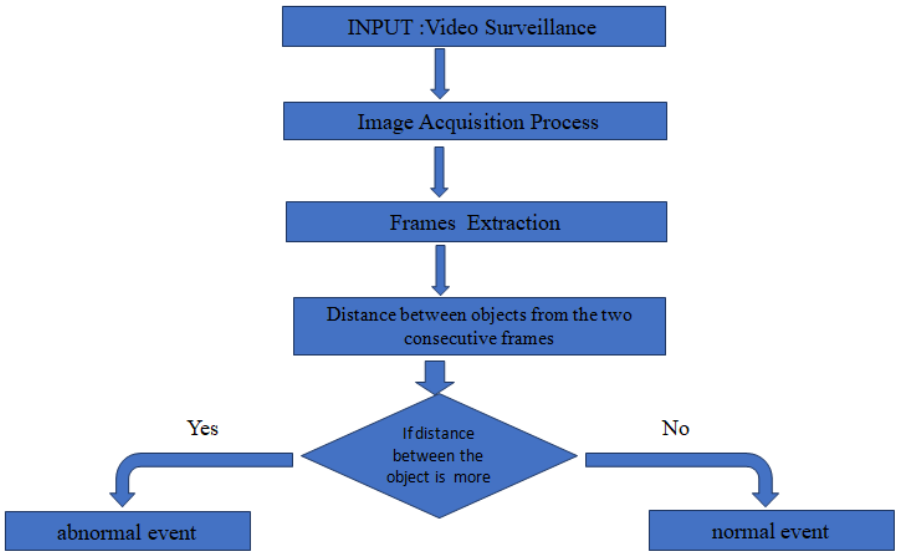

Fig 3.3 Flowchart of proposed work

3.3 Deep Learning :

Deep learning is a machine learning technique that teaches computers to do what comes naturally to humans. In deep learning the model learns how to classify the images,text,audio and video. It is a subpart of machine learning which on the other hand is a subset of Artificial Intelligence which the algorithms inspired by human brain which contain nodes and connection between the nodes. It can transfer the information between all the nodes. The architectures like deep neural networks, deep belief network, deep reinforcement learning, recurrent neural network and convolution neural network are applied to speech recognition, natural language processing, biometric authentication etc...,

The design of the neural network is based on the structure of the human brain. Just as we use our brains to identify patterns and classify different types of information, neural networks can be taught to perform the same tasks on data.

Neural networks enable us to perform many tasks, such as clustering, classification or regression. With neural networks, we can group or sort unlabeled data according to similarities

among the samples in this data. Or in the case of classification, we can train the network on a labeled dataset in order to classify the samples in this dataset into different categories.

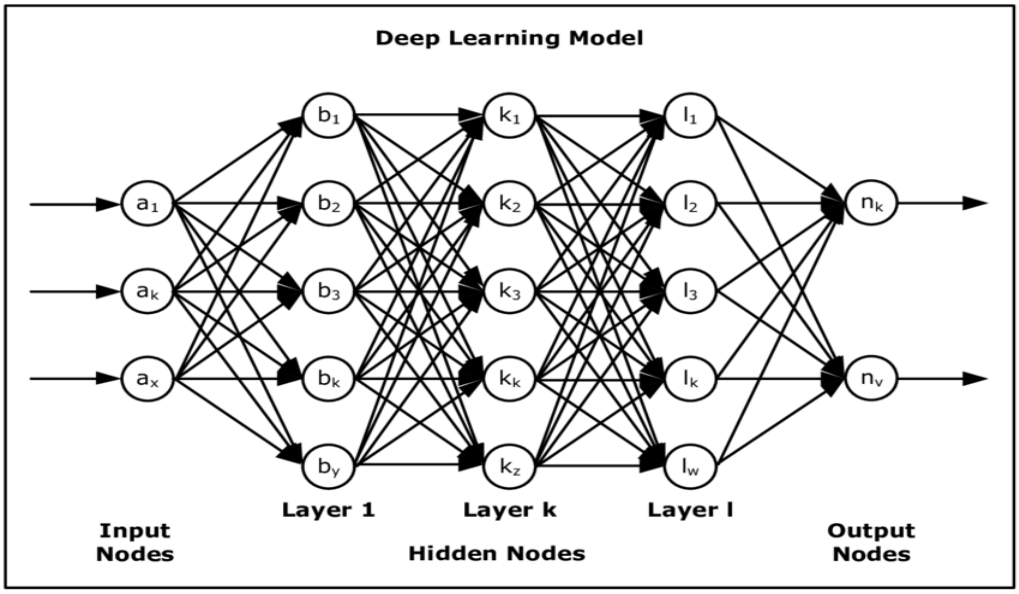

Fig3.4 Deep Learning Model

3.4 Convolutional Neural Network :

In deep learning, Convolution Neural network(CNN) is a class of artificial neural networks(ANN) is commonly used for analyze visual imagery purpose.it is particularly used for finding patterns in images to recognize objects, faces and scenes. CNN inspired by the human brain which contains nodes and each node is connected to all other nodes.it takes the input from the convolution layer and pass the information to all the layers and with the help of bias and weights the image is detected.by using the sigmoid the image is detected A convolution neural network has tens or hundreds of layers to detect the different features of an image.

A simple CNN consists of an input layer, followed by a stack of a convolutional layer with a certain activation function (CL) and a pooling layer (PL), the fully connected layer, and a final classification activation layer. The convolution layer and pooling layer are used for feature extraction and the layers fully connected layer and output layer is used for classification purpose. The convolution layer takes the input as input and produce feature maps. And the pooling layer is reduced the size of feature maps .so the usage of memory is reduced by reducing the size of images and it is also avoid the over fitting. And the regularization techniques are used to reduce

over fitting and also improves the accuracy. fully connected layer is used for classification purpose by using the activation function like sigmoid, SoftMax are used for binary and multiclass classification.

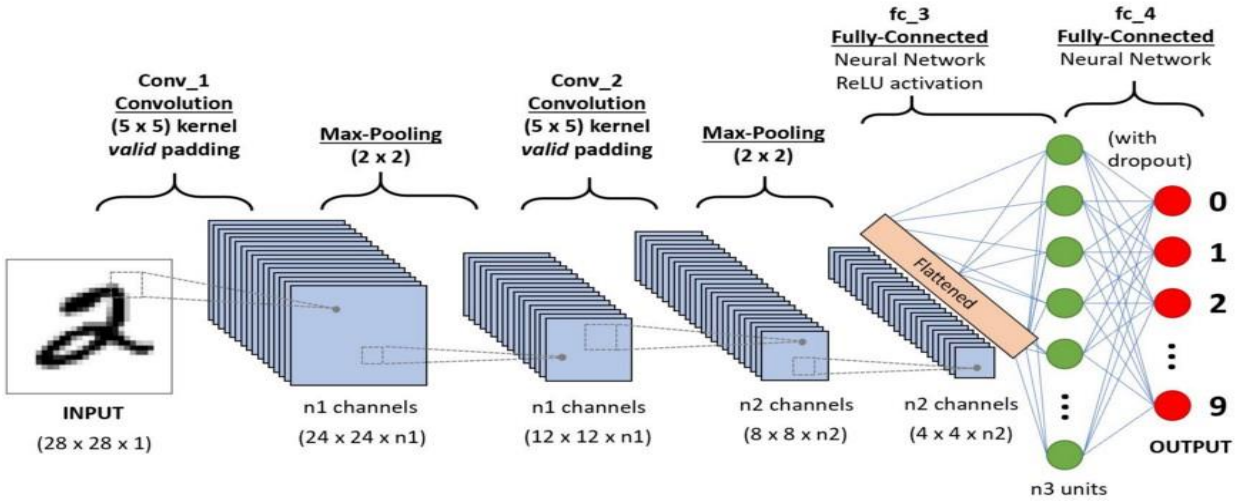

Fig3.5 Convolutional Neural Network Model

3.5 Autoencoder :

Autoencoder is an unsupervised artificial neural network that tells how to compress and encode data efficiently before learning how to rebuild the data from the reduced encoded representation to a representation that is as close to the original input as possible. Autoencoder reduces the dimensions of data by learning how to ignore the noise in the data.

3.6 Spatio -Temporal Autoencoder (ST Autoencoder or STAE) :

Spatio-Temporal Autoencoder (ST Autoencoder or STAE) understands video representation automatically using deep neural networks and extracts features from both spatial and temporal dimensions using 3-dimensional convolutions. Space is referred to as spatial. The term temporal refers to time. When data is collected in both space and time, the term spatiotemporal, or spatial

temporal, is often used in data analysis. It describes a situation in a specific place and time, such as movements across a geographic area over time.

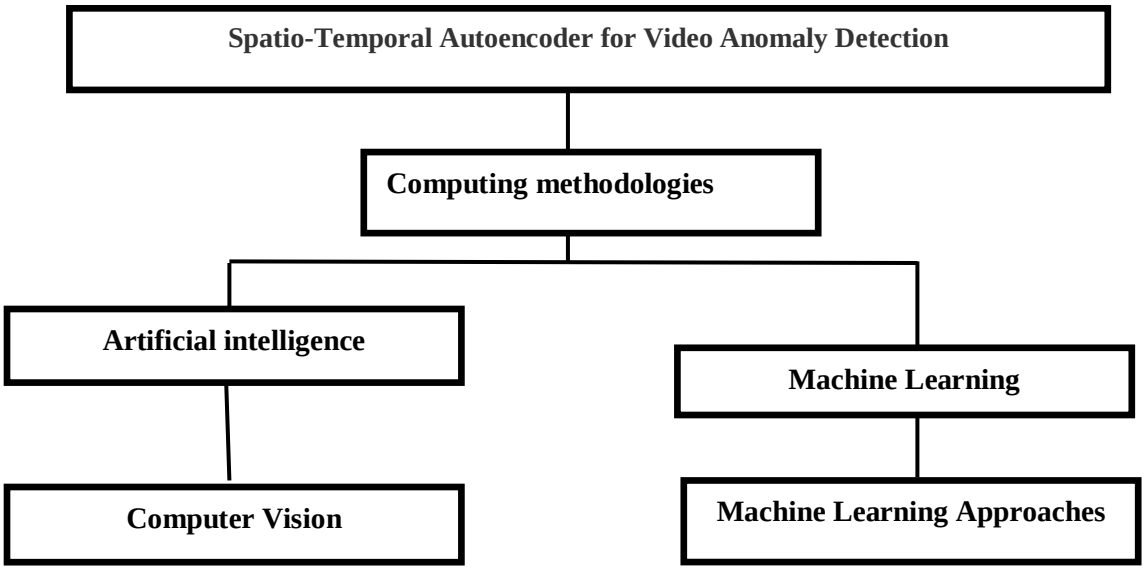

Fig3.6 Flowchart of Video Anomaly Detection

3.7 3D Convolutional Network :

A 3D Convolution can be used to find patterns across 3 spatial dimensions i.e. depth, height and width. One effective use of 3D Convolutions is object segmentation in 3D medical imaging. Since a 3D model is constructed from the medical image slices, this is a natural fit. And action detection in video is another popular research area, where multiple image frames are concatenated across a temporal dimension to give a 3D spatial input, and patterns are found across frames too.3D convolutions apply a 3-dimensional filter to the dataset and the filter moves 3-direction (x, y, z) to calculate the low-level feature representations. Their output shape is a 3-dimensional volume space such as cube or cuboid. They are helpful in event detection in videos, 3D medical images etc. They are not limited to 3d space but can also be applied to 2d space inputs such as images.

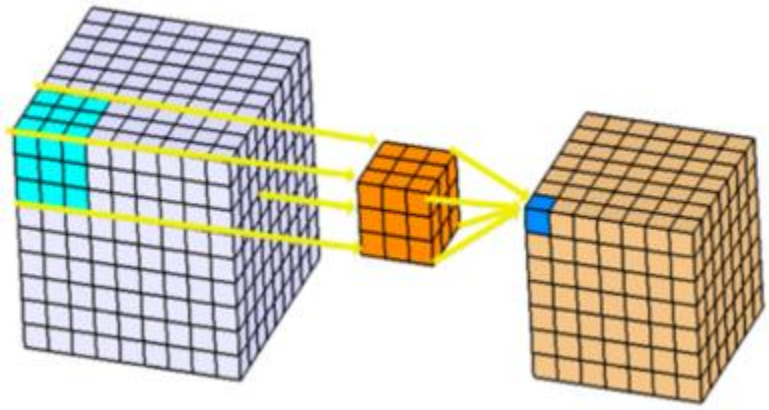

Fig 3.7 Architecture 3D Convolutional Network

3.8 Architecture :

The network architecture for autoencoders can vary between a simple FeedForward network, LSTM network or Convolutional Neural Network depending on the use case.This uses Deep Neural Networks to 3-dimensional for learning spatio-temporal features of the video feed.

For video surveillance, a spatio temporal autoencoder, which is based on a 3D convolution network is used. The encoder part extracts the spatial and temporal information, and then the decoder reconstructs the frames. The abnormal events are identified by computing the reconstruction loss using Euclidean distance between original and reconstructed batch. It uses spatial temporal encoders to identify abnormal activities.Then, it trains an autoencoder for abnormal event detection. The abnormal events are detected based on the euclidean distance of the custom video feed and the frames predicted by the autoencoder.

Here, threshold value for abnormal events is set as 0.0068.

3.9 Steps in Anomaly Detection :

There are totally 5 steps :-

1. Data Pre-Processing
2. Loading the Keras Models
3. Training the Model

4. Export the Trained Model

5. Testing the Detector

Step 1: Data Pre-Processing

Download the videos i.e. 16 training videos and 12 testing videos and divide it by frames.There may be images with random objects in the background.Various background conditions such as dark, light, indoor, outdoor, etc.Save all the images in a folder called images and all images should be in .jpg format.Divide each and every video into frames and save the frames in a directory separated by the type of anomaly or situation as well as resize the images to scale.Reshape and normalize the images.

Step 2: Loading the Keras Models

Import the three models Convolutional 3D, Convolutional LSTM 2Dand Convolutional 3D Transpose.Using Sequential define filters, padding and activation of these models. HereRelu is used.The optimizer are Adam and metric loss be Categorical Cross entropy.

Step 3: Training the Model

The Numpy file is to be saved in runs the training process.Array of all images from frames in video will kept in training.npy file.

Step 4: Export the Trained Model

The model will save a checkpoint every 600 seconds while training up to 5 checkpoints. Then, as new files are created, older files are deleted.A file called model.h5 is created which will be used while testing later.Epochs were used as arg.epoch and batch size for training was 1.Another file called training.npy would be created it contains the array form of all the coordinates required while testing. So here no frozen inference graph or pdtxt file is created.

Step 5: Testing the Detector

Load the model.h5 file and training.npy file.Test the Videos as Normal or Abnormal Event.

3.10 Code Implementation :

Imports:

```
from keras.preprocessing.image import img_to_array,load_img
import numpy as np
import glob
import os
import cv2


from keras.layers import Conv3D,ConvLSTM2D,Conv3DTranspose
from keras.models import Sequential
from keras.callbacks import ModelCheckpoint, EarlyStopping
import imutils
```

Initialize directory path variable and describe a function to process and store video frames:

```
store_image=[]
train_path='/content/drive/My Drive/project/'
fps=5
train_videos=os.listdir(train_path+'train_path')
train_images_path='/content/drive/My Drive/project/train/frames/'
os.makedirs(train_images_path)
def store_inarray(image_path):
    image=load_img(image_path)
    image=img_to_array(image)
    image=cv2.resize(image, (227,227), interpolation = cv2.INTER_AREA)
    gray=0.2989*image[:,:,0]+0.5870*image[:,:,1]+0.1140*image[:,:,2]
    store_image.append(gray)
```

Extract frames from video and call store function:

```
for video in train_videos:
    os.system( 'ffmpeg -i {}/{} -
r 1/{}  {}/frames/%03d.jpg'.format(train_path,video,fps,train_path))
    #print(video)
    vidcap = cv2.VideoCapture("/content/drive/My Drive/project/train_path/"+video)
    success,image = vidcap.read()
    count = 1
while success:
        cv2.imwrite("/content/drive/My Drive/project/train/frames/%d.jpg" % count, image)     # sa
ve frame as JPEG file
        success,image = vidcap.read()
        count += 1
    images=os.listdir(train_images_path)
    for image in images:
        image_path=train_images_path + '/' + image
        #image_path=train_image_path+'/'+image
        print("ok")
        store_inarray(image_path)
```

Store the store_image list in a numpy file “training.npy”:

```
images=os.listdir(train_images_path)
for image in images:
      image_path=train_images_path + '/' + image
```

```
    store_inarray(image_path)
store_image=np.array(store_image)
a,b,c=store_image.shape
store_image.resize(b,c,a)
store_image=(store_image-store_image.mean())/(store_image.std())
store_image=np.clip(store_image,0,1)
np.save('/content/drive/My Drive/project/training.npy',store_image)
```

Create spatial autoencoder architecture:

```
stae_model=Sequential()

stae_model.add(Conv3D(filters=128,kernel_size=(11,11,1),strides=(4,4,1),padding='valid',input_shape=(227,227,10,1),activation='tanh'))
stae_model.add(Conv3D(filters=64,kernel_size=(5,5,1),strides=(2,2,1),padding='valid',activation='tanh'))
stae_model.add(ConvLSTM2D(filters=64,kernel_size=(3,3),strides=1,padding='same',dropout=0.4,recurrent_dropout=0.3,return_sequences=True))
stae_model.add(ConvLSTM2D(filters=32,kernel_size=(3,3),strides=1,padding='same',dropout=0.3,return_sequences=True))
stae_model.add(ConvLSTM2D(filters=64,kernel_size=(3,3),strides=1,return_sequences=True, padding='same',dropout=0.5))
stae_model.add(Conv3DTranspose(filters=128,kernel_size=(5,5,1),strides=(2,2,1),padding='valid',activation='tanh'))
stae_model.add(Conv3DTranspose(filters=1,kernel_size=(11,11,1),strides=(4,4,1),padding='valid',activation='tanh'))
```

```
stae_model.compile(optimizer='adam',loss='mean_squared_error',metrics=['accuracy'])
```

```
stae_model.summary()
```

S.No	Layer (type)	Output Shape	Parameters
1	conv3d (Conv3D)	(None, 55, 55, 10, 128)	15616
2	conv3d_1 (Conv3D)	(None, 26, 26, 10, 64)	204864
3	conv_lstm2d (ConvLSTM2D)	(None, 26, 26, 10, 64)	295168
4	conv_lstm2d_1 (ConvLSTM2D)	(None, 26, 26, 10, 32)	110720
5	conv_lstm2d_2 (ConvLSTM2D)	(None, 26, 26, 10, 64)	221440
6	conv3d_transpose (Conv3DTranspose)	(None, 55, 55, 10, 128)	204928
7	conv3d_transpose_1 (Conv3DTranspose)	(None, 227, 227, 10, 1)	15489

Table 3.1 Sequential Model Table

Total parameters	Trainable parameters	Non-trainable parameters
1,068,225	1,068,225	0

Table 3.2 Parameters Table

Train the autoencoder on the "training.npy" file and save the model with name "saved_model.h5":

```
training_data=np.load('/content/drive/My Drive/project/training.npy')

frames=training_data.shape[2]

frames=frames-frames%10

training_data=training_data[:,:,:frames]

training_data=training_data.reshape(-1,227,227,10)

training_data=np.expand_dims(training_data,axis=4)

target_data=training_data.copy()


epochs=60

batch_size=1


callback_save = ModelCheckpoint("/content/drive/My Drive/project/saved_model.h5", monitor=
"mean_squared_error", save_best_only=True)

callback_early_stopping = EarlyStopping(monitor='val_loss', patience=3)


stae_model.fit(training_data,target_data, batch_size=batch_size, epochs=epochs, callbacks = [cal
lback_save,callback_early_stopping])
```

```
stae_model.save("/content/drive/My Drive/project/saved_model.h5
```

“test.py”:

```
import cv2
import numpy as np
from keras.models import load_model
import argparse
from PIL import Image
import imutils
from google.colab.patches import cv2_imshow

def mean_squared_loss(x1,x2):
    difference=x1-x2
    a,b,c,d,e=difference.shape
    n_samples=a*b*c*d*e
    sq_difference=difference**2
    Sum=sq_difference.sum()
    distance=np.sqrt(Sum)
    mean_distance=distance/n_samples

    return mean_distance
model=load_model("/content/drive/My Drive/project/saved_model.h5")
```

```
cap = cv2.VideoCapture("/content/drive/My Drive/project/testing_videos/01.avi")
print(cap.isOpened())

while cap.isOpened():
    imagedump=[]
    ret,frame=cap.read()

    for i in range(10):
        ret,frame=cap.read()
        image = imutils.resize(frame,width=700,height=600)

        frame=cv2.resize(frame, (227,227), interpolation = cv2.INTER_AREA)
        gray=0.2989*frame[:,:,0]+0.5870*frame[:,:,1]+0.1140*frame[:,:,2]
        gray=(gray-gray.mean())/gray.std()
        gray=np.clip(gray,0,1)
        imagedump.append(gray)

    imagedump=np.array(imagedump)
    imagedump.resize(227,227,10)
    imagedump=np.expand_dims(imagedump,axis=0)
    imagedump=np.expand_dims(imagedump,axis=4)

    output=model.predict(imagedump)
```

```
    loss=mean_squared_loss(imagedump,output)

    if frame.any()==None:
        print("none")

    if cv2.waitKey(10) & 0xFF==ord('q'):
        break
    if loss>0.00068:
        print('Abnormal Event Detected')
        cv2.putText(image,"Abnormal Event",(100,80),cv2.FONT_HERSHEY_SIMPLEX,2,(0,0,2
55),4)
    cv2_imshow(image)

cap.release()
cv2.destroyAllWindows()
```

4. RESULTS & DISCUSSION

The result should be detection of Abnormal Event in the given video input. Whenever a abnormal event detected in the video, the "Abnormal Event" Appears on the screen. By computing, the reconstruction loss using Euclidean distance between original image and reconstructed image the output is displayed as normal or abnormal event. If the loss is greater than the threshold value then the output is detected as abnormal events otherwise it is detected as normal video.

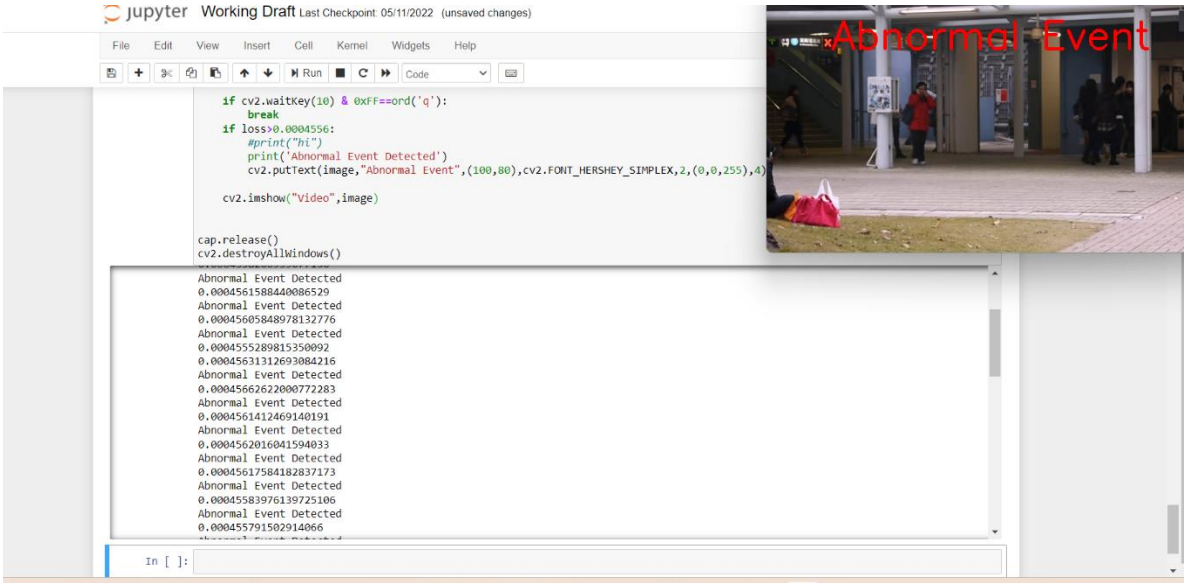

Fig 4.1 Loss Values Result

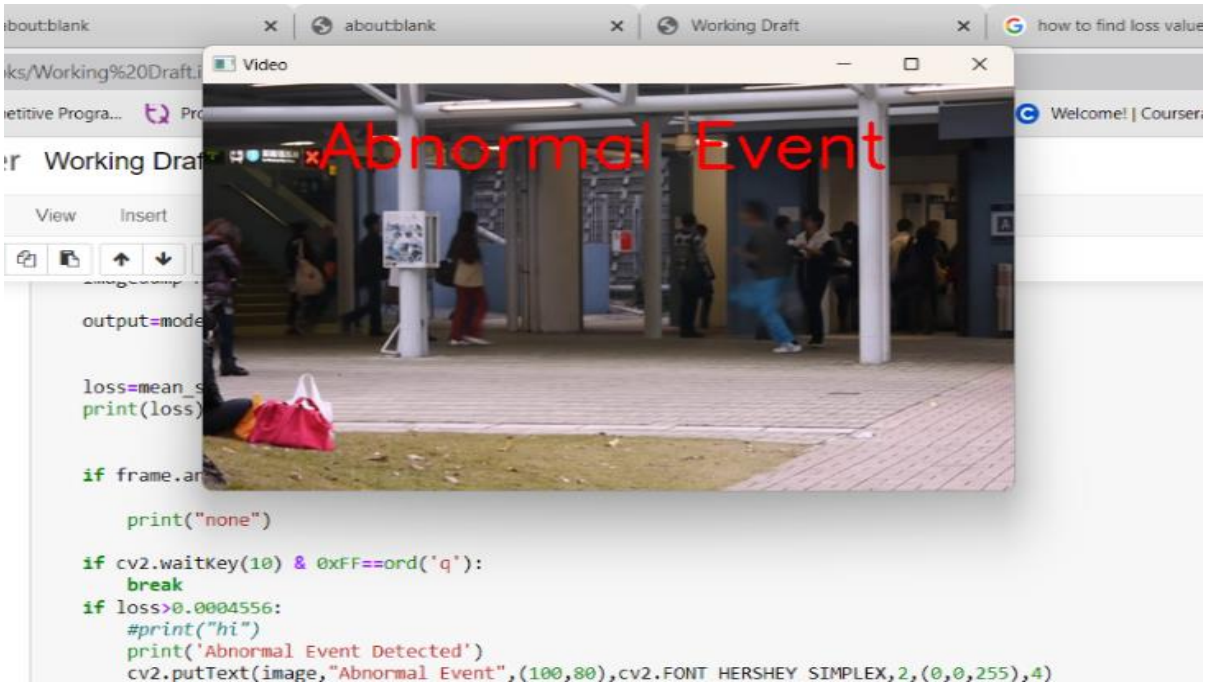

Fig 4.2 Detected Abnormal

In the above output diagram, the person is running, so the Euclidean distanace between is very high and the loss is greater than threshold value.so it is detected as abnormal event.the output blinks as abnormal event in the top of the video.

Fig 4.3 Normal Event

In the above output diagram, there is no difference between two frames then it is detected as normal and then it is detected as normal and the output shows as normal event.
Whenever an action which is anomaly is detected, the required measures should be taken to control it and reduce it. This safeguards the public and property too.

5. CONCLUSION & FUTURE SCOPE

This project presents an approach for anomalous detection techniques in the crowded areas. The proposed approach is Spatio-Temporal Auto Encoder, which is based on 3-Dimensional Convolution Neural Network which are convolution 3D, convolution LSTM2D, convolution 3D Transpose. The spatial and temporal information is extracted by the encoded part and the frames are reconstructed by the decoder part. A CNN is used to learn about the normal and abnormal events. The abnormal events are detected by computing the reconstruction loss using Euclidean distance between original image and reconstructed image. Evaluations are conducted on publicly available datasets like Avenue dataset. This application is very help in present public scenario as everyone wants safety atmost. Most of the incidents is happening due to the information gap. Whenever there is property information, immediately actions can be reduced and controlled in short gap of time period. This also even gives the confidence to the public about their safety. The results indicate the proposed work is more effective.

REFERENCES

1. Direkoglu, C. (2020). Abnormal crowd behavior detection using motion information images and convolutional neural networks. *IEEE Access*, *8*, 80408-80416.

2. Nawaratne, R., Alahakoon, D., De Silva, D., & Yu, X. (2019). Spatiotemporal anomaly detection using deep learning for real-time video surveillance. *IEEE Transactions on Industrial Informatics*, *16*(1), 393-402.

3. Mehmood, A. (2021). Efficient Anomaly Detection in Crowd Videos Using Pre-Trained 2D Convolutional Neural Networks. *IEEE Access*, *9*, 138283-138295.

4. Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A spectrogram image-based network anomaly detection system using deep convolutional neural network. *IEEE Access*, *9*, 87079-87093.

5. Almazroey, A. A., &Jarraya, S. K. (2020, April). Abnormal Events and Behavior Detection in Crowd Scenes Based on Deep Learning and Neighborhood Component Analysis Feature Selection. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 258-267). Springer, Cham.

6. 2.Tariq, S., Farooq, H., Jaleel, A., & Wasif, S. M. (2021). Anomaly detection with particle filtering for online video surveillance. *IEEE Access*, *9*, 19457-19468.

7. Duman, E., &Erdem, O. A. (2019). Anomaly detection in videos using optical flow and convolutional autoencoder. *IEEE Access*, *7*, 183914-183923.

8. Cruz-Esquivel, E., & Guzman-Zavaleta, Z. J. (2022). An examination on autoencoder designs for anomaly detection in video surveillance. *IEEE Access*.

9.Javed, A. R., Usman, M., Rehman, S. U., Khan, M. U., &Haghighi, M. S. (2020). Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4291-4300.

10.Ullah, W., Ullah, A., Haq, I. U., Muhammad, K., Sajjad, M., &Baik, S. W. (2021). CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks. *Multimedia Tools and Applications*, *80*(11), 16979-16995.

11.Ye, O., Deng, J., Yu, Z., Liu, T., & Dong, L. (2020). Abnormal event detection via feature expectation subgraph calibrating classification in video surveillance scenes. *IEEE Access*, *8*, 97564-97575.

12.Franklin, R. J., &Dabbagol, V. (2020, January). Anomaly detection in videos for video surveillance applications using neural networks. In *2020 Fourth International Conference on Inventive Systems and Control (ICISC)* (pp. 632-637). IEEE.

13. Liu, S., Chen, Z., Pan, M., Zhang, Q., Liu, Z., Wang, S., ... & Wan, C. (2019). Magnetic anomaly detection based on full connected neural network. IEEE Access, 7, 182198-182206.

14. Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3), 924-935.

15 Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE access, 6, 48231-48246.