WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Abnormal Activity Detection for College using CNN Algorithm

Prof. Deepali Dhadwad, Khushi Yadav*[1],Neha Wavhal*[2],Divya Dumbre*[3],Sandesh Datir*[4]

[*1, 2, 3,4] Student Department of Computer Engineering, Indira college of Engineering and management, Pune
Savitribai Phule Pune University, Pune, Maharashtra, India
Deepali.dagale@indiraicem.ac.in kyadav3503@gmail.com[1],
nehawavhal1803@gmail.com[2],
divyadumbre36@gmail.com[3],
sandeshdatir4112@dypic.in[4]

ABSTRACT :

In today's insecure world the video surveillance plays an important role for the security of the indoor as well as outdoor places. With the increasing in the number of anti-social activates that have been taking place, security has been given utmost importance lately. Many Organizations have installed CCTVs for constant Monitoring of people and their interactions. For a developed Country with a population of 64 million, every person is captured by a camera 30 times a day. A lot of video data generated and stored for a certain time duration. A 704x576 resolution image recorded at 25fps will generate roughly 20GB per day. Constant Monitoring of data by humans to judge if the events are abnormal is near impossible task as requires a workforce and their constant attention. This creates a need to automate the same. Also , there is need to show in which frame and which part of it contain the unusual activity which aid the faster judgment of the unusual activity being abnormal. This is done by converting video into frames and analyzing the persons and their activates from the processed frame .Machine learning and Deep Learning Algorithms and techniques support us in a wide accept to make possible.

Keywords: videosurveillance , anti-social activities, Constant Monitoring

I. INTRODUCTION :

In Human face and human behavioural pattern play an important role in person identification. Visual information is a key source for such identifications. Surveillance videos provide such visual information which can be viewed as live videos, or it can be played back for future references. The recent trend of 'automation' has its impact even in the field of video analytics. Video analytics can be used for a wide variety of applications like motion detection, human activity prediction, person identification, abnormal activity recognition, vehicle counting, people counting at crowded places, etc. In this domain, the two factors which are used for person identification are technically termed as face recognition and gait recognition respectively. Among these two techniques, face recognition is more versatile for automated person identification through surveillance videos. Face recognition can be used to predict the orientation of a person's head, which in turn will help to predict a person's behaviour. Motion recognition with face recognition is very useful in many applications such as verification of a person, identification of a person and detecting presence or absence of a person at a specific place and time. In addition, human interactions such as subtle contact among two individuals, head motion detection, hand gesture recognition and estimation are used to devise a system that can identify and recognize suspicious behaviour among pupil in an examination hall successfully. This paper provides a methodology for suspicious human activity detection through face recognition.

Machine Learning :

Machine learning (ML) plays a significant role in abnormal event detection in video surveillance by automatically identifying unusual or suspicious behavior in real-time, reducing the need for constant human monitoring. Here's how ML is applied to this field:

1. Feature Extraction

- ML models first extract relevant features from video frames, such as object movements, size, shape, or trajectory.
- These features are used to represent the visual scene in a more abstract, computable form for further analysis.

2. Object Detection and Tracking

- Algorithms like **YOLO (You Only Look Once)** or **SSD (Single Shot Detector)** can detect and classify objects (e.g., cars, people) in video frames.
- **Tracking algorithms** like **SORT (Simple Online and Realtime Tracking)** or **DeepSORT** track object movement over time, providing the context for determining if an event is abnormal.

3. Supervised Learning

- **Pre-labeled datasets** are used to train models to recognize specific types of abnormal events (e.g., violence, break-ins).

- **Neural networks** such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) are often used to learn patterns of normal and abnormal behaviors.

4. Unsupervised Learning

- In scenarios where labeled data is not available, **unsupervised learning** models like autoencoders, clustering algorithms, and Gaussian Mixture Models (GMMs) can detect anomalies by learning the normal patterns in video data and flagging deviations from these patterns.
- **Principal Component Analysis (PCA)** or **k-means clustering** can be applied to detect outliers without prior knowledge of what constitutes an abnormal event.

5. Deep Learning for Spatio-Temporal Analysis

- **Long Short-Term Memory (LSTM)** networks or **3D CNNs** are used to model spatio-temporal data, which helps in detecting complex events that evolve over time, such as a sudden fall or a fight.
- **Recurrent Neural Networks (RNNs)** can capture the temporal dependencies in sequences of video frames, crucial for detecting abnormalities that occur over time.

6. Abnormal Behavior Detection

- Algorithms can learn normal behavior patterns from data, and any deviation is flagged as abnormal. For example, an ML model can learn the usual walking patterns in an area, and any sudden or erratic behavior, like running or loitering, can be marked as suspicious.
- **Behavioral analysis models** may be trained to detect unusual object trajectories (e.g., a person running in a restricted area).

7. Action Recognition

- ML models are used to recognize specific actions or events. Techniques like **pose estimation** and **optical flow** are used to recognize human activities, and deviations from expected actions can be flagged.
- Example: If a person is loitering or moving in a manner inconsistent with normal behavior, the system will trigger an alert.

8. Real-Time Detection

- Real-time event detection can be achieved using lightweight models that can process video streams at a high frame rate.
- **Edge computing** can be employed to perform on-device analysis, reducing latency and enabling real-time response to abnormal events.

9. Alert Systems

- The output of abnormal event detection is often used to trigger real-time alerts (e.g., sending a notification to security personnel).
- In more advanced systems, automatic responses like locking doors or focusing the camera on suspicious objects may be triggered.

II. LITERATURE SURVEY :

The table below shows various existing system for abnormal event detection.

Table-1: Literature Survey Table

Sr. No.	Paper name	Author Name	Description
1.	Suspicious Activity Recognition in Video Surveillance System	Ms.U.M.Kamthe, Dr. C.G.Patil	In today's insecure world the video surveillance plays an important role for the security of the indoor as well as outdoor places. The components of video surveillance system such as behavior recognition, understanding and classifying the activity as normal or suspicious can be used for real time applications. In this paper the hierarchical approach is used to detect the different suspicious activities such as loitering, fainting, unauthorized entry etc. This approach is based on the motion features between the different objects. First of all the different suspicious activities are defined using semantic approach.
2.	Suspicious Activity Detection from Videos using YOLOv3	Nipunjita Bordoloi1 , Anjan Kumar Talukdar2 , Kandarpa Kumar Sarma	Human activity detection for video system is an automated way of processing video sequences and making an intelligent decision about the actions in the video. It is one of the growing areas in Computer Vision and Artificial Intelligence. Suspicious activity detection is the process of detecting unwanted human activities in places and situations. This is done by converting video into frames and analyzing the activities of persons from the processed frames. Human detection has always been a challenging problem as human bodies are non-rigid and changes shape arbitrarily.

3.	Suspicious Activity Detection in Surveillance Footage	Sathyajit Loganathan, Gayashan Kariyawasam	Suspicious activities are of a problem when it comes to the potential risk it brings to humans. With the increase in criminal activities in urban and suburban areas, it is necessary to detect them to be able to minimize such events. Early days surveillance was done manually by humans and were a tiring task as suspicious activities were
			uncommon compared to the usual activities. With the arrival of intelligent surveillance systems, various approaches were introduced in surveillance. We focus on analyzing two cases, those if ignored could lead to high risk of human lives, which are detecting potential gun-based crimes and detecting abandoned luggage on frames of surveillance footage. We present a deep neural network model that can detect handguns in images and a machine learning and computer vision pipeline that detects abandoned luggage so that we could identify potential gun-based crime and abandoned luggage situations in surveillance footage. Keywords—Gun detection, Abandoned luggage detection, Computer Vision, Surveillance.

IV.SYSTEM ARCHITECTURE :

- In this system we have used CNN algorithm.
- Technology used is machine learning.
- In this system we collect video dataset then convert video to frame Then train data after training detect the suspicious activity detected.

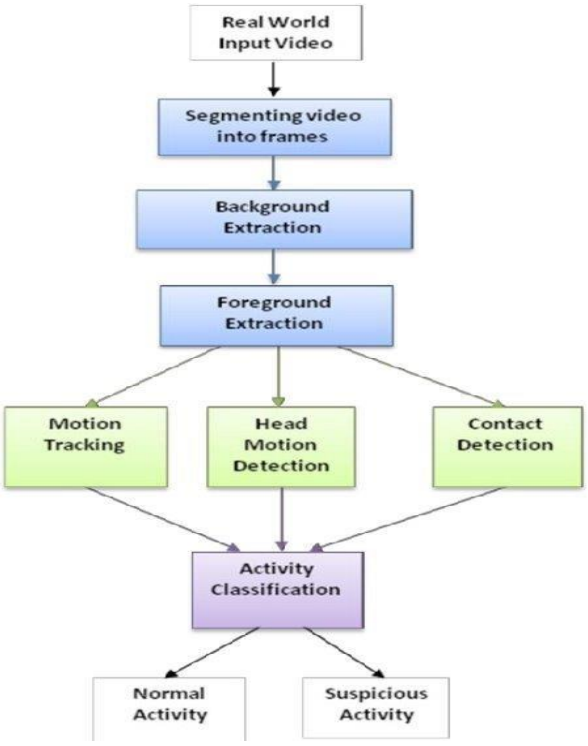


Fig.1: System Architecture

UML DIAGRAMS

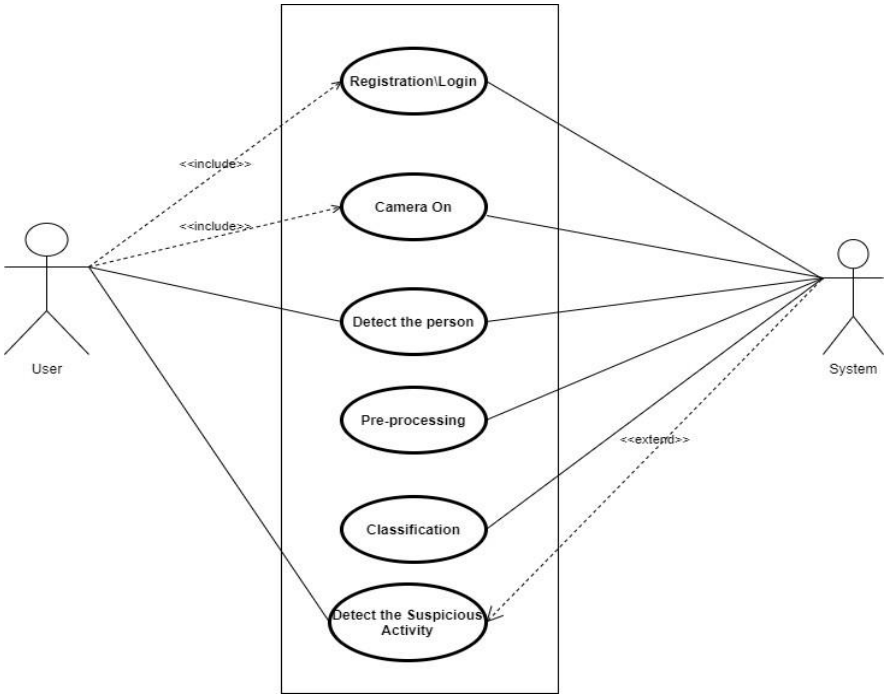


Fig. 3: Use case diagram

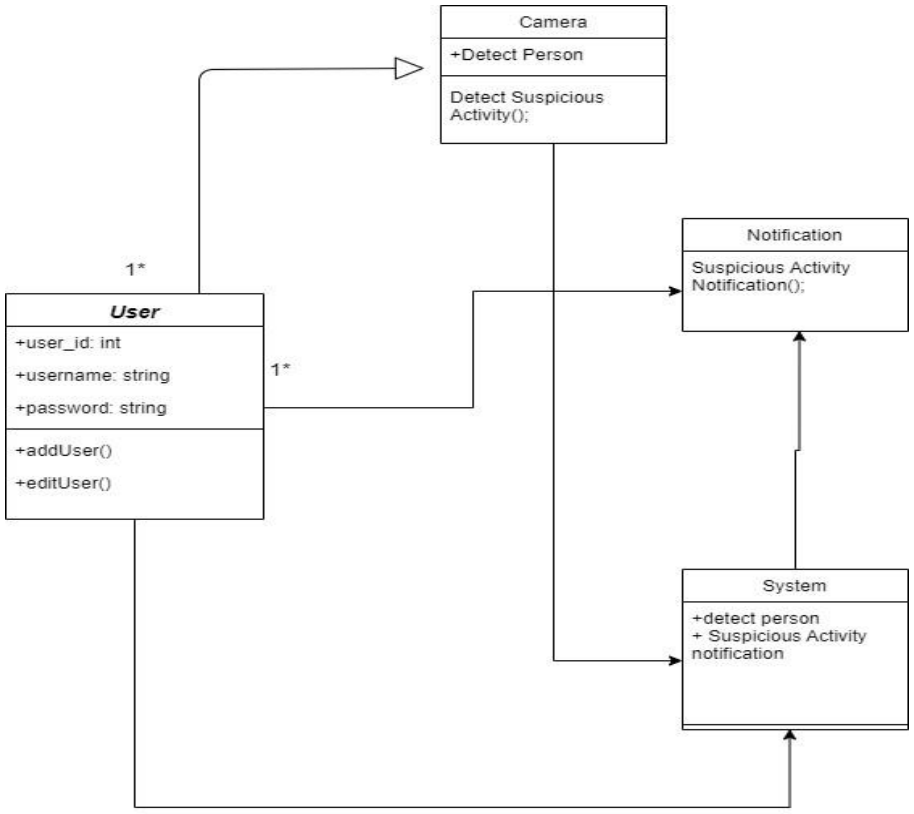


Fig. 4: Class diagram

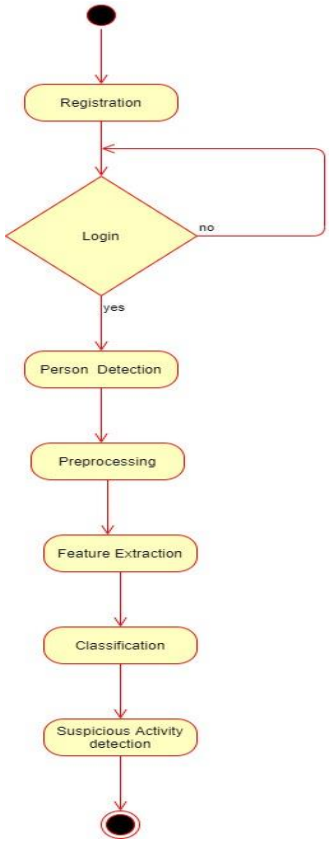


Fig. 5: Activity Diagram

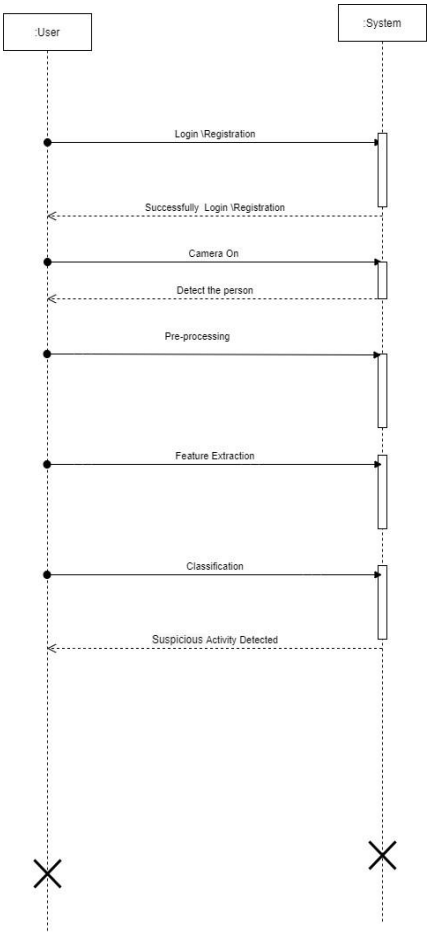


Fig.6: Sequence diagram

ALGORITHMS USED:

CNN Algorithm:

In video surveillance systems, Convolutional Neural Networks (CNNs) are widely used for tasks like object detection, recognition, tracking, and even anomaly detection. Here's how CNN algorithms are typically applied in video surveillance:

1. Object Detection

- Use Case: Detecting humans, vehicles, or other objects of interest in the surveillance footage.
- CNN Application: CNNs are trained on large datasets to identify objects in video frames. Popular architectures for object detection in surveillance include:
  - YOLO (You Only Look Once): Detects objects in real-time with high speed.
  - Faster R-CNN: A more accurate but slower method for detecting objects.
  - SSD (Single Shot Detector): A balance between speed and accuracy.

These models can localize and classify objects in each video frame, which is vital for monitoring areas, detecting intrusions, or identifying suspicious activities.

2. Face Recognition

- Use Case: Identifying individuals in a crowd or granting access to authorized personnel.
- CNN Application: CNNs like FaceNet, DeepFace, or VGG-Face extract facial features and compare them with a database of known faces. CNNs are extremely effective at learning the intricate patterns of human faces, which can be used for recognition or verification.

3. Human Activity Recognition

- Use Case: Detecting suspicious behaviors or specific actions (e.g., falling, loitering, or fighting).
- CNN Application: 3D CNNs (which take both spatial and temporal information into account) are often used for videobased human activity recognition. They analyze sequences of frames to recognize patterns of movement and actions.

4. Anomaly Detection

- Use Case: Identifying unusual events like break-ins, unattended baggage, or violent actions.
- CNN Application: CNN-based autoencoders or recurrent neural networks (RNNs) combined with CNNs can detect anomalies in video streams by learning "normal" patterns of behavior and flagging deviations from these patterns.

5. Multi-Object Tracking

- Use Case: Following the movement of multiple objects (people, vehicles) across different frames.
- CNN Application: Object detection CNNs like YOLO can be combined with tracking algorithms (e.g., Kalman Filters, SORT) to not only detect but also track objects across frames in real time.

Workflow in a Video Surveillance System

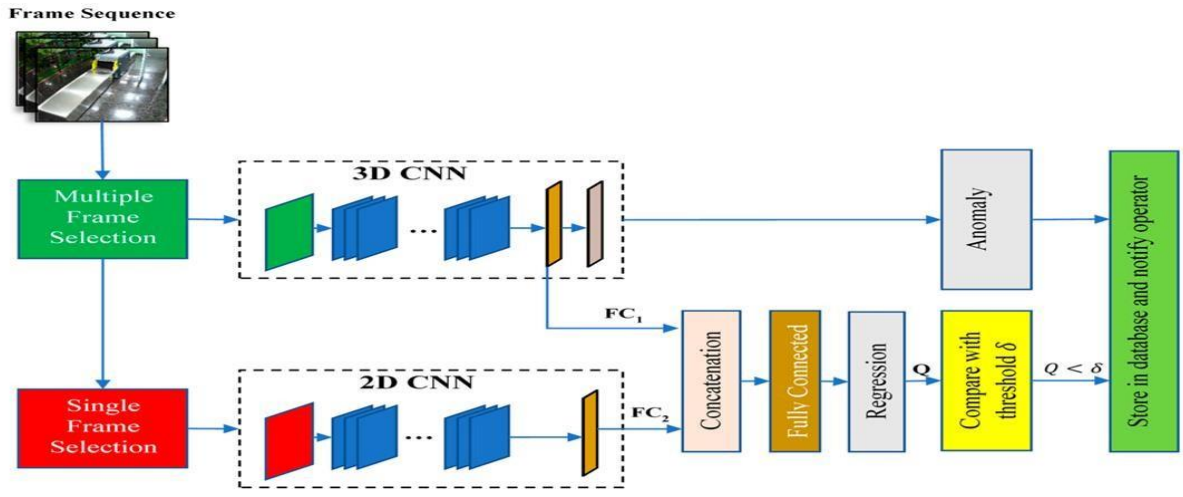
1. Frame Extraction: The video is split into individual frames.
2. Preprocessing: Frames are resized, normalized, and prepared for the CNN.
3. Feature Extraction: The CNN processes each frame and extracts features.
4. Object Detection/Recognition: Detected objects are classified, and their positions are determined.
5. Post-Processing: Identified objects or activities are logged, tracked, or further processed for alerting.

Popular CNN Architectures in Video Surveillance

- ResNet: Deep residual networks are effective for feature extraction.
- Inception: Known for its efficiency in learning multi-scale features.
- MobileNet: Often used in edge devices for real-time surveillance due to its lightweight nature.

By using CNN algorithms, video surveillance systems can automate the monitoring process, improving response times and reducing human error.

Fig . CNN Algorithm used in Video Surveillance



Advantages:

1. Early Threat Detection

- **Advantage**: AED systems can quickly identify potential threats or unusual behaviors in real-time.
- **Benefit**: This allows for early intervention, preventing incidents such as theft, violence, or accidents before they escalate, enhancing security and safety.

2. Automation and Reduced Human Monitoring

- **Advantage**: AED automates the process of identifying abnormal events, reducing the reliance on human operators to continuously monitor video feeds.
- **Benefit**: This minimizes human errors due to fatigue or inattention and improves efficiency, as security personnel can focus on responding to alerts rather than passively monitoring footage.

3. Real-time Alerts and Response

- **Advantage**: AED systems provide immediate alerts when an anomaly is detected, ensuring that security teams are notified instantly.
- **Benefit**: This enables faster response times to incidents such as intrusions, unauthorized access, or suspicious behavior, potentially averting dangerous situations.

4. Improved Surveillance in Complex Environments

- **Advantage**: AED systems can operate in dynamic or crowded environments, such as airports, shopping malls, or public events, where detecting abnormal behavior manually is difficult.
- **Benefit**: The system can effectively monitor large areas with high foot traffic and identify abnormal activities, such as loitering, unattended bags, or erratic movements, that may go unnoticed by human observers.

Limitations:

1.Difficulty in Defining "Abnormal" Events

- **Limitation**: It can be challenging to precisely define what constitutes an abnormal event, as behaviors considered abnormal in one context may be normal in another.
- **Impact**: This can lead to false positives (detecting normal behavior as abnormal) or false negatives (missing genuinely abnormal behavior), reducing the accuracy of the system.

2. High Dependency on Training Data

- **Limitation**: AED systems rely on extensive training data to learn what is "normal" and "abnormal." If the training data
- is insufficient or not representative of real-world scenarios, the system may perform poorly.
- **Impact**: Incomplete or biased datasets can lead to inaccurate detection, especially in diverse or changing environments.

3. False Positives and False Negatives

- **Limitation**: AED systems can generate false positives (incorrectly identifying normal events as abnormal) or false negatives (failing to detect actual abnormal events).
- **Impact**: High false positive rates can lead to unnecessary interventions and wasted resources, while false negatives can result in missed incidents, compromising security.

4. Sensitivity to Environmental Changes

- **Limitation**: AED systems can be sensitive to environmental factors like lighting conditions, weather changes, or camera angles. Changes in these factors can impact the system's ability to accurately detect anomalies.
- **Impact**: Poor performance in certain conditions (e.g., low light or cluttered scenes) can reduce the system's reliability.

Applications :

1. **Security and Surveillance:** CNNs help detect unusual activities in surveillance videos, like theft or violence in public spaces. They can also identify unauthorized access to restricted areas, such as airports or banks.
2. **Healthcare:** In hospitals, CNNs can spot sudden changes in patient health, like irregular heart rates or unusual movements in elderly patients. They assist doctors in finding anomalies in X-rays or MRIs, like tumors.
3. **Traffic Monitoring:** CNNs analyze traffic videos to spot accidents or unusual traffic patterns. They also assess driver behavior to identify reckless driving or violations.
4. **Finance:** CNNs monitor banking transactions to catch unusual activity that may indicate fraud. They help spot unusual trading patterns in the stock market that could signify market manipulation.
5. **Manufacturing:** CNNs can identify defects in products during production. They also monitor machinery to detect abnormal behavior and predict failures.
6. **Environmental Monitoring**: CNNs analyze satellite images to spot signs of wildfires, like unusual heat patterns. They help identify abnormal pollution levels in the air or water.
7. **Social Media and Content Analysis**: CNNs can detect inappropriate content in images and videos on social media. They also analyze user posts to catch sudden changes in public opinion.
8. **Robotics**: CNNs help robots detect obstacles in their path to navigate safely. They recognize unusual behavior in humans to ensure safe collaboration with robots.

9. **Sports Analytics:** CNNs track player movements to identify signs of fatigue or injury. They analyze game footage to spot unexpected tactics from opponents.
10. **Cybersecurity:** CNNs monitor network traffic to detect unusual patterns that might indicate cyber attacks. They identify abnormal software behavior that could suggest malicious activity.

VII. CONCLUSION :

In conclusion, A system that processes real-time CCTV footage to detect suspicious activity can significantly enhance security while reducing human involvement. Recent advancements in technology enable the detection of suspicious human behavior, offering a more proactive approach to security management. This opens the door to various applications, such as monitoring public spaces, workplaces, or restricted areas. Additionally, improvements in activity tracking provide even greater precision, allowing for more detailed insights into human behavior. These innovations can be integrated into surveillance systems for automated alerts, increasing response times and overall efficiency in security tasks. Ultimately, this technology has the potential to transform how security and monitoring are conducted, ensuring a safer environment with fewer resources.

VIII. ACKNOWLEDGEMENT :

We would like to express our sincere gratitude and thank **Prof.Deepali Dhadwad** his invaluable advice and guidance throughout the project and for giving us an opportunity to work under our department.Our special thanks to **Dr. Soumitra Das** , Head of Computer Engineering Department, ICEM and **Prof.Sunil Rathod** who motivated us to learn and enhance our knowledge. We would also like to thank staff members of our college for their support and guidance.

X. REFERENCES :

1. Eralda Nishani, Betim Cico : "Computer Vision Approaches based on Deep Learning and Neural Networks" *Deep Neural Networks for Video Analysis of Human Pose Estimation- 2017 6th mediterranean conference on embedded computing* (meco), 11-15 june 2017, bar, montenegro
2. Naimat Ullah Khan , Wanggen Wan : "A Review of Human Pose Estimation from Single Image"- *9781-5386-5195-7/18/ 2018 IEEE*
3. Qiuhui Chen, Chongyang Zhang, Weiwei Liu, and Dan Wang, "Surveillance Human Pose Dataset And Performance Evaluation For Coarse-Grained Pose Estimation*", Athens 2018*.
4. Hanguen Kim, Sangwon Lee, Dongsung Lee, Soonmin Choi, JinsunJu and Huyun Myung "Real-Time Human Pose Estimation and Gesture Recognition from depth Images Using Superpixels and SVM classifier."- *Sensors 2015, 15, 12410-12427; doi:10.3390/s150612410*
5. Tripathi, Rajesh and Jalal, Anand and Agarwal, Subhash(2017). "Suspicious Human Activity Recognition: a Review". *Artificial Intelligence Review. 50.10.1007/s10462-017-9545-7.*
6. E. Eksioglu. Decoupled algorithm for MRI reconstruction using nonlocal block matching model: BM3DMRI. Journal of *Mathematical Imaging and Vision, 56(3):430–440, 2016.*
7. S. Wang, Z. Su, L. Ying, X. Peng, S. Zhu, F. Liang, D. Feng, and D. Liang. Accelerating magnetic resonance imaging via deep learning. In *Proceedings of the IEEE International Symposium on Biomedical Imaging, pages 514–517, 2016.*
8. L. Xu, J. Ren, C. Liu, and J. Jia. Deep convolutional neural network for image deconvolution. In Advances in Neural Information Processing *Systems, pages 1790–1798, 2014.*
9. *Y. Yang, J. Sun, H. Li, and Z. Xu. Deep ADMM-Net for compressive sensing* MRI. In Advances in Neural Information Processing Systems, pages 10–18, 2016.
10. Z. Zhan, J.-F. Cai, D. Guo, Y. Liu, Z. Chen, and X. Qu. Fast multiclass dictionaries learning with geometrical directions in MRI reconstruction. *IEEE Transactions on Biomedical Engineering, 63(9):1850– 1861, 2016.*