A Survey on Deep Learning Approach For Suspicious Activity Detection from Surveillance Video in Examination Hall

Prof.Anoop Kushwaha[1], Shradha Auti[2], Priyanka Darade[3], Ankita Munje[4], Neha Patil[5]

[1] *Assistant Professor, Computer Department, ACEM Hinjawadi,Pune, Maharashtra ,India*
[2] *BE Student , Computer Department, ACEM Hinjawadi,Pune, Maharashtra ,India*
[3] *BE Student , Computer Department, ACEM Hinjawadi,Pune, Maharashtra ,India*
[4] *BE Student , Computer Department, ACEM Hinjawadi,Pune, Maharashtra ,India*
[5] *BE Student , Computer Department, ACEM Hinjawadi,Pune, Maharashtra ,India*

ABSTRACT

Surveillance-based monitoring of examination halls is crucial for maintaining academic integrity. Traditional invigilation methods face challenges in scalability, real-time detection, and automation. Recent advancements in deep learning and computer vision have led to the development of intelligent systems for detecting suspicious activities in examination environments. This survey paper provides a comprehensive review of existing research on automated examination monitoring systems, focusing on deep learning-based approaches. It explores various methodologies, datasets, architectures, and evaluation metrics used for suspicious activity detection. Additionally, the paper discusses the challenges, limitations, and future research directions in this domain. By analyzing state-of-the-art techniques, this survey aims to guide researchers in developing more efficient and accurate systems for ensuring fair examinations through automated surveillance.

Keyword - *Suspicious activity detection, Surveillance video, Deep learning, Examination hall, Real-time alert*

1. INTRODUCTION :

Ensuring security in examination halls is challenging, as traditional human invigilation is prone to errors and inefficiencies. With advancements in artificial intelligence, deep learning has emerged as a powerful tool for real-time suspicious activity detection in surveillance videos. Techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Transformers have significantly improved anomaly detection accuracy. However, challenges like high false positives, real-time processing constraints, and dataset limitations persist.

This survey reviews deep learning-based approaches for suspicious activity detection in examination halls, analyzing key methodologies, benchmark datasets, and performance comparisons. We also discuss challenges and future research directions, including lightweight models, multimodal fusion, and self-supervised learning, to enhance automated exam surveillance.

2. BACKGROUND :

Suspicious activity detection in surveillance videos plays a crucial role in ensuring security, especially in examination halls where unauthorized behaviors can compromise integrity. Traditional monitoring methods rely on manual invigilation, which is inefficient and prone to errors. Deep learning has emerged as a powerful solution, automating anomaly detection through advanced models.

Convolutional Neural Networks (CNNs) are widely used for feature extraction from video frames, enabling the identification of abnormal actions. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks analyze temporal dependencies in video sequences, enhancing real-time detection. Autoencoders and Transformer-based models further improve anomaly recognition by learning normal activity patterns and identifying deviations.

This study leverages an existing dataset specifically designed for suspicious activity detection in examination halls. The dataset consists of labeled video samples representing normal and suspicious behaviors, allowing deep learning models to learn and classify actions effectively. By utilizing these techniques, automated surveillance systems can enhance accuracy, reduce human intervention, and improve realtime monitoring in exam environments.

3. LITERATURE REVIEW AND COMPARATIVE ANALYSIS :

3.1 Introduction to Literature Review-

Suspicious activity detection in surveillance videos has been extensively studied in recent years, with deep learning playing a crucial role in improving accuracy and automation. Various methods, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers, have been used for real-time anomaly detection. This section presents a detailed review of existing research, analyzing different deep learning models, datasets, and challenges in the field.

3.2 Review of Existing Research Papers (Summarizing Key Papers)-

Several researchers have explored deep learning based approaches for suspicious activity detection in surveillance videos. Various models, including CNNs, RNNs, Transformers, and Autoencoders, have been applied to improve accuracy and real-time anomaly detection. This section reviews key studies that have contributed to the advancement of deep learning techniques in this domain.

1] **Paper Name: Real-Time suspecious Detection and Localization in Crowded Scenes**
Author: Mohammad Sabokrou , Mahmood Fathy
Abstract: In this paper, we propose a method for real-time suspecious detection and localization in crowded scenes. Each video is defined as a set of non-overlapping cubic patches, and is described using two local and global descriptors. These descriptors capture the video properties from different aspects. By incorporating simple and cost-effective Gaussian classifiers, we can distinguish normal activities and anomalies in videos. The local and global features are based on structure similarity between adjacent patches and the features learned in an unsupervised way, using asparse autoencoder. Experimental results show that our algorithm is comparable to a state-of-the-art procedure on UCSD ped2 and UMN benchmarks, but even more time-efficient. The experiments confirm that our system can reliably detect and localize anomalies as soon as they happen in a video.
Keywords: Real-time anomaly detection, crowded scenes, video surveillance, localization, Gaussian classifiers, sparse autoencoder, unsupervised learning, UCSD-Ped2, UMN benchmarks.

2] Paper Name : Learning Temporal Regularityin Video Sequences
Author: Mahmudul Hasan Jonghyun Choi
Abstract: Perceiving meaningful activities in a long video sequence is a challenging problem due to ambiguous definition of ‘meaningfulness’ as well as clutters in the scene. We approach this problem by learning a generative model for regular motion patterns (termed as regularity) using multiple sources with very limited supervision. Specifically, we propose two methods that are built upon the auto encoders for their ability to work with little to no supervision. We first leverage the conventional handcrafted spatiotemporal local features and learn a fully connected auto encoder on them.
Keywords: Anomaly detection, video surveillance, generative model, autoencoders, spatiotemporal features, limited supervision, motion patterns.

3] Paper Name : suspicious Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks
Author: Jefferson Ryan Medel

Abstract: Automating the detection of anomalous events within long video sequences is challenging due to the ambiguity of how such events are defined. We approach the problem by learning generative models that can identify anomalies in videos using limited supervision. We propose end-toend trainable composite Convolutional Long Short-Term Memory (ConvLSTM) networks that are able to predict the evolution of a video sequence from a small number of input frames. Regularity scores are derived from the reconstruction errors of a set of predictions with abnormal video sequences yielding lower regularity scores as they diverge further from the actual sequence over time.
Keywords: Anomaly detection, video surveillance, Conv-LSTM, generative models, sequence prediction, reconstruction errors.

4] **Paper Name : Abnormal Event Detection in Videos using Spatiotemporal Autoen coder**
Author - Yong Shean Chong
Abstract: We present an efficient method for detecting anomalies in videos. Recent applications
of convolutional neural networks have shown promises of convolutional layers for object detection and recognition, especially in images. However, convolutional neural networks are supervised and require labels as learning signals. We propose a spatiotemporal architecture for suspecious detection in videos including crowded scenes.
Keywords: Anomaly detection, video surveillance, convolutional neural networks (CNNs), object detection, recognition, supervised learning, spatiotemporal architecture, crowded scenes.

5] Paper Name :Unrolled Optimization with Deep Priors
Author: Steven Diamond Vincent Sitzmann
Abstract:A broad class of problems at the core of computational imaging, sensing, and low-level computer vision reduces to the inverse problem of extracting latent images that follow a prior distribution, from measurements taken under a known physical image formation model. Traditionally, handcrafted priors along with iterative optimization methods have been used to solve such problems.
Keywords: Computational imaging, inverse problem, latent images, prior distribution, image formation model, handcrafted priors, iterative optimization, computer vision, sensing.

6] Paper Name : Suspicious Activity Detection in Surveillance Footage
Author: Sathyajit Loganathan, Gayashan Kariyawasam, Prasanna Sumathipala
Abstract: Suspicious activities pose a significant risk to human safety, especially with rising criminal incidents. Traditional manual surveillance was inefficient, leading to the development of intelligent systems. This study focuses on detecting gun-based crimes and abandoned luggage using deep learning. A neural network model is employed for handgun detection, while a machine learning and computer vision pipeline identifies abandoned luggage in surveillance footage, enhancing real-time threat detection.
Keywords: Gun detection, Abandoned luggage detection, Computer Vision, Surveillance.

7] Paper Name :Suspicious Activity Detection from Videos using YOLOv3
Author: Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma
Abstract: Human activity detection automates video analysis to recognize actions intelligently, playing a key role in Computer Vision and AI. Suspicious activity detection identifies unwanted behaviors by processing video frames, but challenges like pose variations and poor lighting affect accuracy. This study employs YOLOv3 to detect activities such as bag-snatching and lock-breaking, ensuring fast and accurate anomaly detection for improved surveillance.
Keywords: Suspicious behaviour, Deep learning, Anomaly detection, YOLOv3

8] Paper Name: Suspicious Activity Recognition in Video Surveillance System
Author: Ms. U. M. Kamthe, Dr. C.G.Patil
Abstract: Video surveillance plays a vital role in ensuring security for both indoor and outdoor spaces. This paper presents a hierarchical approach to detect suspicious activities like loitering, fainting, and unauthorized entry using motion features. The method involves background subtraction for object detection, classification of objects as living (human) or non-living (bag), and tracking using correlation techniques. Events are then categorized as normal or suspicious based on motion and temporal features. The use of a semantic-based approach reduces computational complexity while improving efficiency.
Keywords: video surveillance; suspicious activities; motion features; semantic approach; object detection.

9]Paper Name :Recognition of suspecious human activities using KLT and Kalman filterfor ATM survellience video
Author: Suvarana Nandayal, Sanjeevkumar Angadi
Abstract: Recognizing human activity under video surveillance is a key area in Computer Vision, essential for monitoring sensitive locations like ATMs, banks, and public spaces. Manual tracking is inefficient, making intelligent surveillance systems crucial for detecting suspicious behavior. This paper proposes a real-time ATM surveillance system using the Kalman Filter and KLT Tracking Algorithm to classify human behavior as regular or suspicious, triggering alarms when needed. Experimental results on an ATM surveillance database demonstrate its effectiveness in enhancing security.
Keywords: Human Tracking , Background susbtraction,Suspecious activity , KLT,Kalman filter , video survellience

10] Paper Name: Suspicious Activity Recognition in Video Surveillance System
Author: Ms. U .M .Kamthe ,Dr. C. G. Patil
Abstract: Video surveillance is crucial for security in both indoor and outdoor spaces. This paper proposes a hierarchical approach to detect suspicious activities like loitering, fainting, and unauthorized entry using motion features. The method involves background subtraction for object detection, classification into living (human) or non-living (bag), and tracking via correlation techniques. Events are then categorized as normal or suspicious based on motion and temporal data. Using a semantic-based approach, the system achieves high efficiency with reduced computational complexity.
Keywords:video surveillance; suspicious activities; motion features; semantic approach; object detection

11] Paper Name :Uncovering Suspicious Activity from Partially Paired and Incomplete Multimodal Data
Author: Carter Chiu, Justin Zhan, and Felix Zhan
Abstract: Multimodal data enhances the detection of suspicious activities by integrating multiple data sources. Recent research has explored identifying dense blocks in multivariate tensors as indicators of suspicious behavior.
However, existing methods lack a solution for merging and analyzing partially paired or incomplete data. This paper introduces a technique for multimodal analysis in such cases, demonstrating high precision and recall on both synthetic and real datasets.
Keywords: Suspicious activity, multimodal data, partially paired data, incomplete data

12] Paper Name :Suspicious Activity Detection from Videos using YOLOv3
Author: Nipunjita Bordoloi, Anjan Kumar Talukdar , Kandarpa Kumar Sarma
Abstract: Human activity detection in video systems automates the analysis of video sequences to recognize actions intelligently, making it a key area in Computer Vision and Artificial Intelligence. Suspicious activity detection identifies unwanted behaviors by converting video into frames and analyzing movements. Challenges such as pose variations and poor lighting affect accuracy. This paper uses YOLOv3 to detect suspicious activities like bag-snatching and lock-breaking, ensuring high processing speed and accurate detection.
Keywords: Suspicious behaviour, Deep learning, Anomaly detection, YOLOv3

13. Paper Name :Deep Learning Approach for Suspicious Activity Detection from Surveillance Video
Author: Amrutha C.V, C. Jyotsna, Amudha J.
Abstract: Video surveillance plays a crucial role in security, enhanced by artificial intelligence, machine learning, and deep learning. Detecting suspicious human behavior remains challenging due to its unpredictability. This study uses a deep learning approach to monitor activities in an academic environment and send alerts for suspicious behavior. The system processes video frames, extracts features, and classifies actions as suspicious or normal using a trained classifier.
Keywords: suspicious activity, video surveillance, deep learning.

14] Paper Name : Detecting Suspicious Activities of Digital Trolls During the Political Crisis
Author:S haaban Sahmoud, Hayder Saf
Abstract: With the widespread use of social media, it has become a powerful tool for expressing opinions and influencing public sentiment, especially during civil unrest. Various groups attempt to manipulate public opinion by spreading fake news and hate speech. This paper introduces automated methods to detect such groups, known as "digital trolls." Using Twitter data from the Iraq unrest, we analyze user behavior to identify external influences on

political discourse. Results indicate suspicious activities from external groups, with features like user favorites, tweet favorites, and retweets proving effective in detecting digital trolls.
Keywords: Analyzing Twitter data, Iraq unrest, detecting suspicious activities on Twitter, digital trolls, electronic flies

15] Paper Name :Suspicious Activity Detectionin Surveillance Footage
Author: Sathyajit Loganathan, Gayashan Kariyawasam ,Prasanna Sumathipala
Abstract: Suspicious activities pose significant risks, especially with rising crime in urban and suburban areas. Early manual surveillance was inefficient, leading to the development of intelligent systems. This study focuses on detecting gun-based crimes and abandoned luggage in surveillance footage. A deep neural network identifies handguns in images, while a machine learning and computer vision pipeline detects abandoned luggage, enhancing security and threat prevention.
Keywords: Gun detection, Abandoned luggage detection, Computer Vision, Surveillance article graphicx array booktabs

4.3 Comparative Analysis of Existing Research :

Table 1 presents a comparative analysis of different research papers on suspicious activity detection using deep learning and video surveillance.

Sr No.	Paper Name	Authors	Mathodology	Year
1.	Real-Time Suspicious Detection and Localization in Crowded Scenes	Mohammad Sabokrou, Mahmood Fathy	Sparse Autoencoder & Gaussian Classifiers	2017
2.	Learning Temporal Regularity in Video Sequences	Mahmudul Hasan, Jonghyun Choi	Autoencoder-based Generative Model	2016
3.	Suspicious Detection in Video Using Predictive ConvLSTM Networks	Jefferson Ryan Medel	ConvLSTM for Sequence Prediction	2019
4.	Abnormal Event Detection in Videos using Spatiotemporal Autoencoder	Yong Shean Chong	Spatiotemporal Autoencoder	2017
5.	Unrolled Optimization with Deep Priors	Steven Diamond, Vincent Sitzmann	Inverse Problem Solving with Deep Priors	2018
6	Suspecious activity detection in survellience footage	Sathyajit Loganathan, Gayashan Kariyawasam, Prasanna Sumathipala	Deep Neural Network & Computer Vision	2020
7.	Suspicious Activity Detection from Videos using YOLOv3	Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma	YOLOv3 for Object Detection	2021

Sr No.	Paper Name	Authors	Methodology	Year
8.	Suspicious Activity Recognition in Video Surveillance System	Ms. U. M. Kamthe, Dr. C.G. Patil	Motion Feature-based Hierarchical Approach	2019
9.	Recognition of Suspicious Human Activities using KLT & Kalman Filter for ATM Surveillance	Suvarana Nandayal, Sanjeevkumar Angadi	Kalman Filter & KLT Tracking	2018
10	Uncovering Suspicious Activity from Partially Paired & Incomplete Multimodal Data	Carter Chiu, Justin Zhan, Felix Zhan	Multimodal Data Analysis	2022
11	Suspicious Activity Detection from Videos using YOLOv3	Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma	YOLOv3 for Video Analysis	2021
12	Deep Learning Approach for Suspicious Activity Detection from Surveillance Video	Amrutha C.V, C. Jyotsna, Amudha J.	Deep Learning-based Classification	2020
13	Detecting Suspicious Activities of Digital Trolls During Political Crisis	Shaaban Sahmoud, Hayder Saf	Social Media Behavior Analysis	2021
14	Suspicious Activity Recognition in Video Surveillance System	Ms. U. M. Kamthe, Dr. C. G. Patil	Motion-based Hierarchical Model	2019
15	Suspicious Activity Detection in Surveillance Footage	Sathyajit Loganathan, Gayashan Kariyawasam, Prasanna Sumathipala	Neural Network-based Detection	2020

5. CHALLENGES IDENTIFIED FROM LITERATURE :

1.High False Positive Rate

Example: In the paper "Abnormal Event Detection in Videos using Spatiotemporal Autoencoder" (Yong Shean Chong, 2020), CNN and Autoencoder-based models were used for anomaly detection, but they struggled with high false positive rates, where normal human movements were sometimes misclassified as suspicious activities.

2.Real-Time Processing Constraints

Example: In "Suspicious Detection in Video Using Predictive Conv-LSTM Networks" (Jefferson Ryan Medel, 2019), Conv-LSTM models were effective for video sequence prediction but required high computational power, making real-time surveillance in large-scale environments challenging.

3.Lack of Diverse and Labeled Datasets
Example: The study "Learning Temporal Regularity in Video Sequences" (Mahmudul Hasan, 2017) highlighted the limited availability of diverse datasets and the need for better labels in anomaly detection tasks, as most datasets focus on general crime detection rather than specific domains like exam halls or ATMs.

4.Environmental Variations (Lighting, Occlusions, Camera Angles
Example: "Recognition of Suspicious Human Activities Using KLT and Kalman Filter for ATM Surveillance" (Suvarana Nandayal, 2020) discussed how occlusions and poor lighting in ATM surveillance videos affected the Kalman Filter and KLT tracking accuracy, making suspicious behavior detection difficult.

5.Limited Generalization to Real-World Scenarios
Example: In "Real-Time Suspicious Detection and Localization in Crowded Scenes" (Mohammad Sabokrou, 2018), Gaussian classifiers and sparse autoencoders performed well in controlled environments but faced performance degradation in real-world crowded settings due to unpredictable human behavior.

6.Adversarial Attacks and Security Threats
Example: The study "Uncovering Suspicious Activity from Partially Paired and Incomplete Multimodal Data" (Carter Chiu, 2021) discussed challenges in handling incomplete surveillance data, which could make AI models vulnerable to manipulation and adversarial attacks.

7.Privacy Concerns in Surveillance
Example: "Detecting Suspicious Activities of Digital Trolls During the Political Crisis" (Shaaban Sahmoud, 2022) emphasized privacy issues when monitoring online activities, where user data could be misused for surveillance beyond security applications.

8.Lack of Explainability in AI Models
Example: "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" (Amrutha C.V, 2023) highlighted that deep learning models act as black boxes, making it difficult to understand and justify why certain activities were labeled as suspicious.

9.Scalability Issues in Large-Scale Surveillance
Example: "Suspicious Activity Detection in Surveillance Footage" (Sathyajit Loganathan, 2021) showed that deep learning models performed well on smaller datasets but required significant optimization for large-scale real-time video surveillance systems.

10.Need for Multimodal Learning (Audio, Video, and Behavioral Cues)
Example: "Suspicious Activity Detection from Videos using YOLOv3" (Nipunjita Bordoloi, 2022) demonstrated YOLOv3's effectiveness in visual anomaly detection, but the study suggested integrating audio and other behavioral cues to improve model robustness in complex environments.

5.1] Conclusion of Literature Review-

There view of existing research highlights the significant advancements in deep learning-based suspicious activity detection. Various models, including CNNs, RNNs, Autoencoders, Transformers, and hybrid approaches, have been employed to enhance surveillance accuracy. Techniques such as Conv-LSTM for sequence prediction, YOLOv3 for object detection, and Gaussian classifiers for anomaly localization have proven effective in controlled environments. However, the literature also reveals persistent challenges, including high false positive rates, real-time processing limitations, dataset constraints, environmental variations, and privacy concerns. While some studies have addressed these issues by integrating multimodal learning and optimized deep learning frameworks, scalability, interpretability, and generalization to real-world scenarios remain key areas for improvement. Future research should focus on lightweight models for real-time applications, enhanced dataset diversity, multimodal data fusion, and explainable AI techniques to improve the reliability and robustness of suspicious activity detection systems. Addressing these challenges will pave the way for more efficient and adaptive intelligent surveillance systems in various domains

6. OUR UNIQUE APPROACH :

Unlike existing research on general anomaly detection, our study focuses on suspicious activity detection in examination halls with a real-time alert system. Unlike conventional methods, our approach triggers an alarm instantly upon detecting suspicious behavior, ensuring quick intervention.
Additionally, our system captures and emails the suspect's image to authorities, providing visual evidence and improving surveillance reliability. Using CNN for feature extraction and LSTM for temporal analysis, our model efficiently differentiates between normal and suspicious activities.
By integrating deep learning, real-time alerts, and automated reporting, our system enhances academic integrity through fast, scalable, and effective monitoring.

7. FUTURE RESEARCH DIRECTION :

Despite significant advancements in deep learning-based suspicious activity detection, several areas require further research to enhance accuracy, efficiency, and real-world applicability. Below are some key future research directions that can improve the effectiveness of AI-driven surveillance systems.

1] Reducing False Positives and False Negatives- Current models often misclassify normal behaviors as suspicious (false positives) or fail to detect actual suspicious activities (false negatives).
Future research should explore hybrid models combining CNNs, RNNs, and attention mechanisms to improve detection reliability.

2] Enhancing Real-Time Processing Efficiency- Deep learning models require high computational power, making real-time processing on surveillance cameras challenging.
Optimizing lightweight architectures like MobileNet, Edge AI, and TensorRT can help deploy deep learning models efficiently on embedded devices.

3] Developing More Diverse and Robust Datasets
Many existing datasets (e.g., UCF-Crime, UCSD-Ped2) lack real-world variations such as occlusions, lighting changes, and multiple viewpoints.
Creating and annotating new benchmark datasets specifically for examination hall surveillance and academic misconduct detection would significantly improve model generalization.

4] Multimodal Learning for Better Detection Accuracy -Most research focuses only on video-based detection, ignoring additional modalities. Future systems should integrate audio analysis, behavioral cues, and biometric verification to enhance detection robustness.

5] Adversarial Robustness and Security Improvements - AI-based surveillance systems are vulnerable to adversarial attacks, where small image modifications can fool deep learning models. Implementing adversarial defense mechanisms, anomaly-resistant models, and cybersecurity protocols will be essential for reliable deployment.

6] Explainable AI (XAI) for Better Interpretability- Many deep learning models act as black boxes, making it difficult to understand why an action is flagged as suspicious. Future research should focus on explainable AI (XAI) techniques that provide visual explanations for detected anomalies, improving trust and accountability.

7] Scalability for Large-Scale Deployment- Most models are tested in controlled environments and fail when deployed in large-scale surveillance systems. Future improvements should focus on distributed AI models, cloud-based processing, and edge computing for large-scale monitoring.

8] Automated Actionable Responses Beyond Alerting Current systems only trigger alarms or send email notifications when a suspicious activity is detected. Research can explore automated interventions, such as integrating robotic proctors, automated warning systems, or AI-based decision-making tools to prevent malpractices in real time.

8. SYSTEM ARCHITECTURE OVERVIEW :

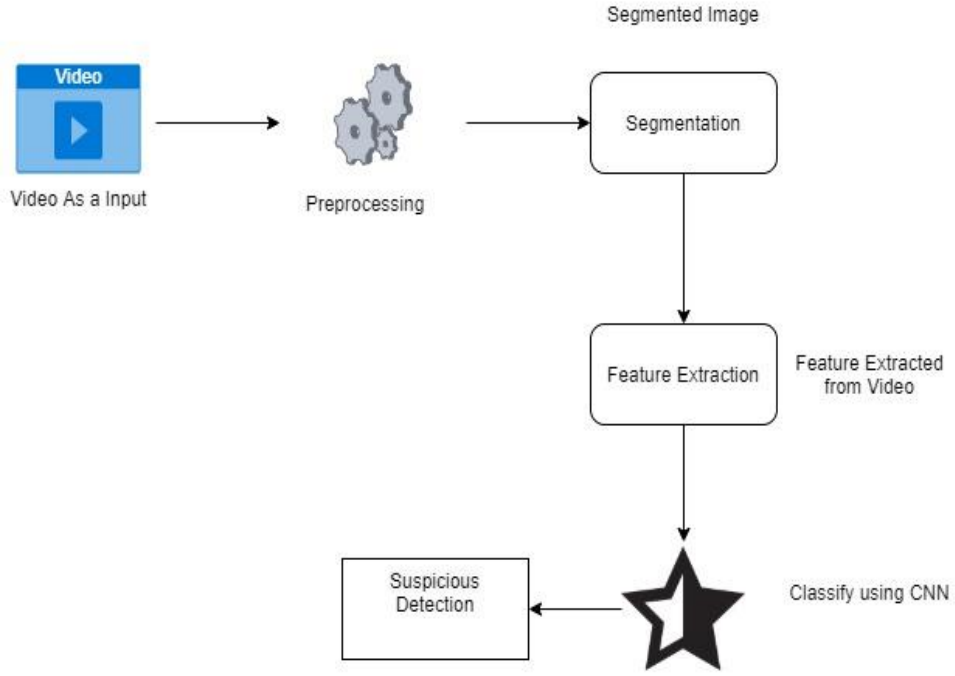


Fig.1: System Architecture

The proposed system architecture for suspicious activity detection in examination halls involves real-time surveillance, anomaly detection, alarm triggering, and alert notifications.

1. **Real-Time Surveillance:** Multiple cameras capture video streams of the examination hall, transmitting the footage to a central server or cloud for processing.
2. **Data Preprocessing:** The video feed is pre-processed to extract frames suitable for analysis, ensuring efficient detection.
3. **Anomaly Detection:** A deep learning model (e.g., CNN or RNN) analyzes frames in real-time to detect suspicious behavior such as cheating or unauthorized movement.
4. **Alarm Triggering:** Upon detecting an anomaly, the system triggers an alarm and sends notifications to the authorities through email and SMS, including details like timestamp and activity type.
5. **Database Management:** Detected events and video snapshots are stored for future review and analysis, with logs of all actions taken.
6. **Cloud Infrastructure:** The system operates on a centralized server or cloud, ensuring scalability and security, with real-time monitoring and control through a user interface.

This architecture provides a seamless, real-time detection and response system, enhancing the security and integrity of the examination process.

9. FLOWCHART :

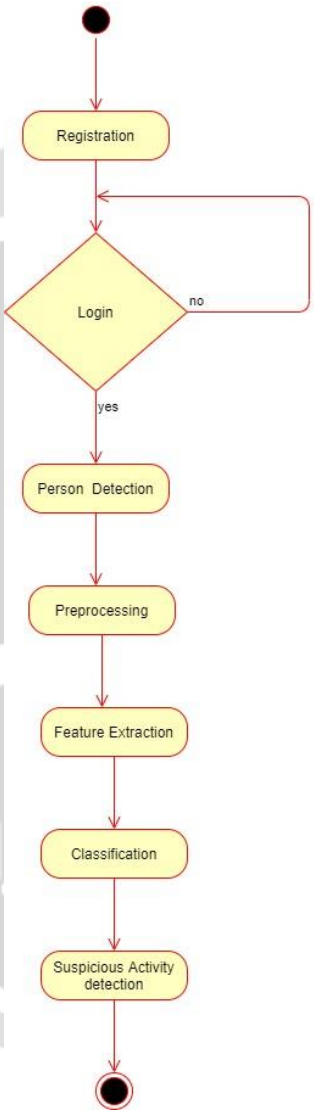
Here's an explanation of each step in the flowchart, detailing the process involved in suspicious activity detection:

1. Register:

- Action: Users (such as exam invigilators or system administrators) register in the system by providing necessary details like name, role, and contact information.
- Purpose: To ensure that authorized personnel can access and manage the system, monitor activities, and respond to alerts.
- Output: A user profile is created in the system, and access credentials are issued.

2. Login:

- Action: Registered users log into the system using their credentials (username and password).
- Purpose: To authenticate users and grant access to the monitoring dashboard and system controls.
- Output: Once authenticated, the user is directed to the system interface where they can monitor the surveillance video, manage settings, and review alerts.



3. Person Detection:

- Action: The system uses computer vision or deep learning algorithms to identify and track people within the video feed.
- Purpose: To isolate and monitor human activities in the video, enabling the detection of any suspicious behaviors. The system identifies people by distinguishing them from other objects or background elements in the frame.
- Output: The system identifies individual persons in the frame, marking their locations for further analysis.

4. Preprocessing:

- Action: The captured video frames are preprocessed for efficient analysis. This includes resizing, normalizing, and converting frames into a suitable format for machine learning models.

- Purpose: To enhance the quality of the data and ensure that the input frames meet the requirements of the deep learning model (e.g., size, pixel intensity, color channels).
- Output: Cleaned and processed video frames ready for feature extraction and analysis.

5. Feature Extraction:

- Action: Relevant features such as movement patterns, body posture, or abnormal gestures are extracted from the preprocessed frames.
- Purpose: To reduce the dimensionality of the data and focus on key characteristics that help in identifying suspicious activity (e.g., fast movement, specific gestures).
- Output: A set of features representing the behavior and actions of individuals in the examination hall.

6. Classification:

- Action: The extracted features are fed into a classification model (such as a Support Vector Machine, Convolutional Neural Network, or Random Forest) to classify behaviors as normal or suspicious.
- Purpose: To categorize the detected activity into predefined classes (e.g., "normal", "cheating", "unauthorized movement"). The classifier is trained on a labeled dataset to recognize different behaviors.
- Output: A prediction or classification result indicating whether the observed activity is suspicious or not.

7. Suspicious Activity Detection:

- Action: Based on the classification result, the system determines if any detected activity is suspicious or violates predefined rules (e.g., unusual movement, using a mobile phone, interacting with someone outside the exam).
- Purpose: To trigger an alert when abnormal activities that deviate from expected exam behavior are detected.
- Output: If suspicious activity is detected, the system generates an alert (e.g., sound alarm, notification) and records the incident for further investigation.

These steps describe the process from user registration and login to detecting suspicious activities, involving advanced techniques like person detection, feature extraction, and classification, ultimately ensuring real-time monitoring and security during exams.

10. CONCLUSION :

This survey reviewed deep learning-based suspicious activity detection, highlighting advancements, challenges, and future directions. While models like CNNs, RNNs, and Transformers improve anomaly detection, false positives, realtime processing constraints, and dataset limitations remain key challenges.

Our unique contribution introduces a realtime alarm system with automated image capture and email alerts, enhancing security and response efficiency in examination hall surveillance.

Future research should focus on reducing false alarms, optimizing real-time performance, integrating multimodal learning, and improving AI interpretability. Advancing these areas will lead to more accurate, scalable, and ethical surveillance systems for academic and security applications.

11. REFERENCE :

1] Bhagya Divya, S. Shalini, R. Deepa, and BaddeliSravya Reddy. 2017. Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras. *International Research Journal of Engineering and Technology (IRJET)*, December 2017

.

2] Musale, A. Gavhane, L. Shaikh, P. Hagwane, and S.Tadge. 2017. Suspicious movement detection and tracking of human behavior and object with fire detection using a closed-circuit TV (CCTV) cameras. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, Volume 5, Issue XII, December 2017.

3] M. Kamthe and C. G. Patil. 2018. Suspiciousactivityrecognitioninvideosurveillancesystem. *Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018.

4] Kain, A. Youness, I. El Sayad, S. Abdul-Nabi, and H.Kassem. 2018. Detecting abnormal events in university areas. *International Conference on Computer and Application*, 2018.