IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12821

ABNORMAL BEHAVIOUR DETECTION

Sindhu BM[1], Swetha CS[2]

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology[2]

Abstract: Modern security teams in busy public spaces often struggle to keep up with ever-growing video surveillance demands, missing crucial incidents due to human fatigue and excessive false alarms. This project puts forward a smart, automated surveillance tool that uses only the movement patterns captured by cameras—never faces or identifying features—to spot genuinely suspicious activities like fights or panic situations in crowds. Built using open-source tools on regular computers, the system breaks up video footage, analyzes how people move, and recognizes the difference between everyday strolls and dangerous behavior, all while preserving privacy. Its machine learning algorithms learn from thousands of real-life examples, so it's accurate and alert only when it really matters, drawing attention to anomalies with clear boxes and labels on the screen. In essence, this research marks a step toward smarter, fairer public safety, making advanced surveillance accessible and ethical for crowded places everywhere.

Keywords: Abnormal Behaviour Detection, Computer Vision, Optical Flow Analysis, Machine Learning, Crowd Surveillance, SVM (Support Vector Machine), KNN (K-Nearest Neighbours), Logistic Regression.

I. INTRODUCTION

Keeping crowded places like shopping malls, train stations, and public events safe is a big challenge for security staff, who can easily miss threats while juggling dozens of camera feeds. Most traditional surveillance systems either overwhelm teams with false alarms or risk people's privacy by storing personal data.

This project introduces a smarter, privacy-friendly way to automatically spot unusual or suspicious behavior in video footage. Instead of identifying faces, the system pays attention only to how people move—like noticing the difference between someone running to catch a bus and someone involved in a fight or panic. By relying on proven computer vision techniques and cutting-edge machine learning, the system quietly watches for warning signs and instantly highlights them onscreen, complete with color-coded labels.

With a simple interface and real-time updates, the technology helps security teams cut through the noise so they can focus on real incidents—making public spaces not only safer, but also more respectful of everyone's privacy. It works on typical computers and can be set up easily, making advanced safety accessible to places of all sizes.

II. RELATED WORK

The detection of abnormal behavior in surveillance videos has witnessed substantial advancements through the use of deep learning and computer vision techniques, which have greatly enhanced the accuracy and applicability of monitoring systems.

Kuppusamy and Bharathi surveyed the application of Convolutional Neural Networks (CNNs) for detecting abnormal human behaviors in both crowded and uncrowded environments. Their work highlights how CNNs efficiently extract spatial and temporal features from videos, which is crucial for distinguishing normal pedestrian activity from suspicious behaviors like fighting or panic[1]. They also discuss the limitations posed by varying image resolutions and the importance of diverse datasets for training robust models.

Greer et al. (2023) provided a comprehensive review of crowd anomaly detection, categorizing different types of anomalies and their associated datasets. By organizing abnormal behaviors into distinct taxonomies, their work aids researchers in benchmarking and developing systems tailored to specific anomaly types, such as crowd turbulence or isolated abnormal acts[10].

The study by Madhusudhan Reddy et al. (2021) combined the YOLO real-time object detection framework with CNN-based spatial feature extraction to recognize abnormal human behaviors. This hybrid method improved the system's ability to localize individuals and analyze their interactions in real-time, demonstrating promising results for practical surveillance applications[9].

Kumar and Sampath(2023) introduced spatiotemporal inter-fused autoencoder model that surpasses several popular classifiers in detecting crowd anomalies across multiple benchmark datasets[11]. Their deep learning model leverages attention mechanisms and multi-modal data integration, reaching accuracy rates exceeding 99%, indicating the value of combining spatial and temporal data.

Finally, Mishra and Meher (2024) proposed customized lightweight CNN model optimized for efficient abnormal

DOI: 10.17148/IARJSET.2025.12821

activity detection with lower latency and energy consumption [7] . Using MobileNet-based segmentation to eliminate irrelevant video frames, their approach enhances computational efficiency, making real-time detection more accessible for systems with limited computational resources.

Together, these studies illustrate a clear progression toward multi-faceted, deep learning-enhanced surveillance systems capable of accurately identifying abnormal human activities under diverse and challenging conditions. The present project builds on these approaches by combining optical flow analysis, classical classifiers such as SVM and KNN, and privacy-preserving motion features for reliable, real-time abnormal behavior detection.

III. PROPOSED SYSTEM

The new system uses smart computer programs to watch videos and spot problems automatically, like fights, people panicking, or other unusual actions—learning from the way cutting-edge artificial intelligence is now used all over the world. Instead of looking at faces or collecting personal information, it pays attention only to how people move, which means people's privacy is protected and there's less risk of breaking any rules about personal data. The system can keep an eye on many cameras at once, and if something looks odd in any video, it instantly marks the spot with a colored box so security staff know exactly where to look and what's happening, so alerts are sent quickly, helping security react much faster compared to older systems that required someone to watch all screens all the time. Smart learning techniques are used to teach the system what's "normal" and what's not, so it keeps getting better the more videos it checks. It combines simple models and advanced deep learning, making sure the system is accurate and works for different places or crowd situations. The whole setup is affordable and easy to use, needing only normal computers and free software tools, so it can be put in places of any size, not just big or rich organizations.

IV. EXISTING SYSTEM

Lots of video screens, not enough eyes: Older systems count on security guards to watch lots of video feeds at once all day. This is tiring, and it's easy for guards to miss actual incidents.

Too many useless alarms: The system rings an alert for any movement—whether it's a person just walking or doing something unusual. This means security gets bombarded with too many false alarms for normal behavior.

Privacy problems: To try and improve accuracy, some systems use facial recognition or track individuals closely, which collects a lot of private information—sometimes without people even knowing.

Not smart enough: These systems can't really tell whether what they're seeing is harmless or dangerous. They struggle to tell the difference between someone running for a bus and someone in a fight.

Hard to expand: If a company wants to monitor more cameras or a bigger space, it has to hire more people to watch the screens, driving up costs fast.

Slow reactions: It often takes too long for someone to spot a problem and respond, so issues sometimes aren't handled until it's too late.

Bottom line: The old way wastes security staff's time, causes privacy worries, and still doesn't keep crowded places as safe as they should be.

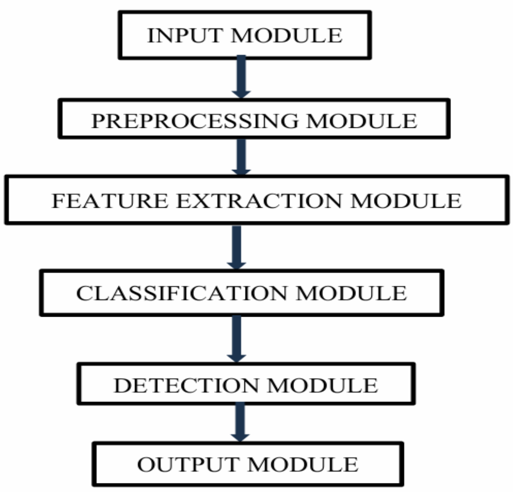

Fig 1: System Architecture

DOI: 10.17148/IARJSET.2025.12821

The abnormal behaviour detection system's architecture consists of a number of interconnected parts that process video input and produce activity predictions collectively. The principal elements consist of:
Input Module: Source can be surveillance footage or pre-recorded dataset.
Preprocessing Module: Extracts frames, resizes, normalizes, and augments them.
Feature Extraction Module: Calculate optical flow feature, morphological analysis and combines motion and shape descriptors for each object.
Classification Module: Utilizing three classifiers to train model such as SVM, KNN ,Logistic Regression.
Detection Module :Abnormal objects are highlighted with a red rectangle .
Output Module: Displays predicted activities with confidence scores.

V. IMPLEMENTATION

Python: Python is ideal for image processing and machine learning due to its clean syntax and vast library support.
OpenCV (Open Source Computer Vision Library):OpenCV is widely used for real-time image and video processing.
NumPy : Efficient array handling and mathematical operations.
scikit-learn: Provides easy to-use implementations of standard machine learning algorithms.
Matplotlib(Visualization): Helps in visualizing model performance and image data.
Computer Vision: Computer Vision is the field of enabling machines to "see" and interpret visual information like images and videos.
Machine Learning (ML) : Machine learning is a method of teaching computers to learn from data without being explicitly programmed.

- **K-Nearest Neighbors (KNN)** : It compares a new data point with its 'k' closest points (neighbors) in the training dataset and assigns the most common label among them.
- **Logistic Regression** : It estimates the probability that a data point belongs to a certain class.
- **Support Vector Machine (SVM)**

Working: It finds the optimal hyperplane that separates two classes with the maximum margin.

VI. EVALUATION AND RESULT

The evaluation of this Abnormal Behaviour Detection project shows it to be a highly effective system that can accurately distinguish between normal and abnormal activities in videos of crowded public spaces. Using a combination of advanced image processing, optical flow analysis, and three machine learning models—K-Nearest Neighbours, Support Vector Machine, and Logistic Regression—the system was trained on thousands of video frames capturing both usual pedestrian movements and unusual behaviors like fighting or panic. It was rigorously tested on videos with various scenarios including clear instances of abnormal events, multiple activities happening simultaneously, low-light conditions, occlusions, and corrupted input files.
Overall, the system performed exceptionally well, correctly identifying suspicious behaviors with high confidence while maintaining a low false-alarm rate. It was able to overlay clear bounding boxes around abnormal regions in the video frames, displaying real-time alerts that aid security personnel's quick response. The model demonstrated stability and reliability, even when processing multiple video streams at once, and handled challenging conditions gracefully. This all means the system is not only accurate but also practical, protecting people's safety without generating unnecessary distractions or invading privacy.
In simpler terms, the project's results prove that this smart system can reliably tell when something unusual is happening in crowded places by simply watching how people move, not who they are. It highlights the trouble spots clearly, so security can act quickly and confidently. It works well in different lighting, watches many cameras at the same time, and even deals with imperfect video without crashing. This makes it a trustworthy helper that improves security while respecting everyone's privacy and helping reduce.

VII. CHALLENGES

- Too Many False Alarms: Sometimes, the system mistakes normal things—like someone running to catch a bus—for something dangerous, and keeps sounding alerts that aren't needed.
- Busy and Tricky Places: When places get crowded, dark, or have lots of angles (like shadows or blocked views), the system can struggle to spot what's really happening.
- Hard to Use in New Settings: If the system is set up in a place it isn't used to, it might miss out on real problems or give wrong alerts, because it learned from a totally different spot.
- Needs to Be Super Fast: In real life, security needs answers right away. But checking lots of videos at once, every second, takes a lot of computer power.

- People's Privacy: Some old systems watch faces or collect private data, which most people don't want—and it can even break privacy laws.
- Making Good Training Videos: To teach the system what's normal or not, lots of real videos need to be found, watched, and labelled by hand, which takes a lot of work and patience.

VIII. ETHICAL AND PRIVACY CONSEDERATION

The Abnormal Behaviour Detection project is built with ethics and privacy at its core, ensuring people are protected not just from danger but also from intrusive surveillance. Unlike many older security systems, this solution does not use facial recognition or try to identify individuals by their personal details. Instead, it simply watches for unusual movement patterns, such as fighting or sudden panic, and leaves regular, day-to-day actions alone. Everything the system processes—whether it's video or motion data—is stripped of any personal information, so no one's identity is ever at risk. Alerts are created only when truly abnormal activity is detected, and every decision the system makes is clear and easy for operators to understand. With these choices, the project respects privacy laws, avoids unfair profiling, and prevents stored security data from being misused. The end result is a surveillance tool that keeps public spaces safe while letting ordinary people go about their lives without feeling watched or singled out, balancing technology with respect and fairness for everyone.

IX. FUTURE WORK

- Real-time Implementation
- Deep Learning Integration
- Scalability to Larger Datasets
- Environmental Adaptability
- Alert and Notification System
- User-friendly Interface

X. CONCLUSION

The created abnormal behavior detection system serves as an example of how machine learning and computer vision may be integrated to enhance safety and surveillance applications. The system can differentiate between typical and aberrant human behavior by utilizing video frames, foreground extraction, optical flow analysis, and feature extraction. In order to automate the detection process that would otherwise necessitate constant human monitoring, the classifiers then generate predictions that indicate suspicious or anomalous actions in video sequences. The project demonstrated through testing that the pipeline can accurately recognize anomalous occurrences and process input data with reliability. The system is easy to maintain, expand, and connect with real-time applications because of its modular design, which handles each step independently, including preprocessing, optical flow production, and classification. Although speed, accuracy, and practical adaptability can always be improved, this study offers a solid basis for creating more intelligent and effective surveillance systems.

REFERENCES

[1]. Human abnormal behavior detection using CNNs in crowded and uncrowded surveillance – A survey P. Kuppusamy, V.C. Bharathi * School of Computer Science & Engineering, VIT AP University, Andhra Pradesh, India .

[2]. The use of convolutional neural networks for abnormal behavior recognition in crowd scenes Yangkai Wu , Luhua Qiu , Jinming Wang .

[3]. Efficient Anomaly Detection in Crowd Videos Using Pre-Trained 2D Convolutional Neural Networks - ABID MEHMOOD Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia

[4]. Arslan Basharat ,Alexei Gritai, Mubarak Shah,"Learning object motion patterns for anomaly detection and improved object detection",In Proceedings Conference: 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition,Anchorage, Alaska, USA , 24-26 June 2008 Anomaly detection in crowded scenes: technologies, challenges and opportunities

[5]. Massive Crowd Abnormal Behaviors Recognition Using C3D -Reem Alharthi, Areej Alhothali, Bander Alzahrani, Sahar Aldhaheri

[6]. Enhancing Crowd Safety at Hajj: Real-Time Detection of Abnormal Behavior Using YOLOv9 - AMANI A. ALSABEI, TAHANI M. ALSUBAIT AND HOSAMH. ALHAKAMI [7] Abnormal Human Behaviour Detection by Surveillance Camera -Manas Ranjan Mishra and Pramod Kumar Meher

[8]. Autonomous abnormal behaviour detection using trajectory analysis Muhammed Shuaau, Ka Fei Thang, Nai Shyan

DOI: 10.17148/IARJSET.2025.12821

Lai School of Engineering, Faculty of Computing, Engineering & Technology, Asia Pacific University of Technology & Innovation, Malaysia

[9]. HUMAN BEHAVIOR AND ABNORMAL DETECTION Dr.C.V.MADHUSUDAN REDDY,B RAMANA, SHAINULLAH FARHANA BANU,YESHA MANFUSA Professor,Assistant Professor, Student Department Of CSE Bheema Institute of Technology and Science, Adoni

[10]. A Review of the Recent Progress on Crowd Anomaly Detection Sarah Altowairqi, Suhuai Luo, Peter Greer School of Information and Physical Sciences, The University of Newcastle, Newcastle, Australia

[11]. Abnormal Crowd Behaviour Detection in Surveillance Videos Using Spatiotemporal Inter Fused Autoencoder Dhivya Karunya Sampath ,Krishna Kumar ,Department of Electronics & Communication Engineering, S.E.A. College of Engineering & Technology, Bengaluru, Visvesvaraya Technological University, Belagavi - 590018, India, 2.Department of Electronics & Abnormal behaviour in massive crowd 1BI23MC131 Communication Engineering, Gopalan College of Engineering and Management, Bengaluru, Visvesvaraya Technological University, Belagavi - 590018, India

[12]. Chaudharya, S., Khana, M.A., Bhatnagara, C. "Multiple anomalous activity detection v id os" In: 6th International Conference on Smart Computing and Communications, in ICSCC 2 Procedia Computer Science, vol. 125, pp. 336–345. Elsevier 2018

[13]. A.B. Mabrouk, E. Zagrouba, "Abnormal behavior recognition for intelligent video surveillance systems", A review Expert Systems with Applications, 91 (2018), pp. 480-491. [14] Riddhi Sonkar, Sadhana Rathod2 , and Renuka Jadhav3, Deepali Patil, "Crowd abnormal behaviour detection using deep learning",Department of Information Technology, Ramrao Adik Institute of Technology,Navi Mumbai, India 2020ITM Web of Conferences 32, 03040 2020.

[15]. Andrew Joemon,Awin Chris Joy,Ashwin Prakash ,Bibin Thomas ,Divya R,"Abnormal Event Detection Using CCTV Camera", International Journal of Innovative Science and Research Technology ,Volume 6, Issue ,6 June 2021.