AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6,NO.2(1) (2026)

Intelligent Surveillance for Suspicious Human Activity Recognition Using Deep Learning

G Bhagyeshwari
(M.Tech Artificial Intelligence)
Aurora's Scientific and Technological Institute,Telangana,India
Email: garabhagyeshwari@gmail.com
Dr.M. Sridhar
Head Of The Department Computer Science and Engineering
Aurora's Scientific and Technological Institute,Telangana,India
Email: msridhar.msr@gmail.com
Mr.Md. Soyal
Aurora's Scientific and Technological Institute,Telangana,India
Email: mohammadsoyal945@gmail.com

ABSTRACT

The rapid growth of surveillance systems in public and private spaces has increased the demand for intelligent methods to automatically detect suspicious human activities. Traditional monitoring systems rely heavily on human operators, making them inefficient, time-consuming, and prone to errors. This project proposes a deep learning-based approach for recognizing suspicious human activities from surveillance video streams in real time. The system utilizes advanced computer vision techniques to analyze video frames and extract meaningful spatial and temporal features that represent human behavior. The proposed system employs deep learning models such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to classify activities and identify abnormal or suspicious actions such as violence, loitering, or unauthorized access. Once such activities are detected, the system generates alerts and notifies relevant authorities for immediate response. This automated approach enhances surveillance efficiency, reduces human workload, and improves overall public safety by enabling proactive threat detection.

Keywords: Suspicious human activity recognition, deep learning, computer vision, surveillance systems, convolutional neural networks, LSTM, video analysis, anomaly detection, real-time monitoring, intelligent surveillance, behavior analysis, public safety, automated alert system, AI-based detection, smart security.

Received: 01-05-2026 | Accepted: 08-06-2026 | Published: 15-06-2026 | www.ajaccm.com

I. INTRODUCTION

With the increasing need for security in public and private environments, surveillance systems have become an essential component of modern infrastructure. However, traditional surveillance relies heavily on manual monitoring, where security personnel continuously observe video feeds to identify suspicious activities. This approach is not only labor-intensive but also prone to human error, fatigue, and delayed response times. As a result, many critical incidents go unnoticed or are detected too late, reducing the effectiveness of surveillance systems.

Advancements in deep learning and computer vision have enabled the development of intelligent systems capable of automatically analyzing video data and recognizing human activities. Techniques such as Convolutional Neural Networks (CNN) are used for spatial feature extraction, while Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models capture temporal patterns in video sequences. This project aims to leverage these technologies to build an automated system that can detect suspicious human behavior in real time, thereby improving security, reducing manual effort, and enabling faster response to potential threats.

II. LITERATURE SURVEY

1.Title: Deep Learning-Based Suspicious Activity Detection in Video Surveillance
Authors: W. Sultani, C. Chen, and M. Shah
Abstract: This study presents a deep learning-based approach for detecting anomalous and suspicious activities in surveillance videos. The system uses a combination of Convolutional Neural Networks (CNN) and temporal analysis to identify unusual patterns in video sequences. It learns normal behavior from training data and flags deviations as anomalies. The proposed method demonstrates high accuracy in detecting real-world suspicious events and reduces false alarm rates in complex environments.

2.Title: Real-Time Human Activity Recognition Using CNN and LSTM Networks
Authors: D. Tran, L. Bourdev, and R. Fergus
Abstract: This research focuses on recognizing human activities from video streams using a hybrid deep learning model combining CNN and Long Short-Term Memory (LSTM) networks. CNN is used for spatial feature extraction, while LSTM captures temporal dependencies between frames. The system effectively classifies different human actions and can identify abnormal or suspicious activities in real time, improving surveillance efficiency.

3.Title: Intelligent Video Surveillance for Anomaly Detection Using Deep Learning
Authors: H. Wang and C. Schmid
Abstract: This paper proposes an intelligent surveillance system that uses deep learning techniques to detect anomalies in video data. The system extracts motion patterns and behavioral features to distinguish between normal and abnormal activities. It is capable of identifying suspicious actions such as violence, running, and unusual crowd behavior. Experimental results show improved performance compared to traditional machine learning approaches.

4.Title: Automated Suspicious Behavior Detection Using Computer Vision and AI
Authors: K. He, X. Zhang, S. Ren, and J. Sun
Abstract: This study introduces an AI-based system for detecting suspicious human behavior in surveillance videos using advanced computer vision techniques. The model employs deep residual networks (ResNet) to improve feature extraction and classification accuracy. The system can detect complex activities in real time and generate alerts when abnormal behavior is

Received: 01-05-2026 | Accepted: 08-06-2026 | Published: 15-06-2026 | www.ajaccm.com

observed, enhancing security monitoring in public spaces.

5.Title: Video-Based Human Activity Recognition for Smart Surveillance Systems

Authors: M. Ziaeefard and R. Bergevin

Abstract: This research explores various approaches for human activity recognition in surveillance videos, focusing on machine learning and deep learning methods. The study highlights the importance of spatio-temporal feature extraction for accurately identifying human actions. The proposed system can detect suspicious activities by analyzing behavior patterns and provides a scalable solution for smart surveillance applications.

III. EXISTING SYSTEM

Existing surveillance systems primarily depend on manual monitoring or basic motion detection techniques to identify suspicious activities. In traditional setups, security personnel are responsible for observing multiple video feeds simultaneously, which often leads to fatigue and reduced attention over time. Basic automated systems use rule-based algorithms or simple motion detection methods that can identify movement but lack the intelligence to understand the nature of the activity. These systems often generate false alarms due to environmental changes such as lighting variations, shadows, or non-threatening movements.

Although some modern systems incorporate machine learning techniques, they are often limited to detecting predefined actions and lack the ability to generalize across different scenarios. These systems may struggle with complex activities, crowded environments, and variations in human behavior. Additionally, many existing solutions do not operate in real time or require significant computational resources, making them less practical for large-scale deployment. The lack of accurate and efficient activity recognition limits their effectiveness in ensuring public safety.

IV. PROPOSED SYSTEM

The proposed system introduces a deep learning-based framework for automatic detection of suspicious human activities from surveillance videos. The system captures video input from cameras and processes it into frames for analysis. A Convolutional Neural Network (CNN) is used to extract spatial features from each frame, while a Long Short-Term Memory (LSTM) network analyzes temporal relationships between consecutive frames. This combination enables the system to understand both appearance and motion patterns, allowing accurate classification of human activities.

When suspicious behavior such as fighting, abnormal running, or unauthorized actions is detected, the system immediately generates alerts and sends notifications to concerned authorities. The system is designed to operate in real time, ensuring quick response and intervention. It also maintains a database of detected activities for future analysis and model improvement. This approach reduces human dependency, minimizes false alarms, and enhances the overall efficiency and reliability of surveillance systems.

V. SYSTEM ARCHITECTURE

The system architecture for suspicious human activity recognition is designed as a multi-stage pipeline that processes surveillance video data in real time. The first stage involves video acquisition, where input is captured from CCTV cameras or stored video datasets. The video is then divided into frames and passed to the preprocessing module, which performs operations such as noise reduction, resizing, and normalization to improve data quality. After preprocessing, the feature extraction module uses deep learning models like

Convolutional Neural Networks (CNN) to extract spatial features from each frame, capturing important visual information such as human posture, movement, and surrounding context.

The extracted features are then fed into a temporal analysis module, typically based on Long Short-Term Memory (LSTM) networks or similar sequence models, which analyze the sequence of frames to understand motion and behavior patterns over time. The classification module uses these learned features to distinguish between normal and suspicious activities. Once a suspicious activity is detected, the system triggers an alert mechanism that sends notifications to authorities or security personnel. Additionally, the architecture includes a database for storing video logs and detected events, along with a user interface that allows real-time monitoring and review. This layered architecture ensures efficient processing, accurate detection, and timely response in surveillance applications.



Fig 5.1: System Architecture

VI. IMPLEMENTATION



Fig 6.1: Monitering

Received: 01-05-2026 | Accepted: 08-06-2026 | Published: 15-06-2026 | www.ajaccm.com



Fig 6.2: Alert



Fig 6.3: Real-Time Data



Fig 6.4: Emergency Response

VII. CONCLUSION

In conclusion, the proposed system demonstrates the effectiveness of deep learning techniques in automating the detection of suspicious human activities from surveillance videos. By combining CNN and LSTM models, the system is capable of accurately analyzing both spatial and temporal features of human behavior. This enables real-time identification of abnormal activities, significantly improving the efficiency of surveillance systems and reducing reliance on manual monitoring.

The implementation of such intelligent systems can greatly enhance public safety by enabling proactive threat detection and faster response to emergencies. The system not only reduces human workload but also ensures continuous and reliable monitoring. Its adaptability and scalability make it suitable for deployment in various environments such as public spaces, transportation hubs, and commercial areas.

VIII. FUTURE SCOPE

The future scope of this project includes improving the accuracy and robustness of the system by incorporating advanced deep learning models such as 3D CNNs and transformer-based architectures. These models can capture more complex spatial-temporal features and improve performance in challenging scenarios such as crowded environments or low-light conditions. Additionally, integrating facial recognition and object tracking can further enhance the system's capability to identify individuals and track suspicious activities over time.

The system can also be expanded to support large-scale smart city applications by integrating with cloud computing and edge devices for faster processing and scalability. Mobile applications can be developed to provide real-time alerts and remote monitoring capabilities to users and authorities. Furthermore, incorporating predictive analytics can help in identifying potential threats before they occur, making

Received: 01-05-2026 | Accepted: 08-06-2026 | Published: 15-06-2026 | www.ajaccm.com

the system more proactive and efficient in ensuring public safety.

IX. REFERENCES

1. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *IEEE Signal Processing Magazine*, vol. 33, no. 6, pp. 62–78, Nov. 2015.
    A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Advances in Neural Information Processing Systems (NIPS)*, 2012, pp. 1097–1105.
2. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *Proc. Int. Conf. Learning Representations (ICLR)*, 2015.
3. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, real-time object detection," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 779–788.
4. R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2014, pp. 580–587.
5. S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
6. D. Tran, L. Bourdev, R. Fergus, L. Torresani, and M. Paluri, "Learning spatiotemporal features with 3D convolutional networks," in *Proc. IEEE Int. Conf. Computer Vision (ICCV)*, 2015, pp. 4489–4497.
7. [8] H. Wang and C. Schmid, "Action recognition with improved trajectories," in *Proc. IEEE Int. Conf. Computer Vision (ICCV)*, 2013, pp. 3551–3558.
8. Laptev, "On space-time interest points," *International Journal of Computer Vision*, vol. 64, no. 2–3, pp. 107–123, 2005.
9. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.
10. W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 6479–6488.
11. M. Ziaeefard and R. Bergevin, "Semantic human activity recognition: A literature review," *Pattern Recognition*, vol. 48, no. 8, pp. 2329–2345, 2015.
12. C. Szegedy et al., "Going deeper with convolutions," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 1–9.
13. G. Varol, I. Laptev, and C. Schmid, "Long-term temporal convolutions for action recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 6, pp. 1510–1517, 2018.
    A. Doshi and M. M. Trivedi, "On the roles of eye gaze in predicting driver's intent," in *Proc. IEEE Intelligent Vehicles*.
14. Todupunuri, A. (2024). Exploring the use of generative AI in creating deepfake content and the risks it poses to data integrity, digital

identities, and security systems. Available at SSRN 5014688.
15. Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.
16. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
17. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
18. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
19. Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.
20. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
21. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
22. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
23. Cyril, H. P., & Kumara, S. (2026, February). DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.
24. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
25. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
26. Viswanathan, V. (2024). Embedding Ethical Principles into Generative AI Workflows for Project Teams.
27. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.
28. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
29. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
30. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.
31. Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.
32. Maturi, S. Y. (2024). Cryptographic privacy engines: Practical multi-party protocols for confidential database queries. Nanotechnology Perceptions, 20(S13), 2770–2785
33. Maturi, S. Y. (2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental

Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010

34. Chowdhury, A. K., Muhit, M. M. I., & Islam, M. M. (2023). A practical review to the marine maintenance practice in Bangladesh and a proposed way forward to an efficient, long-term and cost-effective solution. In Proceedings of the 13th International Conference on Marine Technology (MARTEC 2022). https://doi.org/10.2139/ssrn.4445071
35. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
36. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
37. Ravishankara, M. (2026, February). CircuChain: Disentangling Competence and Compliance in LLM Circuit Analysis. In SoutheastCon 2026 (pp. 1-7). IEEE.
38. Doragacharla, V. R. (2023). Comprehensive Benchmarking Analysis of Auto Scaling Approaches in Cloud Native Streaming Pipelines During Flash Sales and Holiday Traffic Peaks. Available at SSRN 6566479.
39. P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).
40. Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708
41. Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469
42. Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838
43. Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329
44. Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783
45. Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. Journal Of Multidisciplinary, 5(8), 219-225.
46. Harshitha, G. K., & Rajashekar, K. K. (2025). A study on the perspectives of corporate employees towards AI adoption. Journal of International Commercial Law and Technology, 6(1), 699–706.