IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |

Pose Net and IoT Integration: Advanced Threat Detection in Surveillance Systems

Ambica Reddy. S, Ankitha Sharma, Thigulla Amulya, Mrs. Swapna. C

BE, Department of ADCE, Stanley Collage of Engineering and Technology, OU Hyderabad, Telangana, India

Assistant Professor, ADCE, Stanley Collage of Engineering and Technology, OU Hyderabad, Telangana, India

ABSTRACT: This study exploits surveillance technologies with the Internet of Things (IoT) architecture to present a comprehensive solution to solve the growing issues of theft and insecurity. In contrast to traditional systems that utilize post-event evaluation of videos, our method incorporates a comprehensive and small-sized solution onto a single Raspberry Pi. The system employs an efficient object detection model based on Machine Learning, as well as powerful Image Enhancement technology, to recognize human movement even when faced with inadequate circumstances. Earlier attempts to detect human presence and notify the appropriate parties in emergency scenarios using motion detection systems and Internet of Things (IoT) sensors proved to be inaccurate. Our suggested security alarm system provides an economical and effective home monitoring solution by leveraging a Raspberry Pi's low-processing-power chips, sensors, and a Pi camera. More versatility is added to the model by employing machine learning (ML) to train it on a variety of activity datasets. Through the usage of the Pi camera, the system processes images in real-time and sets off a buzzer alarm to alert homeowners or authorized users to possible intrusions or suspicious activity. Residents' total safety is improved by the system's integration of IoT-based design, which fortifies security measures, issues early alerts, and protects against attackers. The limits of current technology are addressed by this creative solution, which offers a dependable and practical method of home protection under a variety of circumstances.

KEYWORDS: Surveillance technologies, home monitoring, low-processing-power chips early alerts

I. INTRODUCTION

One revolutionary development in security is the incorporation of Artificial Intelligence (AI) into surveillance camera s, especially for the purpose of identifying questionable activity. Real-time video feeds are analyzed by AI cameras through the convergence of Machine Learning (ML) and the Internet of Things (IoT), which makes it possible to locate anomalies and possible security issues. In addition to providing a flexible and dynamic response to changing security concerns, this technology is widely used in public areas, transit networks, and commercial businesses. The breadth is broad, but it still needs to solve issues with infrastructure requirements, algorithmic bias, privacy, and security. The ethical and standard laws. In the everchanging surveillance landscape are more important than ever since the proper use of AI cameras requires a careful balance between improving security measures and protecting individual rights. In spite of this progress, there are still some issues and drawbacks that need to be addressed. Security cameras with facial recognition technology are widely used, which raises privacy issues because they may be used for tracking and identification purposes without authorization. Threats to the confidentiality and integrity of recorded video data are presented by the interplay between IoT and surveillance, which creates data security vulnerabilities. Another issue with machine learning models used for suspicious behavior detection is algorithmic bias, which can result in incorrect identification or profiling of particular people or communities. Aside from that, there are operational and budgetary difficulties associated with the implementation of complete AI camera systems due to the significant infrastructure and resource needs, maintenance expenses, and possible latency problems. Even though AI cameras have the ability to completely change the way that people think about security, a thorough grasp of these difficulties is necessary to reduce risks and make sure that these technologies are used in an ethical and responsible manner. Striking a balance between enhancing security measures and safeguarding individual rights requires standardized regulations and guidelines, providing clarity on accountability, transparency, and oversight in the deployment of AI-powered surveillance systems within the domains of IoT, computer vision,and machine learning.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |

II. LITERATURE SURVEY

The focus of this study is on indoor and outdoor security through a discussion of various approaches for identifying anomalous or suspicious human behaviors in digital surveillance. The projects are meant to improve behaviour recognition in real time, which isimportant for spotting any threats. Using a Semantic approach that effectively separates suspicious activity, motion features, and historical data through background subtraction and correlation techniques, one proposed hierarchical method makes use of motion characteristics to identify suspicious behaviors. This reduces computational complexity and increases efficiency.

- Another proposal is to use a deep convolutional architecture for video surveillance, with modules for human subject detection, posture classification, and anomalous behaviour detection based on LSTM. Benchmark datasets verify this method's satisfactory performance in identifying anomalous behaviour inreal-world circumstances.
- The Advance Motion Detection (AMD) technique is introduced to detect unauthorized entry into restricted regions by utilizing background removal with cheap
- Computing cost for real-time video interpretation. However, integration with cutting-edge video collecting techniques in watching zones might be required due to storage capacity constraints.
- Author who wants to automate camera event detection emphasizes the value of surveillance data indexing and storage for public safety, traffic management, and theft prevention. This highlights the import of surveillance research in the context of rising populations andtechnological advancement.
- Another work suggests a semantic-based method that classifies things as living or non-living by using immediate blob matching, Haar-like algorithms, and background removal. It also has the ability to detect the presence of fire.

YEAR	RESERCH PAPER TITLE	AUTHOR'S NAME	METHODOLO GY	RESERACH GAP
2016	"Detection and Tracking of Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras."	Musale, Jitendra, Akshata Gavhane	Haar-like Algorithm.	Object tracking was done using a Real-Time blob-matching algorithm.
2017	"Inspection of suspicious human activity in the crowd sourced areas capturedin surveillance cameras."	Divya, P. Bhagya, S. Shalini, R. Deepa, and Baddeli Sravya Reddy .	Hierarchical approach.	The Semantic approach defines suspicious activities, background subtraction detects objects, correlation technique tracks them,and motion features and temporal information classify events.motion features and temporal information classify events.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |

2018	"Abnormal event detection based on analysis of movement information ofvideo sequence."	Ko, Kwang-Eun, and Kwee-Bo Sim	Hidden Markov model	Detecting abnormal events in video surveillance is difficult but significant for security systems. Making sure that security cameras can spot unusual things happening is really important, but it's not easy.
2019	"Automated Video Surveillance."	Jadhav, Mrs Prajakta,Mrs Shweta Suryawanshi, and Mr Devendra Jadhav	OpenCV, TensorFlow,CNN.	With the advancement of technology and population, surveillance research has become increasingly relevant. The goal of author is to automate camera event detection because time-consuming and inefficient manual monitoring still exists. Since video surveillance is an essential security measure for public safety, traffic

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |

				management, and
				theft prevention in a variety of situations, the author also focuses on the effective storage and indexing of surveillance data.
2020	"Utilizing Deep learning approach for suspicious activity detection from surveillance video."	Amrutha, C. V., C. Jyotsna, and J. Amudha.	Advance Motion Detection (AMD) algorithm.	The system was limited in terms of storage service.
2023	" Suspicious Activity Detection: Techniques, Application and Challenges. "	Nandini Fal Dessai, Prof. Shruti Pednekar.	CNN, LRCN	This system needs to be trained to recognize the suspicious activities that might happen in thoseplaces.

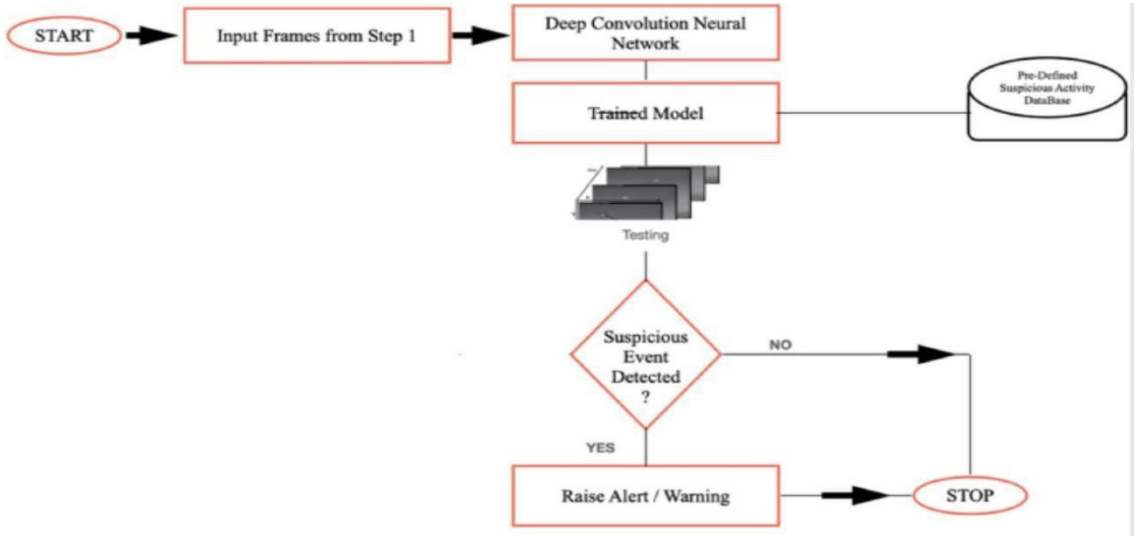
III. METHEDOLOGY

The surveillance system, designed for detecting suspicious activities, integrates three key methodologies to achieve its functionality: IoT integration, CNN for object detection, and PoseNet for human pose estimation. The IoT integration methodology plays a crucial role by incorporating various sensors, such as motion detectors and sound sensors, connected to the Raspberry Pi via GPIO pins. This allows for the capture of non-visual contextual information, enriching the system's understanding of the environment. Object detection using CNNs enhances the system's capacity to recognize and analyze entities within the camera feed, optimizing for real-time processing on the Raspberry Pi and reducing dependency on external servers. PoseNet, operating in real-time on the Raspberry Pi, contributes to the system by analyzing human poses, aiding in the identification of suspicious activities based on human movement patterns. Together, these methodologies create a comprehensive and adaptable surveillance system capable of effectively identifying and responding to security threats in real-time, leveraging both visual and non-visual cues for enhanced accuracy and responsiveness.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |



Proposed system:

REQUIREMENTS:

The following are the hardware and software requirements for implementing the proposed system:

HARDWARE REQUIREMENTS

1. AI Camera: Google Teachable AI camera
2. Raspberry Pi Circuit Board
3. Alarm system

SOFTWARE REQUIREMENTS

1. Operating System: Windows
2. Visual Studio
3. AI Libraries: TensorFlow or PyTorch
4. IoT Platform: MQTT for communication, Azure IoT or Google Cloud IoT Core for data aggregation and analysis
5. Alarm Software: Custom scripts or applications for configuring and controlling the alarm system.

Advantages:

Advantages of using Google Teachable's PoseNet for suspicious activity detection:

1. PoseNet offers real-time human pose estimation, enabling the system to analyze human movements instantly, which is crucial for timely detection of suspicious activities.
2. Google Teachable's PoseNet is known for its accuracy in detecting various human poses, providing reliable data for identifying potential threats accurately.
3. PoseNet is relatively easy to implement and integrate into existing systems, making it accessible for developers with varying levels of expertise.

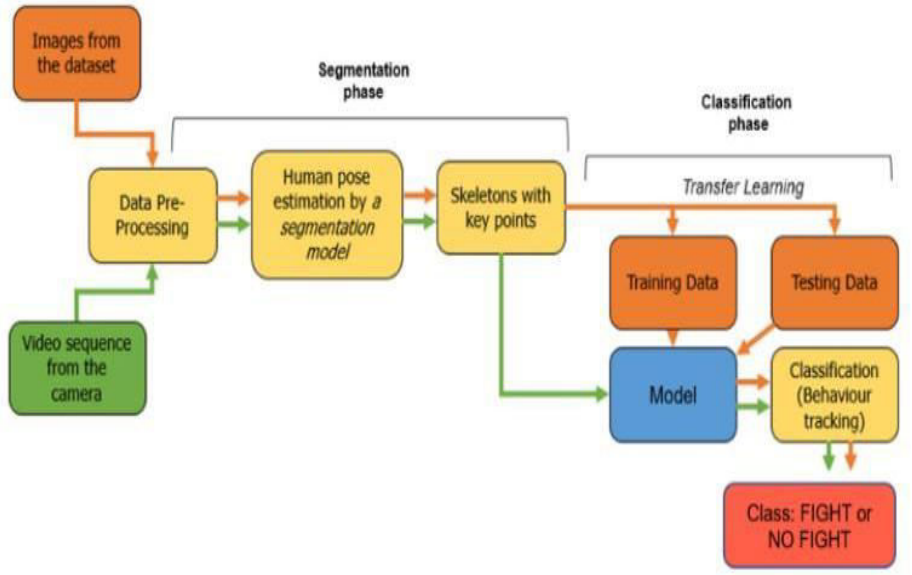
Disadvantages:

1. PoseNet primarily focuses on human pose estimation and may lack the ability to understand complex contextual information, potentially leading to false alarms or missed detections in certain scenarios.
2. PoseNet relies solely on visual cues derived from human poses, which may not be sufficient for detecting certain types of suspicious activities that require additional contextual information from other sensors.
3. While PoseNet can run on edge devices like the Raspberry Pi, it still requires a certain level of computational resources, which may limit its scalability in large-scale surveillance deployments.
4. PoseNet's performance may be affected by variations in lighting conditions, leading to inaccuracies in pose estimation, especially in low-light environments.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305539 |



IV. CONCLUSION

In summary, the integration of IoT technology and AI camera systems for detecting suspicious activity represents a significant advancement in security across various settings. Leveraging PoseNet and smart machine learning techniques, our system identifies potential threats by analyzing unusual motions and postures. The seamless integration of AI and IoT allows for continuous monitoring and rapid response to changing circumstances, showcasing the potential of artificial intelligence in bolstering security systems. PoseNet plays a crucial role in capturing human postures and movements, enhancing behavior analysis and providing a comprehensive surveillance solution. The cooperative synergy between PoseNet and IoT integration further enhances anomaly detection and facilitates smooth communication between the AI camera and connected devices. This preventive security solution offers continuous monitoring and opens doors for future innovations. The effective application of this technology contributes to ongoing advancements in security solutions, paving the way for increasingly complex and intelligent monitoring systems. Overall, our project signifies a significant step forward in utilizing IoT and artificial intelligence to enhance public safety and security on a large scale.

REFERENCES

1. The paper titled "Detection and Tracking of Suspicious Movements of Humans and Objects, Including Fire Detection, Utilizing Closed-Circuit Television (CCTV) Cameras" by Musale, Jitendra, and Akshata Gavhane was published in Volume 5 of the International Journal for Research in Applied Science & Engineering Technology (IJRASET) in 2016.
2. "Inspection of Suspicious Human Activity in Crowdsourced Areas Captured in Surveillance Cameras" by Divya, P., Bhagya, S., Shalini, S., Deepa, R., and Baddeli Sravya Reddy, (IRJET) in 2017.
3. "Deep Convolutional Framework for Abnormal Behavior Detection in a Smart Surveillance System" by Ko, Kwang-Eun, and Kwee-Bo Sim. Volume 67 (2018) of Engineering Applications of Artificial Intelligence.
4. "Automated Video Surveillance" by Jadhav, Mrs. Prajakta, Mrs. Shweta Suryawanshi, and Mr. Devendra Jadhav. (2019).
5. Amrutha, C. V., C. Jyotsna, and J. Amudha presented their work titled "Utilizing Deep Learning for Detecting Suspicious Activities in Surveillance Videos" at the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). Their research was later published in an IEEE journal.
6. "Suspicious Activity Detection: Techniques, Applications, and Challenges" by Nandini Fal Dessai and Prof. Shruti Pednekar. (2023)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details